EFFECTS OF BEHAVIORAL DECISION-MAKING IN GAME-THEORETIC FRAMEWORKS FOR SECURITY RESOURCE ALLOCATION IN NETWORKED SYSTEMS

by

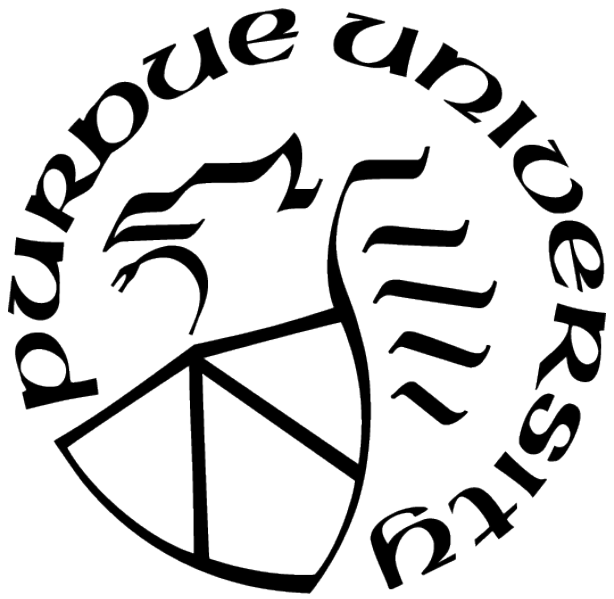
Mustafa Abdallah

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy



School of Electrical and Computer Engineering

West Lafayette, Indiana

August 2022

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Saurabh Bagchi, Co-Chair

School of Electrical and Computer Engineering

Dr. Shreyas Sundaram, Co-Chair

School of Electrical and Computer Engineering

Dr. Timothy Cason

Krannert School of Management

Dr. Xiaojun Lin

School of Electrical and Computer Engineering

Approved by:

Dedicated To

My Father

For supporting me throughout all my life until his death on April 2012. My father traveled for several years to ensure the quality of education for his family members. He taught me to trust in Allah (the Almighty), seek his continuous help, and strive to be a better person throughout my life journey. Being a math teacher, he taught me to love mathematics, try hard to enhance my skills, and work hard to try to achieve my goals.

My Mother

For supporting me and my sisters throughout our lives. For her kind soul, efforts, care, and the unlimited and unconditional love to us despite her health conditions. Seeing her happy with any achievement I have makes me satisfied. May Allah (the Almighty) grant her a long healthy life.

My Wife

For supporting me and taking care of our small family throughout the PhD. For her efforts, care, and unlimited love to me, specially during the stressful times and failures during the challenging journey of the PhD. May Allah (the Almighty) grant her a long healthy life.

ACKNOWLEDGMENTS

First, I would like to express my sincere gratitude to my advisors Prof. Shreyas Sundaram and Prof. Saurabh Bagchi. All throughout my graduate studies, they have given me considerable freedom in pursuing my own research interests. This work would not have been possible without their technical expertise in a vast array of subjects, attention to detail, emphasis on mathematical rigour, focus on practical applications of the work, and patience while going through my drafts countless number of times. Prof. Sundaram and Prof. Bagchi have been very generous in supporting me to attend several conferences and workshops, and been incredibly helpful during the job search process. I recall having a whole semester getting advice from Prof. Sundaram for the job application/interview process. I also recall the many DCSL socials by Prof. Bagchi for having fun and recharging group members' energy. I could not have found any other advisors who are as supportive, passionate and dedicated towards training their graduate students as Prof. Sundaram and Prof. Bagchi.

Second, I would also like to thank the members of my thesis committee (Professors Timothy Cason and Xiaojun Lin) for their feedback and suggestions. I have had an enjoyable and great learning experience collaborating with Prof. Timothy Cason and I learned a lot from his in-depth knowledge in economics and I was amazed how humble and supportive he is. I also have had an enjoyable and great learning experience collaborating with Prof. Parinaz Naghizadeh, Prof. Ashsish Hota, and Prof. Issa Khalil, and I am indebted to Prof. Cason and Prof. Naghizadeh for their support during my job applications. I would also like to thank Dr. Daniel Woods who collaborated with me doing insightful human subject experiments that are well grounded by following experimental economics guidelines.

Third, I specifically thank all my lab mates and colleagues from both groups, specifically Ashraf, Mahmoud, Aritra, Naif, Lintao, Edgardo, Jonny, Hemant, Baike, Amritha, Tong, Heng, and Lei, both for sharing the laughter and having nice souls and cheerful characters that make the PhD journey much better experience.

Finally, this research was supported by grant CNS-1718637 from the National Science Foundation (NSF). I was also supported for one year from Wabash Heartland Innovation Network (WHIN) project from Lilly Endowment Inc. NSF CCF-1919197.

PREFACE

This is the preface.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

CPS	Cyber-Physical Systems
SR	Sensitivity ratio
PNE	Pure Strategy Nash Equilibrium
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
SCADA	Supervisory Control and Data Acquisition
CPR	Common Pool Resources

ABSTRACT

Facing increasingly sophisticated attacks from external adversaries, interdependent systems owners have to judiciously allocate their (often limited) security budget in order to reduce their cyber risks. However, when modeling human decision-making, behavioral economics has shown that humans consistently deviate from classical models of decision-making. Most notably, prospect theory, for which Kahneman and Tversky won the 2002 Nobel memorial prize in economics, argues that humans perceive gains, losses and probabilities in a skewed manner. While there is a rich literature on prospect theory in economics and psychology, most of the existing work studying the security of interdependent systems does not take into account the aforementioned biases.

In this thesis, we propose novel mathematical behavioral security game models for the study of human decision-making in interdependent systems modeled by directed attack graphs. We show that behavioral biases lead to suboptimal resource allocation patterns. We also analyze the outcomes of protecting multiple isolated assets with heterogeneous valuations via decision- and game-theoretic frameworks, including simultaneous and sequential games. We show that behavioral defenders over-invest in higher-valued assets compared to rational defenders. We then propose different learning-based techniques and adapt two different tax-based mechanisms for guiding behavioral decision-makers towards optimal security investment decisions. In particular, we show the outcomes of such learning and mechanisms on four realistic interdependent systems. In total, our research establishes rigorous frameworks to analyze the security of both large-scale interdependent systems and heterogeneous isolated assets managed by human decision makers, and provides new and important insights into security vulnerabilities that arise in such settings.

1. INTRODUCTION

1.1 Problem and Motivation

Today's cyber-physical systems (CPS) are increasingly facing attacks by sophisticated adversaries. The operators of such systems have to judiciously allocate their (often limited) security budgets to reduce security risks of the systems they manage. This resource allocation problem is further complicated by the fact that a large-scale system consists of multiple interdependent subsystems managed by different operators, with each operator in charge of securing her own subsystem. This has led to significant research in understanding how to better secure these systems, with strategic and game-theoretical models receiving increasing attention due to their ability to systematically capture the decisions made by the various entities in the system [1]–[7]. In particular, these settings have been explored under various assumptions on the strategies and information available to defenders and attackers [8]–[10].

Prior work has considered such security decision-making problems in both decision-theoretic and game-theoretic settings [3], [11]. However, most of the existing work relied on *classical models* of decision-making, where all defenders and attackers are assumed to make fully rational risk evaluations and security decisions [3], [12], [13]. On the other hand, behavioral economics has shown that humans consistently deviate from these classical models of decision-making. Most notably, research in *behavioral economics* has shown that humans perceive gains, losses and probabilities in a skewed, nonlinear manner [14]. In particular, humans typically overweight low probabilities and underweight high probabilities, where this weighting function has an inverse S-shape, as shown in Figure 2.2. Many empirical studies (e.g., [14], [15]) have provided evidence for this class of behavioral models.

These effects are relevant for evaluating security of such systems in which decisions on implementing security controls are not made purely by automated algorithms, but rather through human decision-making, albeit with help from threat assessment tools [16]–[18]. There are many articles discussing the prevalence of human factors in security decision-making, both in the popular press [19]–[21] and in academic journals [22], [23], none of which however shed light on the impact of cognitive biases on the overall system security.

This thesis bridges the above gap by studying the effect of the aforementioned human behavioral decision-making bias on security resource allocation problem in two main different settings. Our first objective is exploring such effects in the large-scale interdependent systems in which adversaries often use stepping-stone attacks that can be captured via the notion of *attack graphs* that represent all possible paths that attackers may have to reach their targets within the system [24]. The second objective is to explore behavioral decision-making in different setups (including simultaneous and sequential interactions among defenders and attacker) with isolated assets that have heterogeneous valuations to the defenders using decision- and game-theoretic settings.

The key message of this thesis is:

By incorporating non-linear probability weighting in decision-making modeling, we can predict the effect of behavioral decision-making biases on security resource allocations on networked systems, and provide guidance on mitigating the negative effects such biases.

The thesis also proposes guiding techniques to enhance the human security resource allocation both on individual level (using learning techniques) and social level (using mechanism design) where we explore the difference between rational and behavioral decision-makers on the outcomes of those guiding techniques.

We next provide an overview of the aforementioned settings and our contributions in a variety setting.

1.2 Behavioral and Game-Theoretic Security Investments in Interdependent Systems Modeled by Attack Graphs

In this line of work, we consider the scenario where each (human) defender misperceives the probabilities of successful attack in an "attack graph" model of interdependent systems. We characterize the impacts of such misperceptions on the security investments made by each defender where each defender is responsible for defending a subnetwork (i.e., set of assets). Furthermore, each defender can also invest in protecting the assets of other defenders, which may be beneficial in interdependent systems where the attacker exploits paths through the network to reach certain target nodes. Under appropriate assumptions on the probabilities of successful attack on each edge, we establish the convexity of the perceived expected cost

of each defender and prove the existence of a pure strategy Nash equilibrium (PNE) in this class of games.

We primarily investigate the security investments when users with such behavioral biases act in isolation as well as in a game-theoretic setting. As a result, we find certain characteristics of the security investments under behavioral decision-making that could not have been predicted under classical notions of decision-making (i.e., expected cost minimization) considered in prior work [9]. In particular, we show that nonlinear probability weighting can cause defenders to invest in a manner that increases the vulnerability of their assets to attack. Furthermore, we illustrate the impacts of having a mix of defenders (with heterogeneous levels of probability weighting bias) in the system, and show that the presence of defenders with skewed perceptions of probability can in fact *benefit* the non-behavioral defenders in the system. We then propose a new metric, *Price of Behavioral Anarchy (PoBA)*, to capture the inefficiency of the equilibrium investments made by behavioral decision-makers compared to a centralized (non-behavioral) socially optimal solution, and provide tight bounds for the PoBA.

1.3 Protecting Isolated Assets with Heterogeneous Valuations under Behavioral Probability Weighting

1.3.1 Decision-Theoretic Analysis

One of the seminal works pertaining to strategic (or economic) decision-making in security is [25], which considered a single defender protecting a single node, where the vulnerability of the node can be reduced by investments in that node. The authors provided insights into the investments made by the defender for such settings. Such *decision-theoretic* formulations of defender(s) choosing investments to protect asset(s) against non-strategic attackers have been studied extensively (for example see [9], [26]–[28] and the references therein). However, as mentioned above, in most of these works the defenders are modeled as fully rational decision-makers (perhaps with some measure of risk-aversion [27]) who choose their actions to maximize their expected utilities.

In this work, we introduce prospect theory into a decision-theoretic security framework involving a defender protecting multiple assets with heterogeneous valuations. Specifically, we consider a CPS consisting of many assets, and assume that the defender misperceives the probabilities of successful compromise of each asset. We characterize the impacts of such misperceptions on the security investments made by the defender. In particular, we show that behavioral probability weighting causes the defender to shift more of her investments to higher-valued assets compared to a defender who correctly perceives the attack probabilities. In particular, the number of nodes that have positive investment decreases as the defender becomes more behavioral. This shift in investments thereby leads to an increase in (true) expected loss for the behavioral defender.

1.3.2 Multi-Defender Game-theoretic Analysis

In this work, We consider a setting of common-pool resource game where the resource experiences failure with a probability that decreases with the aggregate investment in the resource. The players in that game are required to invest (subject to a budget constraint) in protecting a given set of nodes from failure. Each node has a certain value to each player, along with a probability of failure, which is a function of the total investment in that node by the players. In this setting, we consider the impacts of behavioral probability weighting (vis-*à*-vis the probability of failure) on the investment strategies; such probability weighting, where humans weight probabilities in a non-linear manner, has been identified by behavioral economists to be a common feature of human decision-making. We study the game-theoretic setting with multiple (behavioral) players and show that pure strategy Nash equilibria exist in that game, and show the uniqueness of the total investments on each node at all equilibria. Furthermore, we show that inverse S-shape behavioral probability weighting (where the player overweights low probabilities and underweights high probabilities) causes the player to shift more of her investments to the higher-valued nodes and underinvest in the low-value nodes, compared to the case where the player perceives the probability of failure correctly. In particular, the number of nodes that have positive investment decreases as the player becomes more behavioral. On the other hand, we show that the number of nodes that

have positive investment increases under S-shape behavioral probability weighting (where the player underweights low probabilities and overweights high probabilities). Finally, we quantify the effect of heterogeneity of behavioral levels on the investments at PNE and compare different possible training policies for enhancing social cost. We illustrate our theoretical findings via numerical simulations.

1.3.3 Sequential Defender-Attacker Game Analysis

In contrast to decision-theoretic formulations of defender(s) that consider non-strategic attackers, game-theoretic models have been explored under various assumptions on the strategies available to the defenders and attackers [3], [4], [9]. In particular, scenarios where the attacker strategically reacts to the defender's actions have been studied in [7], [29], [30]. Of particular interest to our work here is the paper [30], which considered a sequential defender-attacker framework, and showed the optimal strategies for each player. Again, a common thread in much of that existing work is that the defenders and attackers are assumed to behave according to classical models of fully rational decision-making.

In this line of work, we introduce prospect theory into a sequential game-theoretic framework involving one defender and one attacker. Specifically, we consider the scenario where a (human) defender misperceives the probabilities of successful attack in each site. We characterize the impacts of such misperceptions on the security investments made by the defender, and on the decisions of the attacker. In contrast to [31]–[33], where the authors considered the impact of such probability weighting in certain specific classes of interdependent security games without strategic adversaries, we consider the case where the defender places her investments to best protect her sites, accounting for a strategic attacker who chooses which site to compromise to maximize the expected loss of the defender.

We first show the uniqueness of the (perceived) optimal defense allocation of the defender (under behavioral probability weighting). We then characterize the impacts of probability weighting on the investment decisions made by the defenders; in particular, we show that nonlinear perceptions of probability can induce the defender to shift her optimal investments in a manner that increases her loss when attacked. Finally, we introduce the notion of Price

of Behavioral Probability Weighting (PoBW) to quantify the inefficiency of the behavioral defender's investment on her true expected loss. We provide bounds on the PoBW, and provide numerical examples to illustrate the above phenomena.

1.3.4 Simultaneous Attacker-Defender Game Analysis

A particular class of simultaneous move games involving attackers and defenders (where the players have to choose their strategies at the same time, without first observing what the other player has done) have been studied in various contexts. For example, the Colonel Blotto game [34] is a useful framework to model the allocation of a given amount of resources on different potential targets (i.e., battlefields) between the attacker and the defender. Specifically, [35] proposed a solution of the heterogeneous Colonel Blotto game with asymmetric players (i.e., with different resources) and with a number of battlefields that can have different values. While Colonel Blotto games typically involve deterministic success functions (where the player with the higher investment on a node wins that node), other work has studied cases where the win probability for each player is a probabilistic (and continuous) function of the investments by each player [7].

In these works, following classical game-theoretical models of human decision-making, defenders and attackers are considered to be fully rational decision-makers who choose their actions to maximize their expected utilities. Few exceptions have focused on the impact of probability weighting on a single defender's decisions via decision-theoretic analysis (with no strategic attacker) [33], on multiple defenders' investments in networks (with the emphasis being on understanding the role of the network structure) [31], or on behavioral decision-making by both players for settings with a single target [36]. In contrast to these works, we consider the effects of behavioral decision-making in a setting with multiple targets with different values to the players (i.e., the defender and the attacker).

In this work, we introduce prospect theory into a game-theoretic framework involving an attacker and a defender. Specifically, we consider a CPS consisting of many assets, and assume that the defender misperceives the probabilities of successful compromise of each asset. We first establish the convexity of the objective function of each player (i.e., attacker

and defender), and we use this to prove the existence of a pure strategy Nash equilibrium (PNE) for the Behavioral Multi-Target Security Game. We then show the uniqueness of that PNE in our game. We then characterize the optimal investment strategies by the (rational) players. We then show that the defender and the attacker invest more in higher value assets (under appropriate conditions). Subsequently, we show via numerical simulations that nonlinear perceptions of probability can induce defenders to shift more of their investments to the more valuable assets, thereby potentially increasing their (true) expected loss.

1.4 Guiding Behavioral Decision-Makers towards Better Security Investment in Interdependent Systems

In the previous formulations, we have shown that behavioral decision-making leads to suboptimal resource allocation compared to non-behavioral decision-making. In this line of work, we try to guide behavioral decision-makers towards better security investments. In particular, we design a reasoning and security investment decision-making technique for interdependent systems. We propose different learning-based techniques for guiding behavioral decision-makers towards optimal investment decisions for two different scenarios where each scenario represents whether the defender has knowledge of the adversary's history (i.e., chosen attack paths in previous rounds) or not. Our proposed techniques enhance the implemented security policy (in terms of reducing the total system loss when compromised by allocating limited security resources optimally). Our system has components for both single-round and multi-round setups.

We perform a human subject study with N = 145 participants where they choose defense allocations in two simple attack graphs. We then evaluate our system using five synthesized attack graphs that represent realistic interdependent systems and attack paths through them. These systems are DER.1 [17], (modelled by NESCOR), SCADA industrial control system, modeled using NIST guidelines for ICS [12], IEEE 300-bus smart grid [37], E-commerce [13], and VOIP [13]. We do a benchmark comparison with two prior solutions for optimal security controls with attack graphs [16], [38], and quantify the level of the underestimation of loss compared to our evaluation where defenders are behavioral. In conducting our analysis and obtaining these results based on a behavioral model, 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, the estimation of baseline attack probabilities and the types of defense mechanisms in our formulations.

1.5 Using Mechanism Design for Enhancing Security Resource Allocation in Interdependent Systems

Another goal when securing interdependent systems is minimizing the social cost of all stakeholders that are defending such systems. In this line of work, we consider two different tax-based mechanisms for guiding behavioral decision-makers and selfish rational decision-makers towards optimal investment decisions in our interdependent security games. Such mechanisms use monetary payments/rewards to incentivize socially optimal (SO) security behavior, i.e., those minimizing the sum of the costs of all defenders due to a security attack. The two tax-based mechanisms are the 'Externality' mechanism [39] and the Vickrey-Clarke-Groves ('VCG') mechanism [40]. These mechanisms enhance the implemented security policy by incentivizing defenders to allocate their limited security resources to minimize the system's social cost.

We show a fundamental result that there exists no reliable tax-based mechanism which can incentivize the socially optimal investment profile while maintaining a weakly balanced budget (i.e., the central regulator does not pay out-of-pocket money) for all instances of interdependent security games. We show the difference between our result and prior results in the security economics literature [40], [41] in Section 8.7. Our result shows that designing mechanisms in interdependent security games is more challenging compared to monolithic systems. We also show the effect of behavioral biases on the two mechanisms' outcomes in our interdependent security games framework. In particular, we show that the behavioral defenders would pay more taxes compared to rational defenders under such tax mechanisms. We then evaluate our findings using four synthesized attack graphs that represent realistic interdependent systems and attack paths through them. In conducting our analysis, we modify mechanism formulations for our interdependent security games (Section 8.5), and incorporate behavioral biases in our formulations (Section 8.2).

1.6 Summary and Outline

This thesis demonstrates the effect of behavioral bias (from prospect theory) on security decision-making in two main settings. First, it proposes novel mathematical behavioral security game models for the study of human decision-making in interdependent systems modeled by directed attack graphs and shows that behavioral biases lead to suboptimal resource allocation patterns on the attack graph edges. Second, it analyzes the outcomes of protecting multiple isolated assets with heterogeneous valuations via decision- and game-theoretic frameworks, including simultaneous and sequential games. It characterizes the impacts of risk misperceptions on security investments in such settings, and shows that behavioral defenders over-invest in higher-valued assets compared to rational defenders. It then provides different learning-based techniques and adapts two different tax-based mechanisms for guiding behavioral decision-makers towards enhancing their suboptimal security investment patterns and making optimal security investment decisions in the aforementioned settings.

1.6.1 Outline of Thesis

The remainder of this thesis is organized as follows. Chapter 2 presents the analysis of behavioral decision-making in interdependent systems. Chapter 3 and Chapter 4 provide the decision-theoretic analysis and game-theoretic analysis of protecting multiple isolated assets with heterogeneous valuations under risk misperceptions, respectively. In Chapter 5, we present a sequential game setting between the defender and an attacker on a CPS that has multiple targets with heterogeneous valuations. Chapter 6 shows the effect of behavioral decision-making on a simultaneous attacker-defender game. In Chapter 7, we present two novel learning algorithms to guide behavioral decision-makers towards better security investments. In Chapter 8, we adapt two mechanism designs for our interdependent security game to achieve the social optimal (which minimizes the social cost of the system). Chapter 9 concludes this dissertation and provides next steps and future work.

2. Behavioral and Game-Theoretic Security Investments in Interdependent Systems Modeled by Attack Graphs

In this chapter, we consider a system consisting of multiple interdependent assets, and a set of defenders, each responsible for securing a subset of the assets against an attacker. The interdependencies between the assets are captured by an attack graph, where an edge from one asset to another indicates that if the former asset is compromised, an attack can be launched on the latter asset. Each edge has an associated probability of successful attack, which can be reduced via security investments by the defenders. In such scenarios, we investigate the security investments that arise under the non-linear probability weighting bias mentioned earlier. We show that suboptimal investments can arise under such weighting in certain network topologies. We also show that PNE exist in settings with multiple defenders, and study the inefficiency of the equilibrium investments by behavioral defenders compared to a centralized socially optimal solution.

2.1 The Security Game Framework

We now describe our general security game framework, including the attack graph and the characteristics of the attacker and the defenders. Figure 2.1 shows overview of our model.

2.1.1 Attack Graph

We represent the assets in a CPS as nodes of a directed graph $G = (V, \mathcal{E})$ where each node $v_{\mathrm{i}} \in V$ represents an asset. A directed edge $(v_{\mathrm{i}}, v_{\mathrm{j}}) \in \mathcal{E}$ means that if v_{i} is successfully attacked, it can be used to launch an attack on v_{j}. The graph contains a designated source node v_s (as shown in Figure 2.1), which is used by an attacker to begin her attack on the network. Note that v_s is not a part of the network under defense; rather it is an entry point that is used by an attacker to begin her attack on the network.[1]

[1]↑If there are multiple nodes where the attacker can begin her attack, then we can add a virtual node v_s, and add edges from this virtual node to these other nodes with attack success probability 1 without affecting our formulation.

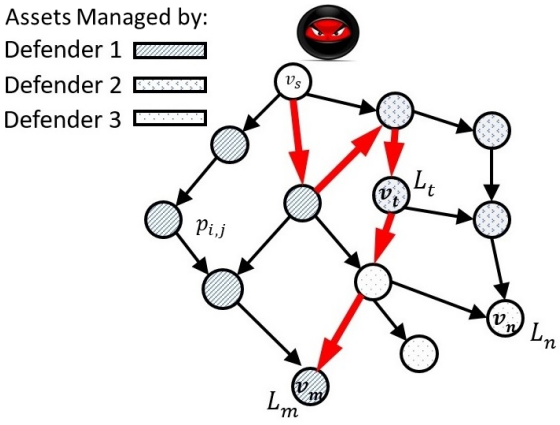


Figure 2.1. Overview of the interdependent security game framework. This CPS consists of three interdependent defenders. An attacker tries to compromise critical assets starting from v_s.

For a general asset $v_t \in V$, we define $\mathcal{P}_t$ to be the set of directed paths from the source v_s to v_t on the graph, where a path $P \in \mathcal{P}_t$ is a collection of edges $\{(v_s, v_1), (v_1, v_2), ..., (v_k, v_t)\}$. For instance, in Figure 2.1, there are two attack paths from v_s to v_t.

Each edge $(v_{\mathrm{i}}, v_{\mathrm{j}}) \in \mathcal{E}$ has an associated weight $p^0_{\mathrm{i,j}} \in (0, 1]$, which denotes the probability of successful attack on asset v_{j} starting from v_{i} in the absence of any security investments.[2]

We now describe the defender and adversary models in the following two subsections.

2.1.2 Strategic Defenders

Let $\mathcal{D}$ be the set of all defenders of the network. Each defender $D_k \in \mathcal{D}$ is responsible for defending a set $V_k \subseteq V \setminus \{v_s\}$ of assets. For each compromised asset $v_m \in V_k$, defender D_k will incur a financial *loss* $L_m \in [0, \infty)$. For instance, in the example shown in Figure 2.1, there are three defenders with assets shown in different shades, and the loss values of specific nodes are indicated.

[2]↑ In practice, CVSS [42] can be used for estimating initial probabilities of attack (for each edge in our setting). For example, [24] takes the Access Complexity (AC) sub-metric in CVSS (which takes values in {low, medium, high}, representing the complexity of exploiting the vulnerability) and maps it to a probability of attack success. The more complex it is to exploit a vulnerability, the less likely an attacker will succeed. Similarly, [43] provides methods and tables to estimate the probability of successful attack from CVSS metrics.

To reduce the attack success probabilities on edges interconnecting assets inside the network, a defender can allocate security resources on these edges.[3] We assume that each defender D_k has a security budget $B_k \in [0, \infty)$. Let $x^k_{\mathrm{i,j}}$ denote the security investment of defender D_k on the edge $(v_\mathrm{i}, v_\mathrm{j})$. We define

$$X_k := \{x_k \in \mathbb{R}^{|\mathcal{E}|}_{\geq 0} | \mathbf{1}^T x_k \leq B_k\}; \tag{2.1}$$

thus X_k is the set of feasible investments for defender D_k and 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 B_k. We denote any particular vector of investments by defender D_k as $x_k \in X_k$. Each entry of x_k denotes the investment on an edge.

Let $\mathbf{x} = \left[x_1, x_2, \ldots, x_{|\mathcal{D}|}\right]$ be a joint defense strategy of all defenders, with $x_k \in X_k$ for defender D_k; thus, $\mathbf{x} \in \mathbb{R}^{|\mathcal{D}||\mathcal{E}|}_{\geq \mathbf{0}}$. Under a joint defense strategy $\mathbf{x}$, the total investment on edge $(v_\mathrm{i}, v_\mathrm{j})$ is $x_{\mathrm{i,j}} \triangleq \sum_{D_k \in \mathcal{D}} x^k_{\mathrm{i,j}}$. Let $p_{\mathrm{i,j}} : \mathbb{R}_{\geq 0} \to [0, 1]$ be a function mapping the total investment $x_{\mathrm{i,j}}$ to an attack success probability, with $p_{\mathrm{i,j}}(0) = p^0_{\mathrm{i,j}}$. In particular, $p_{\mathrm{i,j}}(x_{\mathrm{i,j}})$ is the conditional probability that an attack launched from v_i to v_j succeeds, given that v_i has been successfully compromised.

2.1.3 Adversary Model and Defender Cost Function

In networked cyber-physical systems (CPS), there are a variety of adversaries with different capabilities that are simultaneously trying to compromise different assets. We consider an attacker model that uses stepping-stone attacks [44]. In particular, for each asset in the network, we consider an attacker that starts at the entry node v_s and attempts to compromise a sequence of nodes (moving along the edges of the network) until it reaches its target asset. If the attack at any intermediate node is not successful, the attacker is detected and removed from the network. Note that our formulation allows each asset to be targeted by a different attacker, potentially starting from different points in the network.

In other words, after the defense investments have been made, then for each asset in the network, the attacker chooses the path with the highest probability of successful attack for

[3]↑Note that v_s does not have any incoming edges, and hence, it can not be defended.

that asset (such a path is shown in red in Figure 2.1). Such attack models (where the attacker chooses one path to her target asset) have previously been considered in the literature (e.g., [45], [46]).

To capture this, for a given set of security investments by the defenders, we define the *vulnerability* of a node $v_m \in V$ as $\max_{P \in \mathcal{P}_m} \prod_{(v_i,v_j)\in P} p_{i,j}(x_{i,j})$, where $\mathcal{P}_m$ is the set of all directed paths from the source v_s to asset v_m; note that for any given path $P \in \mathcal{P}_m$, the probability of the attacker successfully compromising v_m by taking the path P is $\prod_{(v_i,v_j)\in P} p_{i,j}(x_{i,j})$, where $p_{i,j}(x_{i,j})$ is the conditional probability defined at the end of Section II-B. In other words, the vulnerability of each asset is defined as the maximum of the attack probabilities among all available paths to that asset.

The goal of each defender D_k is to choose her investment $x_k \in X_k$ in order to minimize the expected cost defined as

$$\hat{C}_k(x_k, \mathbf{x}_{-k}) = \sum_{v_m \in V_k} L_m \left(\max_{P \in \mathcal{P}_m} \prod_{(v_i,v_j)\in P} p_{i,j}(x_{i,j}) \right) \tag{2.2}$$

subject to $x_k \in X_k$, and where $\mathbf{x}_{-k}$ is the vector of investments by defenders other than D_k. Thus, each defender chooses her investments in order to minimize the vulnerability of her assets, i.e., the highest probability of attack among all available paths to each of her assets.[4]

In the next section, we review certain classes of probability weighting functions that capture human misperception of probabilities. Subsequently, we introduce such functions into the above security game formulation, and study their impact on the investment decisions and equilibria.

2.2 Nonlinear Probability Weighting and the Behavioral Security Game

2.2.1 Nonlinear Probability Weighting

The behavioral economics and psychology literature has shown that humans consistently misperceive probabilities by overweighting low probabilities and underweighting high

[4]↑This also models settings where the specific path taken by the attacker or the attack plan is not known to the defender apriori, and the defender seeks to make the most vulnerable path to each of her assets as secure as possible.

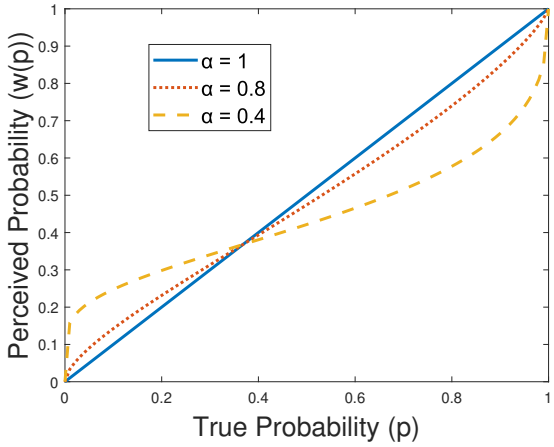


Figure 2.2. Prelec probability weighting function (2.3) which transforms true probabilities p into perceived probabilities $w(p)$. The parameter α controls the extent of overweighting and underweighting.

probabilities [14], [47]. More specifically, humans perceive a "true" probability $p \in [0, 1]$ as $w(p) \in [0, 1]$, where $w(\cdot)$ is a probability weighting function. A commonly studied probability weighting function was proposed by Prelec in [47], and is given by

$$w(p) = \exp\Big[-(-\log(p))^{\alpha}\Big], \quad p \in [0, 1], \tag{2.3}$$

where $\alpha \in (0, 1]$ is a parameter that controls the extent of overweighting and underweighting. When $\alpha = 1$, we have $w(p) = p$ for all $p \in [0, 1]$, which corresponds to the situation where probabilities are perceived correctly. Smaller values of α lead to a greater amount of overweighting and underweighting, as illustrated in Figure 2.2. Next, we incorporate this probability weighting function into the security game defined in the last section, and define the Behavioral Security Game that is the focus of this work.

2.2.2 The Behavioral Security Game

Recall that each defender seeks to protect a set of assets, and the probability of each asset being successfully attacked is determined by the corresponding probabilities on the

edges that constitute the paths from the source node to that asset. This motivates a broad class of games that incorporate probability weighting, as defined below.

Definition 2.2.1. *We define a Behavioral Security Game as a game between different defenders in an interdependent network, where each defender misperceives the attack probability on each edge according to the probability weighting function defined in (2.3).*[5] *Specifically, the perceived attack probability by a defender D_k on an edge $(v_{\mathrm{i}}, v_{\mathrm{j}})$ is given by*

$$w_k(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})) = \exp\Big[-(-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})))^{\alpha_k}\Big], \tag{2.4}$$

where $p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) \in [0,1]$ and $\alpha_k \in (0,1]$.

Remark 1. The subscript k in α_k and $w_k(\cdot)$ allows each defender in the Behavioral Security Game to have a different level of misperception. We will drop the subscript k when it is clear from the context. ■

Incorporating this into the cost function (2.2), each defender D_k seeks to minimize her *perceived expected cost*

$$C_k(x_k, \mathbf{x}_{-k}) = \sum_{v_m \in V_k} L_m \left(\max_{P \in \mathcal{P}_m} \prod_{(v_{\mathrm{i}}, v_{\mathrm{j}}) \in P} w_k\left(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})\right) \right). \tag{2.5}$$

Thus, our formulation complements the existing decision-making models based on vulnerability and cost by incorporating certain behavioral biases in the cost function.

Remark 2. In addition to misperceptions of probabilities, empirical evidence shows that humans perceive costs differently from their true values. In particular, humans (i) compare uncertain outcomes with a reference utility or cost, (ii) exhibit risk aversion in gains and risk seeking behavior in losses, and (iii) overweight losses compared to gains (loss aversion). A richer behavioral model, referred to as cumulative prospect theory [14], incorporates all

[5]↑While existing literature on behavioral aspects of information security, such as [48]–[50] rely on human subject experiments and more abstract decision-making models, we consider the more concrete framework of attack graphs in our analysis. This framework allows for a mapping from existing vulnerabilities to potential attack scenarios. Specifically, one model that is captured by our formulation is to define vulnerabilities by CVE-IDs [51], and assign attack probabilities using the Common Vulnerability Scoring System (CVSS) [42].

these aspects in its cost function. However, in the setting of this chapter, this richer model does not significantly change the cost functions of the defenders. Specifically, the attack on an asset is either successful or it is not. If the reference cost is zero for each asset (i.e., the default state where the asset is not attacked successfully), then successful attack constitutes a loss, and the index of loss aversion only scales the constant L_m by a scalar without changing the dependence of the cost function on the investments. ■

2.2.3 Assumptions on the Probabilities of Successful Attack

The shape of the probability weighting function (2.3) presents several challenges for analysis. In order to maintain analytical tractability, we make the following assumption on the probabilities of successful attack on each edge.

Assumption 1. *For every edge* $(v_{\mathrm{i}}, v_{\mathrm{j}})$*, the probability of successful attack* $p_{\mathrm{i,j}}(x_{\mathrm{i,j}})$ *is log-convex*[6]*, strictly decreasing, and twice continuously differentiable for* $x_{\mathrm{i,j}} \in [0, \infty)$*.*

One particular function satisfying the above conditions is

$$p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) = p^0_{\mathrm{i,j}} \exp(-x_{\mathrm{i,j}}). \tag{2.6}$$

Such probability functions fall within the class commonly considered in security economics (e.g., [25]), and we will specialize our analysis to this class for certain results in that chapter. For such functions, the (true) attack success probability of any given path P from the source to a target v_t is given by

$$\prod_{(v_m,v_n)\in P} p_{m,n}(x_{m,n}) = \left(\prod_{(v_m,v_n)\in P} p^0_{m,n} \right) \exp\left(- \sum_{(v_m,v_n)\in P} x_{m,n} \right). \tag{2.7}$$

Thus, the probability of successful attack on a given path decreases exponentially with the sum of the investments on all edges on that path by all defenders.

[6]↑This is a common assumption in the literature. In particular, [28] shows that log-convexity of the attack probability functions is a necessary and sufficient condition for the optimal security investment result of the seminal paper [25] to hold.

Remark 3. The recent work [9] studied this same class of security games for the case of non-behavioral defenders (i.e., with $\alpha_k = 1, \forall D_k \in \mathcal{D}$). For that case, with probability functions given by (2.6), [9] showed that the optimal investments for each defender can be found by solving a convex optimization problem. Suitable modifications of the same approach to account for the parameter α_k will also work for determining the optimal investments by the behavioral defenders in this work. We omit the details in the interest of space. ■

2.3 Properties of the Optimal Investment Decisions By a Single Defender

We start our analysis of the impact of behavioral decision-making by considering settings with only a single defender (i.e., $|\mathcal{D}| = 1$). In particular, we will establish certain properties of the defender's cost function (2.5), and subsequently identify properties of the defender's optimal investment decisions under behavioral (i.e., $\alpha < 1$) and non-behavioral (i.e., $\alpha = 1$) decision-making. This setting will help in understanding the actions (i.e., best responses) of each player in multi-defender Behavioral Security Games, which we will consider in the next section. In this section, we will refer to the defender as D_k, and drop the vector $\mathbf{x}_{-k}$ from the arguments.

2.3.1 Convexity of the Cost Function

We first establish the convexity of the defender's cost function. To do so, we start with the following result.

Lemma 1. *For $\alpha_k \in (0, 1)$ and $(v_{\mathrm{i}}, v_{\mathrm{j}}) \in \mathcal{E}$, let $h(x_{\mathrm{i,j}}) \triangleq (-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})))^{\alpha_k}$. Then, $h(x_{\mathrm{i,j}})$ is strictly concave in $x_{\mathrm{i,j}}$ for $x_{\mathrm{i,j}} \in [0, \infty)$ under Assumption 1. Moreover, $h(x_{\mathrm{i,j}})$ is concave in $x_{\mathrm{i,j}}$ for $\alpha_k \in (0, 1]$.*

Proof. For ease of notation, we drop the subscripts i, j, and k in the following analysis. First, we focus on the case where $\alpha \in (0, 1)$. Note from Assumption 1 that $0 < p(x) \leq 1$, and so $0 \leq -\log(p(x)) < \infty$ for all $x \in [0, \infty)$.

Now, we prove that $h(x)$ is strictly concave:

$$h(x) = -\alpha(-\log(p(x)))^{\alpha-1}\frac{p(x)}{p(x)}$$
$$h(x) = \alpha(\alpha-1)(-\log(p(x)))^{\alpha-2}\frac{(p(x))^2}{(p(x))^2} + \alpha(-\log(p(x)))^{\alpha-1}\left[\frac{(p(x))^2 - p(x)p(x)}{(p(x))^2}\right].$$

From Assumption 1, $p(x)$ is strictly decreasing and therefore $p(x) < 0$. Thus, the first term on the R.H.S. of $h(x)$ is strictly negative if $\alpha \in (0,1)$. Also, since $p(x)$ is twice-differentiable and log-convex with a convex feasible defense strategy domain $\mathbb{R}_{\geq 0}$, following [52, Subsection 3.5.2], we have $(p(x))^2 \leq p(x)p(x)$, which ensures that the second term is non-positive. Therefore, $h(x)$ is strictly concave.

Finally, if $\alpha = 1$, we have $h(x) = -\log(p(x))$, and since $p(x)$ is log-convex, $h(x)$ is concave. □

Using the above result, we now establish that the defender's cost function (2.5) is convex.

Lemma 2. *For all $\alpha_k \in (0,1]$ and under Assumption 1, the cost function (2.5) of the defender D_k is convex in the defense investment x_k.*

Proof. For each attack path P, define $h_P(x_k) \triangleq \sum_{(v_{\mathrm{i}},v_{\mathrm{j}})\in P} (-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})))^{\alpha_k}$. Then, using the Prelec function in (2.4), the cost in (2.5) is given by

$$C_k(x_k) = \sum_{v_m \in V_k} L_m\Big(\max_{P\in\mathcal{P}_m} \exp(-h_P(x_k))\Big).$$

Note that $h_P(x_k)$ is separable and by Lemma 1, each term in $h_P(x_k)$ is concave in a different variable (i.e., each term corresponds to a different edge $(v_{\mathrm{i}}, v_{\mathrm{j}})$ in the attack path P). Thus, $h_P(x_k)$ is concave in x_k, and so $\exp(-h_P(x_k))$ is convex in x_k. Moreover, the maximum of a set of convex functions is also convex [52, Subsection 3.2.3]. Finally, since $C_k(x_k)$ is a linear combination of convex functions, $C_k(x_k)$ is convex in x_k. □

2.3.2 Uniqueness of Investments

Having established the convexity of the defender's cost function (2.5), we now observe the difference in the investment decisions made by behavioral and non-behavioral defenders. In particular, we first show that the optimal investment decisions by a behavioral defender are unique, and then contrast that with the (generally) non-unique optimal investments for non-behavioral defenders.

Proposition 2.3.1. *Consider an attack graph $G = (V, \mathcal{E})$ and a defender D_k. Assume the probability of successful attack on each edge satisfies Assumption 1 and $\alpha_k \in (0, 1)$ in the probability weighting function (2.4). Then, the optimal investments by defender D_k to minimize (2.5) are unique.*

Proof. Consider the defender's optimization problem for the cost function in (2.5). Denote a path (after investments) to be a "critical path" of an asset if it has the highest probability of successful attack from the source to that asset (note that multiple paths can be critical). The "value" of a path is its probability of successful attack (product of perceived probabilities on each edge in the path).

We claim that in any optimal solution x_k^*, every edge that has a nonzero investment must belong to some critical path. Let (v_a, v_b) be an edge that does not belong to any critical path and suppose by contradiction that x_k^* is an optimal solution of (2.5) in which the edge (v_a, v_b) has a nonzero investment. Now, remove a sufficiently small nonzero investment ϵ from the edge (v_a, v_b) and spread it equally among all of the edges of the critical paths. This reduces the total attack probability on the critical paths and thereby decreases the cost in (2.5), which yields a contradiction. This shows that our claim is true.

Now, suppose that the defender's cost function $C_k(x_k)$ does not have a unique minimizer. Then, there exist two different minimizers x_k^1 and x_k^2. Let $\bar{E} \subseteq \mathcal{E}$ be the set of edges where the investments are different in the two solutions. For each asset $v_m \in V_k$, let $\bar{\mathcal{P}}_m \subseteq \mathcal{P}_m$ be the set of all paths from the source to v_m that pass through at least one edge in $\bar{E}$. Define $x_k^3 = \frac{1}{2}(x_k^1 + x_k^2)$, which must also be an optimal solution of $C_k(x_k)$ (by convexity of $C_k(x_k)$, as established in Lemma 2). Furthermore, a component of x_k^3 is nonzero whenever at least

one of the corresponding components in x_k^1 or x_k^2 is nonzero. In particular, x_k^3 is nonzero on each edge in $\bar{E}$.

For any investment vector x_k, given a path P, we use $x_{k,P}$ to denote the vector of investments on edges on the path P. For each asset $v_m \in V_k$ and path $P \in \mathcal{P}_m$, denote $h_P(x_{k,P}) \triangleq \sum_{(v_\mathrm{i},v_\mathrm{j})\in P} (-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})))^{\alpha_k}$. By Lemma 1, each term of the form $(-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})))^{\alpha_k}$ is strictly concave in $x_{\mathrm{i,j}}$ when $\alpha_k \in (0,1)$. Thus, $h_P(x_{k,P})$ is strictly concave in $x_{k,P}$ for $\alpha_k \in (0,1)$.

Then, using (2.4), the value of the path P is given by

$$f_P(x_{k,P}) \triangleq \prod_{(v_\mathrm{i},v_\mathrm{j})\in P} w_k(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})) = \exp(-h_P(x_{k,P})).$$

Note that by strict concavity of $h_P(x_{k,P})$ in $x_{k,P}$ when $\alpha_k \in (0,1)$, $f_P(x_{k,P})$ is strictly convex in $x_{k,P}$ when $\alpha_k \in (0,1)$. For each asset $v_m \in V_k$, the value of each critical path is

$$\begin{aligned} g_m(x_k) &\triangleq \max_{P\in\mathcal{P}_m} f_P(x_{k,P}) \\ &= \max\left(\max_{P\in\bar{\mathcal{P}}_m} f_P(x_{k,P}), \max_{P\in\mathcal{P}_m\setminus\bar{\mathcal{P}}_m} f_P(x_{k,P})\right). \end{aligned}$$

Now, returning to the optimal investment vector x_k^3, define

$$\hat{M} \triangleq \{v_m \in V_k | \max_{P\in\bar{\mathcal{P}}_m} f_P(x_{k,P}^3) \geq \max_{P\in\mathcal{P}_m\setminus\bar{\mathcal{P}}_m} f_P(x_{k,P}^3)\}.$$

In other words, $\hat{M}$ is the set of assets for which there is a critical path (under the investment vector x_k^3) that passes through the set $\bar{E}$ (where the optimal investments x_k^1 and x_k^2 differ). Now there are two cases. The first case is when $\hat{M}$ is nonempty. We have (from (2.5))

$$\begin{aligned} C_k(x_k^3) &= \sum_{v_m\notin\hat{M}} L_m\, g_m(x_k^3) + \sum_{v_m\in\hat{M}} L_m\, g_m(x_k^3) \\ &\overset{(a)}{=} \sum_{v_m\notin\hat{M}} L_m \max_{P\in\mathcal{P}_m\setminus\bar{\mathcal{P}}_m} f_P(x_{k,P}^3) + \sum_{v_m\in\hat{M}} L_m \max_{P\in\bar{\mathcal{P}}_m} f_P(x_{k,P}^3) \\ &\overset{(b)}{<} \sum_{v_m\notin\hat{M}} L_m \frac{1}{2} \max_{P\in\mathcal{P}_m\setminus\bar{\mathcal{P}}_m} (f_P(x_{k,P}^1) + f_P(x_{k,P}^2)) + \sum_{v_m\in\hat{M}} L_m \frac{1}{2} \max_{P\in\bar{\mathcal{P}}_m} (f_P(x_{k,P}^1) + f_P(x_{k,P}^2)) \end{aligned}$$

$$
\begin{aligned}
&\overset{(c)}{\leq} \sum_{v_m \notin \hat{M}} L_m \, \frac{1}{2} \max_{P \in \mathcal{P}_m} \left(f_P(x^1_{k,P}) + f_P(x^2_{k,P}) \right) + \sum_{v_m \in \hat{M}} L_m \, \frac{1}{2} \max_{P \in \mathcal{P}_m} \left(f_P(x^1_{k,P}) + f_P(x^2_{k,P}) \right) \\
&\overset{(d)}{\leq} \frac{1}{2} \sum_{v_m \notin \hat{M}} L_m \left(\max_{P \in \mathcal{P}_m} f_P(x^1_{k,P}) + \max_{P \in \mathcal{P}_m} f_P(x^2_{k,P}) \right) + \frac{1}{2} \sum_{v_m \in \hat{M}} L_m \left(\max_{P \in \mathcal{P}_m} f_P(x^1_{k,P}) + \max_{P \in \mathcal{P}_m} f_P(x^2_{k,P}) \right) \\
&= \frac{1}{2} \left(\sum_{v_m \in V_k} L_m \, g_m(x^1_k) + \sum_{v_m \in V_k} L_m \, g_m(x^2_k) \right).
\end{aligned}
$$

Note that (a) holds from the definition of $\hat{M}$. Also, (b) holds since for each $P \in \bar{\mathcal{P}}_m$, $f_P(x^3_{k,P}) < \frac{1}{2}(f_P(x^1_{k,P}) + f_P(x^2_{k,P}))$ by strict convexity of f_P in $x_{k,P}$ and since $x^3_{k,P}$ is a strict convex combination of $x^1_{k,P}$ and $x^2_{k,P}$ (by definition of $\bar{\mathcal{P}}_m$). Thus, for $v_m \in \hat{M}$, $\max_{P \in \bar{\mathcal{P}}_m} f_P(x^3_{k,P}) < \max_{P \in \bar{\mathcal{P}}_m} \frac{1}{2}(f_P(x^1_{k,P}) + f_P(x^2_{k,P}))$. Further, (c) holds since the maximum over a subset of the paths ($\bar{\mathcal{P}}_m$ or $\mathcal{P}_m \setminus \bar{\mathcal{P}}_m$) is less than or equal the maximum over the set of all paths $\mathcal{P}_m$. Finally, (d) holds as the maximum of a sum of elements is at most the sum of maxima. Thus, $C_k(x^3_k) < \frac{1}{2}(C_k(x^1_k) + C_k(x^2_k))$ which yields a contradiction to the optimality of x^1_k and x^2_k.

In the second case, suppose $\hat{M}$ is empty. Thus, $\forall v_m \in V_k$, $\max_{P \in \bar{\mathcal{P}}_m} f_P(x^3_{k,P}) < \max_{P \in \mathcal{P}_m \setminus \bar{\mathcal{P}}_m} f_P(x^3_{k,P})$. In other words, for all assets $v_m \in V_k$, no critical paths go through the edge set $\bar{E}$ (since $\bar{\mathcal{P}}_m$ contains all such paths). However, x^3_k has nonzero investments on edges in $\bar{E}$. Thus, x^3_k cannot be an optimal solution (by the claim at the start of the proof). Thus, the second case is also not possible. Hence there cannot be two different optimal solutions, and therefore the optimal investments for the defender D_k are unique. □

In contrast to the above result, the optimal investments by a non-behavioral defender (i.e., $\alpha = 1$) need not be unique. To see this, consider an attack graph where the probability of successful attack on each edge is given by the exponential function (2.6). As argued in equation (2.7), the probability of successful attack on any given path is a function of the *sum* of the security investments on *all* the edges in that path. Thus, given an optimal set of investments by a non-behavioral defender, any other set of investments that maintains the same total investment on each path of the graph is also optimal.

2.3.3 Locations of Optimal Investments for Behavioral and Non-Behavioral Defenders

We next study differences in the *locations* of the optimal investments by behavioral and non-behavioral defenders. In particular, we first characterize the optimal investments by a non-behavioral defender who is protecting a single asset, and subsequently compare that to the investments made by a behavioral defender. In the following result, we use the notion of a *min-cut* in the graph. Specifically, given two nodes s and t in the graph, an edge-cut is a set of edges $\mathcal{E}_c \subset \mathcal{E}$ such that removing $\mathcal{E}_c$ from the graph also removes all paths from s to t. A min-cut is an edge-cut of smallest cardinality over all possible edge-cuts [53].

Proposition 2.3.2. *Consider an attack graph $G = (V, \mathcal{E})$. Let the attack success probability under security investments be given by $p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) = \mathrm{e}^{-x_{\mathrm{i,j}}}$, where $x_{\mathrm{i,j}} \in \mathbb{R}_{\geq 0}$ is the investment on edge $(v_{\mathrm{i}}, v_{\mathrm{j}})$. Suppose there is a single target asset v_t (i.e., all other assets have loss 0). Let $\mathcal{E}_c \subseteq \mathcal{E}$ be a min-cut between the source node v_s and the target v_t. Then, it is optimal for a non-behavioral defender D_k to distribute all her investments equally only on the edge set $\mathcal{E}_c$ in order to minimize (2.2).*

Proof. Let $N = |\mathcal{E}_c|$ represent the number of edges in the min-cut set $\mathcal{E}_c$. Let B be the defender's budget.

Consider any optimal investment of that budget. Recall from (2.7) that for probability functions of the form (2.6), the probability of a successful attack of the target along a certain path P is a decreasing function of the sum of the investments on the edges on that path. Using Menger's theorem [53], there are N edge-disjoint paths between v_s and v_t in G. At least one of those paths has total investment at most $\frac{B}{N}$. Therefore, the path with highest probability of attack from v_s to v_t has total investment at most $\frac{B}{N}$.

Now consider investing $\frac{B}{N}$ on each edge in the min-cut. Since every path from v_s to v_t goes through at least one edge in $\mathcal{E}_c$, every path has at least $\frac{B}{N}$ in total investment. Thus, it is optimal to only invest on edges in $\mathcal{E}_c$.

Finally, consider investing non-equally on edges in $\mathcal{E}_c$ where an edge $(v_{\mathrm{i}}, v_{\mathrm{j}}) \in \mathcal{E}_c$ has investment $x_{\mathrm{i,j}} < \frac{B}{N}$. Under this investment, since there are N edge-disjoint paths from v_s to v_t in G, there exists a path P from v_s to v_t that has total investment less than $\frac{B}{N}$. Thus, the

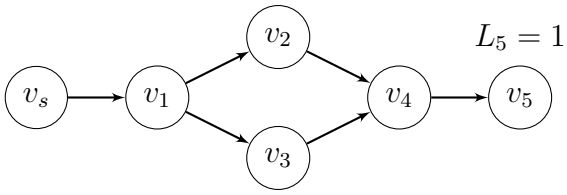


Figure 2.3. An attack graph where a behavioral defender makes suboptimal investment decisions.

path with the highest probability of attack has a probability of attack larger than $\exp\left(-\frac{B}{N}\right)$ (which would be obtained when investing $\frac{B}{N}$ equally on each edge in $\mathcal{E}_c$). Therefore, the true expected cost in (2.2) is higher with this non-equal investment. Thus, the optimal investment on $\mathcal{E}_c$ must contain $\frac{B}{N}$ investment on each edge in $\mathcal{E}_c$. □

Remark 4. The above result will continue to hold for more general probability functions $p_{m,n}(x_{m,n}) = p^0_{m,n}\mathrm{e}^{-x_{m,n}}$ with $p^0_{m,n} \neq 1$ if $\prod_{(v_m,v_n)\in P} p^0_{m,n}$ is the same for every path $P \in \mathcal{P}_t$. The baseline successful attack probability is then the same along every path to v_t, and thus optimal investments can be restricted to the edges in the min-cut set. ■

The conclusion of Proposition 2.3.2 no longer holds when we consider the investments by a behavioral defender (i.e., with $\alpha_k < 1$), as illustrated by the following example.

Example 1. *Consider the attack graph shown in Figure 2.3, with a single defender D (we will drop the subscript k for ease of notation in this example) and a single target asset v_5 with a loss of $L_5 = 1$ if successfully attacked. Let the defender's budget be B, and let the probability of successful attack on each edge $(v_\mathrm{i}, v_\mathrm{j})$ be given by $p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) = \mathrm{e}^{-x_{\mathrm{i,j}}}$, where $x_{\mathrm{i,j}}$ is the investment on that edge. This graph has two possible min-cuts, both of size 1: the edge (v_s, v_1), and the edge (v_4, v_5). Thus, by Proposition 2.3.2, it is optimal for a non-behavioral defender to put all of her budget on either one of these edges.*

Now consider a behavioral defender with $\alpha < 1$. With the above expression for $p_{\mathrm{i,j}}(x_{\mathrm{i,j}})$ and using the Prelec function (2.4), we have $w(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})) = \mathrm{e}^{-x^\alpha_{\mathrm{i,j}}}$. Thus, the perceived expected cost function (2.5) is given by

$$C(\mathbf{x}) = \max\left(\mathrm{e}^{-x^\alpha_{s,1}-x^\alpha_{1,2}-x^\alpha_{2,4}-x^\alpha_{4,5}}, \mathrm{e}^{-x^\alpha_{s,1}-x^\alpha_{1,3}-x^\alpha_{3,4}-x^\alpha_{4,5}}\right),$$

corresponding to the two paths from the source v_s to the target v_t. One can verify (using the KKT conditions) that the optimal investments are given by

$$\begin{aligned} x_{1,2} = x_{2,4} = x_{1,3} = x_{3,4} &= 2^{\frac{1}{\alpha-1}} x_{s,1} \ , \\ x_{4,5} = x_{s,1} = \frac{B - 4x_{1,2}}{2} &= \frac{B}{2 + 4(2^{\frac{1}{\alpha-1}})} \ . \end{aligned} \tag{2.8}$$

Thus, for the true expected cost function (2.2), the optimal investments (corresponding to the non-behavioral defender) yield a true expected cost of e^{-B}, whereas the investments of the behavioral defender yield a true expected cost of $\mathrm{e}^{-2^{\frac{\alpha}{\alpha-1}}} \mathrm{e}^{-\frac{B}{1+2^{\frac{\alpha}{\alpha-1}}}}$, which is larger than that of the non-behavioral defender.

The above example illustrates a key phenomenon: as the defender's perception of probabilities becomes increasingly skewed (captured by α becoming smaller), she shifts more of her investments from the min-cut edges to the edges on the parallel paths between v_1 and v_4. This is in contrast to the optimal investments (made by the non-behavioral defender) which lie entirely on the min-cut edges. Indeed, by taking the limit as $\alpha \uparrow 1$, we have

$$x_{\mathrm{i,j}} = \lim_{\alpha \uparrow 1} 2^{\frac{1}{\alpha-1}} \, x_{s,1} = 2^{-\infty} \, x_{s,1} = 0$$

for edges $(v_{\mathrm{i}}, v_{\mathrm{j}})$ on the two parallel portions of the graph.

We now use this insight to identify graphs where the behavioral defender finds that investing only on the min-cut edges is not optimal.

Proposition 2.3.3. *Consider an attack graph G with a source v_s and a target v_t. Let $\mathcal{E}_c$ be a min-cut between v_s and v_t, with size $|\mathcal{E}_c| = N$. Suppose the graph contains another edge cut $\mathcal{E}_c$ such that $\mathcal{E}_c \cap \mathcal{E}_c = \emptyset$ and $|\mathcal{E}_c| > |\mathcal{E}_c|$. Let the probability of successful attack on each edge $(v_{\mathrm{i}}, v_{\mathrm{j}}) \in \mathcal{E}$ be given by $p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) = \mathrm{e}^{-x_{\mathrm{i,j}}}$, where $x_{\mathrm{i,j}}$ is the investment on that edge. Let B be the budget of the defender. Then, if $0 < \alpha_k < 1$, investing solely on the min-cut set $\mathcal{E}_c$ is not optimal from the perspective of a behavioral defender.*

Proof. Denote $M = |\mathcal{E}_c| > |\mathcal{E}_c| = N$. By Proposition 2.3.2, it is optimal to invest the entire budget uniformly on edges in $\mathcal{E}_c$ in order to minimize the cost function (2.2). We will show

that this investment is not optimal with respect to the behavioral defender's cost function (2.5); we will drop the subscript k in α_k for ease of notation.

Starting with the optimal investments on the min edge cut $\mathcal{E}_c$ where each edge in $\mathcal{E}_c$ has nonzero investment (as given by Proposition 2.3.2), remove a small investment ϵ from each of those N edges, and add an investment of $\frac{N\epsilon}{M}$ to each of the edges in $\mathcal{E}_c$. We show that when ϵ is sufficiently small, this will lead to a net reduction in perceived probability of successful attack on each path from v_s to v_t.

Consider any arbitrary path P from v_s to v_t. Starting with the investments only on the minimum edge cut $\mathcal{E}_c$, the perceived probability of successful attack on path P will be

$$f_1(\mathbf{x}) \triangleq \exp\Big(- \sum_{\substack{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_c,\\ (v_\mathrm{i},v_\mathrm{j})\in P}} x_{\mathrm{i,j}}^{\alpha}\Big).$$

After removing ϵ investment from each of the N edges in $\mathcal{E}_c$, and adding an investment of $\frac{N\epsilon}{M}$ to each of the edges in $\mathcal{E}_c$, the perceived probability on path P will be:

$$f_2(\mathbf{x}) \triangleq \exp\Big(- \sum_{\substack{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_c,\\ (v_\mathrm{i},v_\mathrm{j})\in P}} \Big(\frac{N\epsilon}{M}\Big)^{\alpha} - \sum_{\substack{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_c,\\ (v_\mathrm{i},v_\mathrm{j})\in P}} (x_{\mathrm{i,j}}-\epsilon)^{\alpha}\Big).$$

The net reduction in perceived probability on path P will be positive if $f_2(\mathbf{x}) < f_1(\mathbf{x})$, i.e.,

$$\sum_{\substack{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_c,\\ (v_\mathrm{i},v_\mathrm{j})\in P}} \Big(\frac{N\epsilon}{M}\Big)^{\alpha} + \sum_{\substack{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_c,\\ (v_\mathrm{i},v_\mathrm{j})\in P}} (x_{\mathrm{i,j}}-\epsilon)^{\alpha} > \sum_{\substack{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_c,\\ (v_\mathrm{i},v_\mathrm{j})\in P}} x_{\mathrm{i,j}}^{\alpha}. \tag{2.9}$$

If we define

$$f(\epsilon) \triangleq \sum_{\substack{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_c,\\ (v_\mathrm{i},v_\mathrm{j})\in P}} \Big(\frac{N\epsilon}{M}\Big)^{\alpha} + \sum_{\substack{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_c,\\ (v_\mathrm{i},v_\mathrm{j})\in P}} (x_{\mathrm{i,j}}-\epsilon)^{\alpha},$$

we see that inequality (2.9) is equivalent to showing that $f(\epsilon) > f(0)$. We have

$$\frac{df}{d\epsilon} = \frac{\alpha N}{M} \sum_{\substack{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_c,\\ (v_\mathrm{i},v_\mathrm{j})\in P}} \Big(\frac{N\epsilon}{M}\Big)^{\alpha-1} - \alpha \sum_{\substack{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_c,\\ (v_\mathrm{i},v_\mathrm{j})\in P}} (x_{\mathrm{i,j}}-\epsilon)^{\alpha-1}.$$

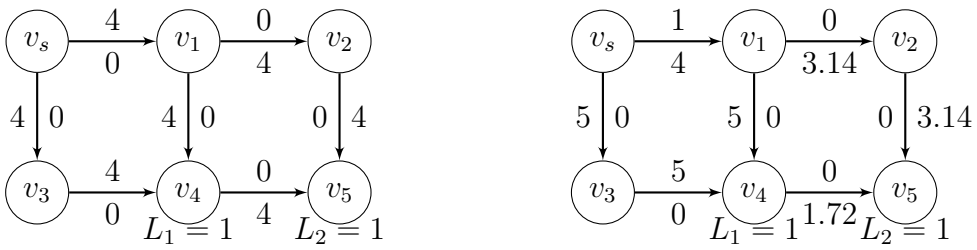


Figure 2.4. An instance of a Behavioral Security Game with multiple PNE. Defenders D_1 and D_2 are behavioral decision-makers with $\alpha_1 = \alpha_2 = 0.5$. The numbers above/left and below/right of the edges represent investments by D_1 and D_2, respectively.

Note that $\lim_{\epsilon \downarrow 0} \frac{df}{d\epsilon} = \infty$ which shows that $f(\epsilon)$ is increasing in ϵ for sufficiently small ϵ. Therefore, $f_2(\mathbf{x}) < f_1(\mathbf{x})$ for sufficiently small ϵ. Since this analysis holds for every path from v_s to v_t, this investment profile outperforms investing purely on the minimum edge cut. □

Note that the graph in Figure 2.3 satisfies the conditions in the above result, with $\mathcal{E}_c = (v_4, v_5)$, $\mathcal{E}_c = \{(v_1, v_2), (v_1, v_3)\}$.

Having established properties of the optimal investment decisions for behavioral and non-behavioral defenders, we next turn our attention to the Behavioral Security Game with multiple defenders, introduced in Section 2.2.

2.4 Analysis of Multi-Defender Games

2.4.1 Existence of a PNE

We first establish the existence of a Pure Strategy Nash Equilibrium (PNE) for the class of behavioral games defined in Section 2.2. Recall that 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 investment.

Proposition 2.4.1. *Under Assumption 1, the Behavioral Security Game possesses a pure strategy Nash equilibrium (PNE) when $\alpha_k \in (0, 1]$ for each defender D_k.*

Proof. The feasible defense strategy space X_k in (2.1) 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 $C(x_k, \mathbf{x}_{-k})$ in (2.5) is convex in $x_k \in X_k$; this follows from Lemma 2 and the fact that the investment $x_{\mathrm{i,j}}$ on each edge is a sum of the investments of all players on that edge. As a result, the Behavioral Security Game is an instance of a *concave game*, which always has a PNE [54]. □

Note that in contrast to the best responses by each player (which were unique when $\alpha_k \in (0, 1)$, as shown in Proposition 2.3.1), the PNE of Behavioral Security Games is not unique in general. We illustrate this through the following example.

Example 2. *Consider the attack graph of Figure 2.4. There are two defenders, D_1 and D_2, where defender D_1 wishes to protect node v_4, and defender D_2 wishes to protect node v_5. Suppose that D_1 has a budget $B_1 = 16$ and D_2 has $B_2 = 12$. Figs. 2.4a and 2.4b illustrate two distinct PNE for this game. We obtained multiple Nash equilibria by varying the starting investment decision of defender D_1 and then following best response dynamics until the investments converged to an equilibrium.*

It is interesting to note that these two Nash equilibria lead to different costs for the defenders. First, for the Nash equilibrium of Figure 2.4a, defender D_1's perceived expected cost, given by (2.5), is equal to $\exp(-4)$, while her true expected cost, given by (2.2), is equal to $\exp(-8)$. Defender D_2 has a perceived expected cost of $\exp(-6)$, and a true expected cost of $\exp(-12)$. In contrast, for the Nash equilibrium in Figure 2.4b, defender D_1 has a perceived expected cost of $\exp\left(-2\sqrt{5}\right)$ and a true expected cost of $\exp(-10)$. Defender D_2 has a perceived expected cost of $\exp(-5.78)$ and a true expected cost of $\exp(-11.28)$.

As a result, the equilibrium in Figure 2.4a is preferred by defender D_2, while the equilibrium in Figure 2.4b has a lower expected cost (both perceived and real) for defender D_1. Note also that the total expected cost (i.e., sum of the true expected costs of defenders D_1 and D_2) is lower in the equilibrium in Figure 2.4b; that is, the PNE of Figure 2.4b would be preferred from a social planner's perspective.

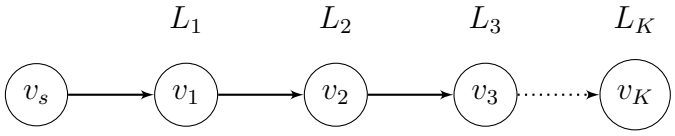


Figure 2.5. An attack graph where PoBA is lower bounded by $(1-\epsilon)\exp(B)$.

2.4.2 Measuring the Inefficiency of PNE: The Price of Behavioral Anarchy

The notion of Price of Anarchy (PoA) is often used to quantify the inefficiency of Nash equilibrium compared to the socially optimal outcome [55]. Specifically, the Price of Anarchy is defined as the ratio of the highest total system cost at a PNE to the total system cost at the social optimum. For our setting, we seek to define a measure to capture the inefficiencies of the equilibrium due to both the defenders' individual strategic behavior and their behavioral decision-making. We thus define the Price of Behavioral Anarchy (PoBA) as the ratio of total system true expected cost of behavioral defenders at the worst PNE (i.e., the PNE with the largest total true expected cost over all PNE), to the total system true expected cost at the social optimum (computed by a non-behavioral social planner).[7]

Specifically, we define $\hat{C}(\mathbf{x}) \triangleq \sum_{D_k \in \mathcal{D}} \hat{C}_k(\mathbf{x})$, where $\hat{C}_k$ (defined in (2.2)) is the true expected cost faced by defender D_k under the investment vector $\mathbf{x}$. Let $X^{\texttt{NE}} := \{\bar{\mathbf{x}} \in \mathbb{R}_{\geq 0}^{|\mathcal{D}||\mathcal{E}|} | \bar{x}_k \in \operatorname{argmin}_{x \in X_k} C_k(x, \bar{\mathbf{x}}_{-k}), \forall D_k \in \mathcal{D}\}$, i.e., $X^{\texttt{NE}}$ is the set of all investments that constitute a PNE. We now define the Price of Behavioral Anarchy as

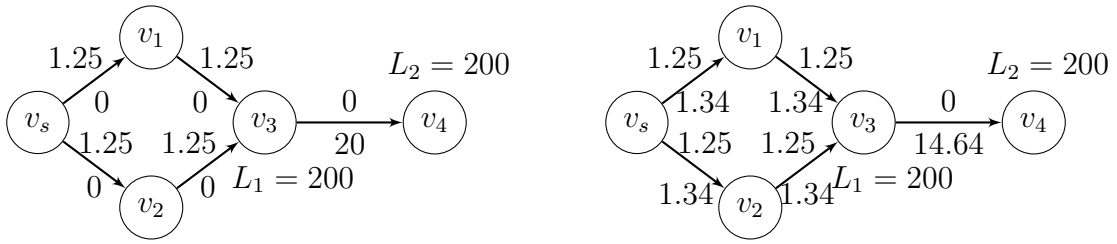
$$PoBA = \frac{\sup_{\bar{\mathbf{x}} \in X^{\texttt{NE}}} \hat{C}(\bar{\mathbf{x}})}{\hat{C}(\mathbf{x}^*)}, \tag{2.10}$$

where $\mathbf{x}^*$ 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 $X^{\texttt{Soc}} := \{\mathbf{x}^* \in \mathbb{R}_{\geq 0}^{|\mathcal{D}||\mathcal{E}|} | \mathbf{1}^T \mathbf{x}^* \leq \sum_{D_k \in \mathcal{D}} B_k\}$, i.e., $X^{\texttt{Soc}}$ is the set of all feasible investments by the social planner, and $\mathbf{x}^* \in \operatorname{argmin}_{\mathbf{x} \in X^{\texttt{Soc}}} \hat{C}(\mathbf{x})$. When $\bar{\mathbf{x}}$ is any PNE, but not necessarily the one with the worst social cost, we refer to the ratio of $\hat{C}(\bar{\mathbf{x}})$ and $\hat{C}(\mathbf{x}^*)$ as the "inefficiency" of the

[7] ↑One could also consider the impact of a behavioral social planner; since the goal of our work is to quantify the (objective) inefficiencies due to behavioral decision-making, we leave the study of a behavioral social planner for future work.

equilibrium. We emphasize that the costs in both the numerator and the denominator are the sum of the *true* (rather than perceived) expected costs of the defenders.

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



(a) $\alpha_1 = 1$, $\alpha_2 = 1$ (b) $\alpha_1 = 1, \alpha_2 = 0.6$

Figure 2.6. The numbers above (below) each edge represent investments by defender D_1 (D_2). In (a), the non-behavioral defender D_1 does not receive any investment contributions from the non-behavioral defender D_2. In (b), the non-behavioral defender D_1 benefits from the investment contributions of the behavioral defender D_2.

Proposition 2.4.2. *Let the sum of the budgets available to all defenders be B, and let the probability of successful attack on each edge $(v_{\mathrm{i}}, v_{\mathrm{j}}) \in \mathcal{E}$ be given by $p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) = \mathrm{e}^{-x_{\mathrm{i,j}}}$. Then, for any attack graph and any profile of behavioral levels $\{\alpha_k\}$, $PoBA \leq \exp(B)$.*

Proof. We start with the numerator of the PoBA in (2.10) (the total true expected cost at the worst PNE). Recall that each defender D_k incurs a loss L_m for each compromised asset v_m. Thus, the worst case true expected cost under any PNE (including the worst PNE) is upper bounded by $\sum_{D_k \in \mathcal{D}} \sum_{v_m \in V_k} L_m$ (i.e., the sum of losses of all assets). On the other hand, the denominator (the socially optimal 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 its attack path). Substituting these bounds into (2.10), we obtain $PoBA \leq \exp(B)$. □

Next, we show that the upper bound on PoBA obtained in Proposition 2.4.2 is asymptotically tight.

Proposition 2.4.3. *For all $B > 0$ and $\epsilon > 0$, there exists an instance of the Behavioral Security Game with total budget B such that the PoBA is lower bounded by $(1-\epsilon)\exp(B)$.*

Proof. Consider the attack graph in Figure 2.5, where the probability of successful attack on each edge $(v_{\mathrm{i}}, v_{\mathrm{j}})$ is given by (2.6) with $p^0_{\mathrm{i,j}} = 1$. 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 defenders (i.e., each defender 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 link (v_s, v_1), so that all nodes have probability of successful attack given by $\exp(-B)$. Thus, the denominator of (2.10) is $\sum_{\mathrm{i}=1}^{K} L_{\mathrm{i}} \exp(-B) = (K+1)\exp(-B)$.

We now characterize a lower bound on the cost under a PNE (i.e., the numerator of (2.10)). 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 (2.5). Thus, D_2's optimization problem, given D_1's investment, is

$$\underset{x^2_{s,1}+x^2_{1,2}=\frac{B}{K}}{\text{minimize}} \quad \mathrm{e}^{-\left(\frac{B}{K}+x^2_{s,1}\right)^{\alpha_2}-\left(x^2_{1,2}\right)^{\alpha_2}}. \tag{2.11}$$

The unique optimal solution of (2.11) (for all $\alpha_2 \in (0,1)$) would be to put all $\frac{B}{K}$ into $x^2_{1,2}$ and zero on $x^2_{s,1}$. This is also optimal (but not unique) when $\alpha_2 = 1$.

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 PoBA under this PNE is lower bounded by $L_1 \exp\left(-\frac{B}{K}\right) = K \exp\left(-\frac{B}{K}\right)$. Thus, the PoBA is lower bounded by

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

As the length of the chain 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 PoBA in the line graph with K nodes is lower bounded by $(1-\epsilon)\exp(B)$. □

Remark 5. The upper bound obtained in Proposition 2.4.2 is agnostic to the structure of the network, the number of defenders, and their degree of misperception of probabilities. In Proposition 2.4.3, our result shows that the upper bound obtained in Proposition 2.4.2 is sharp (i.e., it cannot be reduced without additional assumptions on the game). For any particular instance of the problem, however, we can compute the inefficiency directly, which will depend on the network structure and other parameters of that instance. ■

Before considering the case study, we will conclude this section with an example of an interesting phenomenon, where the (objectively) suboptimal investment decisions made by a behavioral defender with respect to their own assets can actually benefit the other defenders in the network.

Example 3. *We consider the attack graph of Figures 2.6a and 2.6b with two defenders, D_1 and D_2. Defender D_1 wishes to protect node v_3, and defender D_2 wishes to protect node v_4. Note that D_1's asset (v_3) is directly on the attack path to D_2's asset (v_4). Suppose that defender D_1 has a budget $B_1 = 5$, while defender D_2 has a budget $B_2 = 20$. The optimal investments in the following scenarios were calculated using CVX [56].*

Suppose both defenders are non-behavioral. In this case, Proposition 2.3.2 suggests that it is optimal for D_2 to put her entire budget on the min-cut, given by the edge (v_3, v_4). The corresponding PNE is shown in Figure 2.6a. On the other hand, as indicated by Proposition 2.3.3, investing solely on the min-cut is no longer optimal for a behavioral defender. Indeed, Figure 2.6b shows a PNE for the case where D_2 is behavioral with $\alpha_2 = 0.6$,

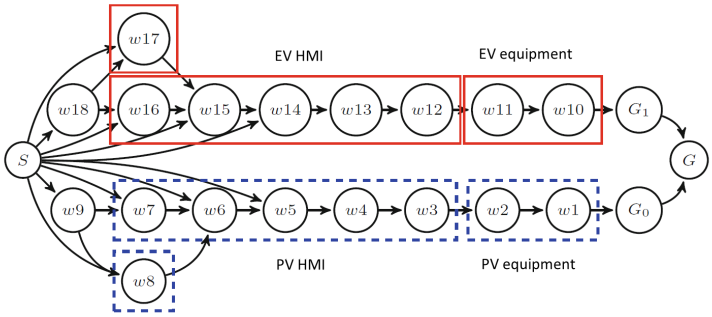


Figure 2.7. Attack graph of a DER.1 failure scenario [17]. It shows stepping-stone attack steps that can lead to the compromise of a photovoltaic generator (PV) (i.e., G_0) or an electric vehicle charging station (EV) (i.e., G_1).

and has spread some of her investment to the other edges in the attack graph. Therefore, D_1's subnetwork will benefit due to the behavioral decision-making by D_2.

It is also worth considering the total system true expected cost of the game at equilibrium, given by $\hat{C}(\bar{\mathbf{x}}) = \hat{C}_1(\bar{\mathbf{x}}) + \hat{C}_2(\bar{\mathbf{x}})$ where $\bar{\mathbf{x}}$ is the investment at the PNE. For this example, when both defenders are non-behavioral (i.e., $\alpha_1 = \alpha_2 = 1$), $\hat{C}(\bar{\mathbf{x}}) = 16.42$, while $\hat{C}(\bar{\mathbf{x}}) = 1.13$ if defender D_2 is behavioral (with $\alpha_1 = 1, \alpha_2 = 0.6$). This considerable drop in the total true expected cost shows that the behavioral defender's contributions to the non-behavioral defender's subnetwork may also be beneficial to the overall welfare of the network, especially under budget asymmetries or if defender D_1's asset is more valuable.

2.5 Case Study

Here, we examine the outcomes of behavioral decision-making in a case study involving a distributed energy resource failure scenario, DER.1, identified by the US National Electric Sector Cybersecurity Organization Resource (NESCOR) [17]. Figure 2.7 is replicated from the attack graph for the DER.1 (Figure 4 in [17]). Suppose the probability of successful attack on each edge is $p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) = \mathrm{e}^{-x_{\mathrm{i,j}}}$. There are two defenders, D_1 and D_2. Defender D_1's critical assets are G_0 and G, with losses of $L_0 = 200$ and $L = 100$, respectively. Defender D_2's critical assets are G_1 and G, also with losses of $L_1 = 200$ and $L = 100$, respectively. Note that G is a shared asset among the two defenders.

We assume that each defender has a security budget of $\frac{B}{2}$ (i.e., the budget distribution is symmetric between the two defenders). For a fair comparison, the social planner has total budget B. In our experiments, we use best response dynamics to find a Nash equilibrium $\bar{\mathbf{x}}$. We then compute the socially optimal investment $\mathbf{x}^*$, and calculate the ratio given by (2.10) to measure the inefficiency of the corresponding equilibrium.

Figure 2.8 shows the value of this ratio as we sweep α (taken to be the same for both defenders) from 0 (most behavioral) to 1 (non-behavioral), for different values of the total budget B. As the figure shows, the inefficiency of the equilibrium decreases to 1 as α increases, reflecting the fact that the investment decisions become better as the defenders become less behavioral; see Section 2.3. Furthermore, Figure 2.8 shows that the inefficiency due to behavioral decision-making becomes exacerbated as the total budget B increases. This happens as behavioral defenders shift higher amounts of their budget to the parallel edges in the networks (i.e., not in the min-cut edge set), as suggested by Proposition 2.3.3. On the other hand, the social planner can significantly lower the total cost when the budget increases, as she puts all the budget only on the min-cut edges, as suggested by Proposition 2.3.2; this reduces the total cost faster towards zero as the budget increases.

Our results may be applicable to other practical scenarios (such as deploying moving-target defense) [9]. While the inefficiency strictly increased with the budget in the above case study, this phenomenon may not occur in all networks. We omit further discussions about these aspects in the interest of space.

2.6 Summary of Findings

In this chapter, I presented an analysis of the impacts of behavioral decision-making on the security of interdependent systems. First, I showed that the optimal investments by a behavioral decision-maker will be unique, whereas non-behavioral decision-makers may have multiple optimal solutions. Second, non-behavioral decision-makers find it optimal to concentrate their security investments on minimum edge-cuts in the network in order to protect their assets, whereas behavioral decision-makers will choose to spread their

[9]Recall that the inefficiency of a particular PNE is the ratio of the total system true expected cost at that PNE to the total system true expected cost at the (non-behavioral) social optimum.

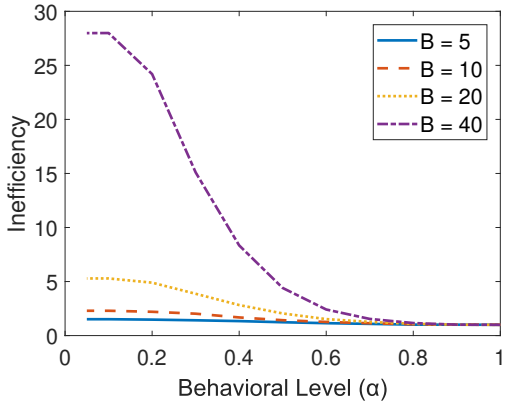


Figure 2.8. The inefficiency for different behavioral levels of the defenders. We observe that the inefficiency increases as the security budget increases, and as the defenders become more behavioral.[9]

investments over other edges in the network, potentially making their assets more vulnerable. Third, I showed that multi-defender games possess a PNE (under appropriate conditions on the game), and introduced a metric that I termed the "Price of Behavioral Anarchy" to quantify the inefficiency of the (behavioral) PNE as compared to the security outcomes under socially optimal investments. I provided a tight bound on PoBA, which depended only on the total budget across all defenders. However, I also showed that the tendency of behavioral defenders to spread their investments over the edges of the network can potentially benefit the other defenders in the network. Finally, I presented a case study where the inefficiency of the equilibrium increased as the defenders became more behavioral.

Overall, my analysis shows that human decision-making (captured by behavioral probability weighting) can have substantial impacts on the security of interdependent systems, and must be accounted for when designing and operating distributed, interdependent systems. The insights that are provided by my work (e.g., that behavioral decision-makers may move some of their security investments away from critical portions of the network) can be used by system planners to identify portions of their network that may be left vulnerable by the human security personnel who are responsible for managing those parts of the network. A future avenue for research is studying the properties of security investments when different edges have different degrees of misperception of attack probabilities.

3. Protecting Assets with Heterogeneous Valuations under Behavioral Probability Weighting

In this chapter, we consider a security setting involving a defender who is required to invest (subject to a budget constraint) in protecting a given set of nodes against attacks. Each node has a certain value to the defender, along with a probability of being successfully compromised, which is a function of the investment in that node by the defender. In this setting, we consider the impacts of behavioral probability weighting (vis-*à*-vis the probability of successful attack) on the investment strategies; such probability weighting, where humans overweight low probabilities and underweight high probabilities, has been identified by behavioral economists to be a common feature of human decision-making. We show that under appropriate conditions on the probability of successful attack, the defender's optimization problem is convex (even under probability weighting). Furthermore, we show that behavioral probability weighting causes the defender to shift more of her investments to the higher-valued nodes and underinvest in the low-value nodes, compared to the case where the defender perceives the probability of attack correctly. In particular, the number of nodes that have positive investment decreases as the defender becomes more behavioral.

3.1 The Multi-Target Security Problem

3.1.1 Strategic Defender

Let $\mathcal{D}$ be a defender who is responsible for defending a set $V = \{v_1, v_2, \ldots, v_n\}$ of assets. For each compromised asset $v_m \in V$, defender $\mathcal{D}$ will incur a financial loss $L_m \in \mathbb{R}_{>0}$. To reduce the attack success probabilities on assets, the defender can allocate security resources on these assets, subject to the constraints described below.

Let $n = |V|$. We assume that defender $\mathcal{D}$ has a security budget $B \in \mathbb{R}_{>0}$. Thus, we define the defense strategy space of the defender by

$$X \triangleq \{\mathbf{x} \in \mathbb{R}^n_{\geq 0} : \sum_{v_{\mathrm{i}} \in V} x_{\mathrm{i}} \leq B\}. \tag{3.1}$$

In words, the defense strategy space for defender $\mathcal{D}$ consists of all non-negative investments on assets such that the sum of all investments does not exceed the budget B. We denote any particular vector of investments by defender $\mathcal{D}$ by $\mathbf{x} \in X$.

3.1.2 Defender's Cost

The investments made by the defender on each asset changes the probability that the asset can be successfully compromised by the attacker. Specifically, for each $v_{\mathrm{i}} \in V$, let $p_{\mathrm{i}} : \mathbb{R}_{\geq 0} \to [0, 1]$ be a function mapping the total defense investment x_{i} to an attack success probability on node v_{i}.

The goal of defender $\mathcal{D}$ is to choose her investment vector $\mathbf{x}$ in order to best protect her assets from being attacked. Mathematically, this is captured via the cost function

$$\overline{C}_D(\mathbf{x}) = \sum_{v_{\mathrm{i}} \in V} L_{\mathrm{i}} p_{\mathrm{i}}(x_{\mathrm{i}}) \tag{3.2}$$

subject to $\mathbf{x} \in X$. In particular, defender $\mathcal{D}$ chooses her investment $\mathbf{x} \in X$ to minimize $\overline{C}_D(\mathbf{x})$.

As discussed in the introduction, problems of this flavor have been studied in a variety of decision- and game-theoretic settings [7], [25]–[27]. However, as also mentioned in the introduction, humans have been shown to systematically misperceive probabilities, which can impact the decisions that defenders make in the presence of risk. We next introduce certain classes of probability weighting functions that capture this phenomenon into the above multi-target security formulation.

3.2 The Behavioral Multi-Target Security Problem

Recall that the defender seeks to protect a set of assets. The probability of each asset being successfully compromised is itself determined by the investments on that asset by the defender. This motivates an optimization problem that incorporates probability weighting, as defined below.

3.2.1 The Multi-Target Behavioral Security Problem

Definition 3.2.1. *We define a Multi-Target Behavioral Security Problem as the optimization problem faced by a defender $\mathcal{D}$ who is protecting a set of assets V, when she misperceives the attack probability on each asset according to the probability weighting function defined in (2.3). Specifically, the perceived attack probability on an asset $v_i \in V$ is given by:*

$$w(p_i(x_i)) = \exp\Big[-(-\log(p_i(x_i)))^{\alpha}\Big], \tag{3.3}$$

where $p_i(x_i) \in [0,1]$, $\alpha \in (0,1]$.

Formally, the optimization problem faced by the defender $\mathcal{D}$ is given by:

$$\underset{\mathbf{x}\in X}{\text{minimize}} \quad C_D(\mathbf{x}) = \sum_{i=1}^{n} L_i w(p_i(x_i)), \tag{3.4}$$

where the strategy space X is defined in (3.1).

The nonlinear nature of the probability weighting function (as shown in Fig. 2.2) leads to a complicated form for the utility function in (3.4). Nevertheless, we will start in the next section by showing that this optimization problem is convex under mild conditions on the probability of attack at each node. We will subsequently characterize properties of the investments by the defender, and identify how probability weighting impacts those decisions.

3.3 Convexity of Multi-Target Behavioral Security Problem

In this section, we prove the convexity of the cost function for the Multi-Target Behavioral Security Problem defined in Section 3.2. Throughout, let the function $p_i(x_i)$ represent the true probability of successful attack on an asset $v_i \in V$ when the total defense investment on that asset is x_i. We make the following assumption on $p_i(x_i)$.

Assumption 2. *The probability of successful attack on each asset $v_i \in V$, $p_i(x_i)$, has the following properties.*

- *$p_i(x_i)$ is twice differentiable with $\lim_{x_i\to\infty} p_i(x_i) = 0$ and $0 < p_i(x_i) < 1$ for any $x_i < \infty$.*

- $p_{\mathrm{i}}(x_{\mathrm{i}})$ *is strictly decreasing and log-convex in* x_{i}.
- $\frac{p_{\mathrm{i}}(x_{\mathrm{i}})}{p_{\mathrm{i}}(x_{\mathrm{i}})}$ *is bounded in* $x_{\mathrm{i}} \in \mathbb{R}_{\geq 0}$.

In other words, the larger the defensive security investment on a target, the less likely that the target will be successfully attacked. There are various probability functions that satisfy the conditions in Assumption 2; two examples are

$$p_{\mathrm{i}}(x_{\mathrm{i}}) = \exp(-x_{\mathrm{i}} - a_{\mathrm{i}}),\ p_{\mathrm{i}}(x_{\mathrm{i}}) = \frac{1}{x_{\mathrm{i}} + a_{\mathrm{i}}},$$

where $a_{\mathrm{i}} \in \mathbb{R}_{>0}$ ($a_{\mathrm{i}} \in \mathbb{R}_{\geq 1}$ in the second case) represents the pre-existing security investments on a node, which decreases the successful attack probability even under no additional defense investment.

Proposition 3.3.1. *Under Assumption 2, for every asset* $v_{\mathrm{i}} \in V$*, the perceived probability of attack* $w(p_{\mathrm{i}}(x_{\mathrm{i}}))$ *is strictly convex in the defense investment* x_{i}*. Thus, the Multi-Target Behavioral Security Problem (3.4) is strictly convex.*

The proof follows by calculating second derivative of $w(p_{\mathrm{i}}(x_{\mathrm{i}}))$ and using Assumption 2.

3.4 Properties of the Optimal Investment Decisions

Proposition 3.3.1 showed that the optimization problem (3.4) is convex as long as each node's probability of successful attack satisfies Assumption 2. However, to gain additional insights and to focus on how heterogeneous node values affect the investments by a behavioral defender, we will assume the following throughout the rest of the chapter.

Assumption 3. *The nodes are ordered such that* $L_1 > L_2 > \cdots > L_n$*. Furthermore, the probabilities of successful attack satisfy* $p_1(x) = p_2(x) = \cdots = p_n(x) = p(x)$*, where* $p(x)$ *satisfies Assumption 2.*

As we will see, interesting phenomomena arise even under the above assumption of identical probability functions at each node (note that compromise of each node is still independent of compromise of any other node, and only depends on the amount of investment on that node).

3.4.1 Ordering of Optimal Investments

Before characterizing the optimal investments by the defender, we will start with the following useful result pertaining to the marginals of the cost function (3.4).

Lemma 3. *Under Assumption 3, the marginal* $L_{\mathrm{i}}\frac{\partial w(p_{\mathrm{i}}(x))}{\partial x}$ *is negative, continuous, and increasing to* 0 *in* x *for all* $\mathrm{i} \in \{1, 2, \ldots, n\}$. *Furthermore, for each pair of nodes* $v_{\mathrm{i}}, v_{\mathrm{j}}$ *with* $\mathrm{i} < \mathrm{j}$, *the marginals satisfy*

$$L_{\mathrm{i}}\frac{\partial w(p_{\mathrm{i}}(x))}{\partial x} < L_{\mathrm{j}}\frac{\partial w(p_{\mathrm{j}}(x))}{\partial x} \tag{3.5}$$

for all $x \in \mathbb{R}_{\geq 0}$.

Proof. The perceived expected loss at node v_{i} is given by $L_{\mathrm{i}}w(p_{\mathrm{i}}(x_{\mathrm{i}}))$. Differentiating (3.3) with respect to the defender's investment in that node, we obtain

$$L_{\mathrm{i}}\tfrac{\partial w(p_{\mathrm{i}}(x))}{\partial x} = \alpha L_{\mathrm{i}}(-\log(p_{\mathrm{i}}(x)))^{\alpha-1}w(p_{\mathrm{i}}(x))\frac{p_{\mathrm{i}}(x)}{p_{\mathrm{i}}(x)}. \tag{3.6}$$

This function is negative (since $p_{\mathrm{i}}(x)$ is negative and $-\log(p_{\mathrm{i}}(x))$ is positive). Furthermore it is continuous, and increasing in x ($w(p_{\mathrm{i}}(x))$ is strictly convex as shown in Proposition 3.3.1, and thus we have $\frac{\partial}{\partial x}(\frac{\partial w(p_{\mathrm{i}}(x))}{\partial x}) > 0$). To show that the marginal goes to zero as $x \to \infty$, we note that

$$\lim_{x\to\infty}\left|L_{\mathrm{i}}\frac{\partial w(p_{\mathrm{i}}(x))}{\partial x}\right| = \lim_{x\to\infty}\left|\alpha L_{\mathrm{i}}(-\log(p_{\mathrm{i}}(x)))^{\alpha-1}w(p_{\mathrm{i}}(x))\right|\left|\frac{p_{\mathrm{i}}(x)}{p_{\mathrm{i}}(x)}\right| = 0,$$

since $p_{\mathrm{i}}(x) \to 0$ as $x \to \infty$ (which means $w(p_{\mathrm{i}}(x)) \to 0$ and $-\log(p_{\mathrm{i}}(x)) \to \infty$), and $\frac{p_{\mathrm{i}}(x)}{p_{\mathrm{i}}(x)}$ is bounded by Assumption 2. This proves the first part of the result. For the second part, note that if $L_{\mathrm{j}} < L_{\mathrm{i}}$ and $p_{\mathrm{i}}(x) = p_{\mathrm{j}}(x) = p(x)$ under Assumption 3, we obtain

$$L_{\mathrm{i}}(-\log(p(x)))^{\alpha-1}w(p(x))\frac{p(x)}{p(x)} < L_{\mathrm{j}}(-\log(p(x)))^{\alpha-1}w(p(x))\frac{p(x)}{p(x)},$$

for all $x \in \mathbb{R}_{\geq 0}$. Multiplying both sides by α to obtain the marginals, we have the ordering given by (3.5). □

We now give our first result on the nature of the optimal investments by the defender. Note that the exact values of these investments will be a function of α, but we elide the dependence on α for notational convenience (unless we explicitly require it).

Proposition 3.4.1. *Consider a defender $\mathcal{D}$ and a set of n assets satisfying Assumption 3. Then, the optimal defense allocation of (3.4), denoted $\mathbf{x}^* = \begin{bmatrix} x_1^* & x_2^* & \dots & x_n^* \end{bmatrix}^\intercal$, has the property that $x_1^* \geq x_2^* \geq \cdots \geq x_n^*$.*

Proof. From the KKT conditions for the defender's best response, for every pair of nodes v_i and v_j with nonzero optimal investments, the marginals must satisfy $L_\mathrm{i} \frac{\partial(w(p_\mathrm{i}(x_\mathrm{i})))}{\partial x_\mathrm{i}}|_{x_\mathrm{i}=x_\mathrm{i}^*} = L_\mathrm{j} \frac{\partial(w(p_\mathrm{j}(x_\mathrm{j})))}{\partial x_\mathrm{j}}|_{x_\mathrm{j}=x_\mathrm{j}^*}$.

If the probability of successful attack on the asset v_i satisfies Assumption 2, the perceived probability of successful attack on v_i would be given by (3.3).

Under Assumption 3, the above marginals under the defender's optimal investments would satisfy

$$L_\mathrm{i}(-\log(p(x_\mathrm{i}^*)))^{\alpha-1} w(p(x_\mathrm{i}^*)) \frac{p(x_\mathrm{i}^*)}{p(x_\mathrm{i}^*)} = L_\mathrm{j}(-\log\Big(p(x_\mathrm{j}^*)\Big))^{\alpha-1} w(p(x_\mathrm{j}^*)) \frac{p(x_\mathrm{j}^*)}{p(x_\mathrm{j}^*)} \tag{3.7}$$

for all nodes $v_\mathrm{i}, v_\mathrm{j}$ with nonzero optimal investments x_i^* and x_j^*, respectively. Using (3.7) and assuming without loss of generality that $\mathrm{i} < \mathrm{j}$, we obtain

$$\begin{aligned}
&(-\log(p(x_\mathrm{i}^*)))^{\alpha-1} w(p(x_\mathrm{i}^*)) \frac{p(x_\mathrm{i}^*)}{p(x_\mathrm{i}^*)} \\
&\quad = \frac{L_\mathrm{j}}{L_\mathrm{i}} (-\log\Big(p(x_\mathrm{j}^*)\Big))^{\alpha-1} w(p(x_\mathrm{j}^*)) \frac{p(x_\mathrm{j}^*)}{p(x_\mathrm{j}^*)} \\
&\quad \geq (-\log\Big(p(x_\mathrm{j}^*)\Big))^{\alpha-1} w(p(x_\mathrm{j}^*)) \frac{p(x_\mathrm{j}^*)}{p(x_\mathrm{j}^*)}
\end{aligned}$$

since $L_\mathrm{i} \geq L_\mathrm{j}$ and all of the above expressions are negative. As the marginals are increasing in x (by Lemma 3), the above expression implies $x_\mathrm{i}^* \geq x_\mathrm{j}^*$. This concludes the proof. □

The above result shows that the defender will invest more in higher-valued assets (and this is true for all $\alpha \in (0, 1]$).

3.4.2 Water-Filling Nature of Investments

To gain further insights into the optimal investments, we can leverage Lemma 3 to introduce the following quantities.

Definition 3.4.1. *Suppose the nodes satisfy Assumption 3. For all* $\mathrm{i} \in \{1, 2, \ldots, n\}$ *and* $\mathrm{j} \in \{1, 2, \ldots, n\}$ *with* $\mathrm{i} < \mathrm{j}$*, define the quantity* $x^*_{\mathrm{ij}} \in \mathbb{R}_{\geq 0}$ *to be such that*

$$L_{\mathrm{i}} \frac{\partial w(p_{\mathrm{i}}(x))}{\partial x}\bigg|_{x=x^*_{\mathrm{ij}}} = L_{\mathrm{j}} \frac{\partial w(p_{\mathrm{j}}(x))}{\partial x}\bigg|_{x=0}. \tag{3.8}$$

We will use the notation $x^*_{\mathrm{ij}}(\alpha)$ *when needed to explicitly indicate the dependence of* x^*_{ij} *on* α*.*

Note that by Lemma 3, the quantity x^*_{ij} exists and is unique for each $\mathrm{i} < \mathrm{j}$ (by virtue of the fact that the marginals are negative, continuous, and increasing to 0 in x). Based on the above definition, we now present the following result.

Proposition 3.4.2. *Under Assumption 3, node* v_{j} *will have a nonzero optimal investment* x^*_{j} *if and only if the defense budget satisfies* $B > \sum_{\mathrm{i}=1}^{\mathrm{j}-1} x^*_{\mathrm{ij}}$*.*

Proof. First suppose that v_{j} has a nonzero optimal investment x^*_{j}, and suppose by way of contradiction that $B \leq \sum_{\mathrm{i}=1}^{\mathrm{j}-1} x^*_{\mathrm{ij}}$. Then, $\exists \mathrm{i} \in \{1, \ldots, \mathrm{j}-1\}$ such that $x^*_{\mathrm{i}} < x^*_{\mathrm{ij}}$ (i.e., it would not be possible to put x^*_{ij} or more investment in each node v_{i} that precedes v_{j} without exceeding the budget). By the definition of x^*_{ij} in Definition 3.4.1, and using Lemma 3, we have

$$\begin{aligned} L_{\mathrm{i}} \frac{\partial(w(p_{\mathrm{i}}(x_{\mathrm{i}})))}{\partial x_{\mathrm{i}}}|_{x_{\mathrm{i}}=x^*_{\mathrm{i}}} &< L_{\mathrm{j}} \frac{\partial(w(p_{\mathrm{j}}(x_{\mathrm{j}})))}{\partial x_{\mathrm{j}}}|_{x_{\mathrm{j}}=0} \\ &< L_{\mathrm{j}} \frac{\partial(w(p_{\mathrm{j}}(x_{\mathrm{j}})))}{\partial x_{\mathrm{j}}}|_{x_{\mathrm{j}}=x^*_{\mathrm{j}}} \end{aligned}$$

which yields a contradiction since the marginals must all be equal at the optimal investments. Thus, if $x^*_{\mathrm{j}} > 0$, it must be that $B > \sum_{\mathrm{i}=1}^{\mathrm{j}-1} x^*_{\mathrm{ij}}$.

To prove the other direction, suppose that $B > \sum_{\mathrm{i}=1}^{\mathrm{j}-1} x^*_{\mathrm{ij}}$. Suppose by way of contradiction that $x^*_{\mathrm{j}} = 0$. Then, we have $x^*_k = 0 \ \forall k > \mathrm{j}$ (from Proposition 3.4.1). Thus, we have $x^*_1 + x^*_2 + \cdots + x^*_{\mathrm{j}-1} = B$ and $\exists \mathrm{i} \in \{1, \ldots, \mathrm{j}-1\}$ s.t. $x^*_{\mathrm{i}} > x^*_{\mathrm{ij}}$.

Now, we show that moving a sufficiently small investment ϵ from asset v_{i} to asset v_{j} will lead to a net reduction in perceived cost in (3.4), thereby contradicting the optimality of these investments.

Starting with the given nonzero investments on the assets $\{v_1, \ldots, v_{\mathrm{j}-1}\}$, the perceived cost in (3.4) will be:

$$C_D(\mathbf{x}^*) = \sum_{k=1}^{n} L_k w(p_k(x_k^*)).$$

From the asset v_{i} that had $x_{\mathrm{i}}^* > x_{\mathrm{ij}}^*$, remove a sufficiently small investment ϵ, and add an investment of ϵ to asset v_{j}. Denote the modified investment vector by $\bar{\mathbf{x}}$. The perceived cost in (3.4) under this investment vector will be

$$C_D(\bar{\mathbf{x}}) = \sum_{k \notin \{\mathrm{i},\mathrm{j}\}} L_k w(p_k(x_k^*)) + L_{\mathrm{i}} w(p_{\mathrm{i}}(x_{\mathrm{i}}^* - \epsilon)) + L_{\mathrm{j}} w(p_{\mathrm{j}}(\epsilon)).$$

The net reduction in perceived cost will be positive if $C_D(\bar{\mathbf{x}}) < C_D(\mathbf{x}^*)$. Define

$$f(\epsilon) = L_{\mathrm{i}} w(p_{\mathrm{i}}(x_{\mathrm{i}}^* - \epsilon)) + L_{\mathrm{j}} w(p_{\mathrm{j}}(\epsilon)),$$

and note that

$$C_D(\mathbf{x}^*) = \sum_{k \notin \{\mathrm{i},\mathrm{j}\}} L_k w(p_k(x_k^*)) + f(0)$$
$$C_D(\bar{\mathbf{x}}) = \sum_{k \notin \{\mathrm{i},\mathrm{j}\}} L_k w(p_k(x_k^*)) + f(\epsilon).$$

Thus, $C_D(\bar{\mathbf{x}})$ will be smaller than $C_D(\mathbf{x}^*)$ if $f(\epsilon) < f(0)$. We have

$$\frac{df}{d\epsilon} = -\, L_{\mathrm{i}} \frac{\partial w(p_{\mathrm{i}}(x))}{\partial x}\bigg|_{x = x_{\mathrm{i}}^* - \epsilon} + L_{\mathrm{j}} \frac{\partial w(p_{\mathrm{j}}(x))}{\partial x}\bigg|_{x=\epsilon}.$$

Since $x_{\mathrm{i}}^* > x_{\mathrm{ij}}^*$, we have (from Lemma 3 and the definition of x_{ij}^*)

$$L_{\mathrm{i}} \frac{\partial w(p_{\mathrm{i}}(x))}{\partial x}\bigg|_{x = x_{\mathrm{i}}^*} > L_{\mathrm{j}} \frac{\partial w(p_{\mathrm{j}}(x))}{\partial x}\bigg|_{x=0}.$$

Thus, $\lim_{\epsilon \downarrow 0} \frac{df}{d\epsilon}$ is negative, which shows that $f(\epsilon)$ is decreasing for sufficiently small ϵ. Thus, $C_D(\bar{\mathbf{x}}) < C_D(\mathbf{x}^*)$ for sufficiently small ϵ which yields a contradiction. □

The above result indicates that the optimal investments by the defender have a "water-filling" nature. Specifically, given a budget B, the defender invests in node v_1 until the investment reaches x^*_{12}, at which point the defender invests in both v_1 and v_2 (keeping their marginals the same) until the investments in each reach x^*_{13} and x^*_{23}, respectively. At that point, the defender adds investments to v_1, v_2 and v_3 simultaneously (keeping their marginals equal), and continues in this manner until the entire budget is spent.

3.4.3 Effect of Probability Weighting on Investments

The above results held irrespective of the particular value of $\alpha \in (0, 1]$. Recall that α controlled the extent of underweighting and overweighting in the Prelec probability weighting function (2.3). In particular, smaller values of α correspond to a larger amount of overweighting and underweighting (see Fig. 2.2). We now study the impact of probability weighting on the investments (i.e., how the investments change as α changes).

Lemma 4. *Suppose Assumption 3 holds, and furthermore that* $p(0) \leq \frac{1}{\mathrm{e}}$. *Then,* $\forall \mathrm{i} \in \{1, \ldots, n\}$ *and* $\mathrm{j} \in \{1, \ldots, n\}$ *with* $\mathrm{i} < \mathrm{j}$, *the quantity* $x^*_{\mathrm{ij}}(\alpha)$ *is decreasing in* α.

Proof. From Definition 3.4.1, the value of $x^*_{\mathrm{ij}}(\alpha)$ is given by (3.8) for all $\mathrm{i} < \mathrm{j}$. Using the expression for the marginals given by (3.6), and noting that $p_{\mathrm{i}}(x) = p_{\mathrm{j}}(x) = p(x)$ from Assumption 3, $x^*_{\mathrm{ij}}(\alpha)$ satisfies the equation

$$L_{\mathrm{i}}(-\log\Big(p(x^*_{\mathrm{ij}}(\alpha))\Big))^{\alpha-1} w(p(x^*_{\mathrm{ij}}(\alpha))) \frac{p(x^*_{\mathrm{ij}}(\alpha))}{p(x^*_{\mathrm{ij}}(\alpha))} = L_{\mathrm{j}}(-\log(p(0)))^{\alpha-1} w(p(0)) \frac{p(0)}{p(0)}. \tag{3.9}$$

In (3.9), taking the logarithm of both sides and differentiating yields that $\frac{dx^*_{\mathrm{ij}}}{d\alpha}$ is given by:

$$\frac{dx^*_{\mathrm{ij}}}{d\alpha} = \frac{\Big[\Big(-\log\Big(p(x^*_{\mathrm{ij}})\Big)\Big)^{\alpha} - 1\Big] \log\Big(-\log\Big(p(x^*_{\mathrm{ij}})\Big)\Big)}{z(x^*_{\mathrm{ij}})} - \frac{[(-\log(p(0)))^{\alpha} - 1] \log(-\log(p(0)))}{z(x^*_{\mathrm{ij}})}$$

where

$$z(x_{ij}^*) = (\alpha - 1 - \alpha(-\log\Big(p(x_{ij}^*)\Big))^{\alpha})\frac{p(x_{ij}^*)}{p(x_{ij}^*)\log\Big(p(x_{ij}^*)\Big)} + \frac{p(x_{ij}^*)p(x_{ij}^*) - (p(x_{ij}^*))^2}{p(x_{ij}^*)p(x_{ij}^*)}.$$

From Assumption 2, we have $p(x_{ij}^*) < 0$, $\log\Big(p(x_{ij}^*)\Big) < 0$ and $p(x)$ is log-convex, thus $p(x_{ij}^*)p(x_{ij}^*) - (p(x_{ij}^*))^2 \geq 0$. Thus, the denominator $z(x_{ij}^*)$ of $\frac{dx_{ij}^*}{d\alpha}$ is negative.

From Assumption 2 and the assumption that $p(0) \leq \frac{1}{e}$, we have $-\log\Big(p(x_{ij}^*)\Big) > 1$ and $-\log(p(0)) \geq 1$. Thus, we have $\log\Big(-\log\Big(p(x_{ij}^*)\Big)\Big) > 0$ and $\log(-\log(p(0))) \geq 0$. Moreover, we have

$$\begin{aligned} x_{ij}^* > 0 &\iff p(x_{ij}^*) < p(0) \\ &\iff -\log\Big(p(x_{ij}^*)\Big) > -\log(p(0)) \\ &\iff (-\log\Big(p(x_{ij}^*)\Big))^{\alpha} > (-\log(p(0)))^{\alpha} \\ &\iff (-\log\Big(p(x_{ij}^*)\Big))^{\alpha} - 1 > (-\log(p(0)))^{\alpha} - 1. \end{aligned}$$

Thus, the numerator of $\frac{dx_{ij}^*}{d\alpha}$ is positive and hence the derivative $\frac{dx_{ij}^*}{d\alpha}$ is negative, yielding that $x_{ij}^*(\alpha)$ is decreasing in α. □

The above result leads to the following key outcome, showing that behavioral players will generally invest in fewer nodes than non-behavioral players (given the same budget).

Proposition 3.4.3. *Suppose Assumption 3 holds, and furthermore that $p(0) \leq \frac{1}{e}$. Then, the number of nodes that have positive optimal investment is nondecreasing in α.*

Proof. Consider $\alpha_1 \in (0, 1]$ and $\alpha_2 \in (0, 1]$, with $\alpha_1 < \alpha_2$. Let $\{x_{ij}^*(\alpha_1)\}$ and $\{x_{ij}^*(\alpha_2)\}$ be the corresponding sets of investment thresholds for each of those values of α, where $x_{ij}^*(\alpha)$ is defined in Definition 3.4.1. From Lemma 4 we have $x_{ij}^*(\alpha_2) < x_{ij}^*(\alpha_1)$ for all $i < j$.

Let k be the index of the last node that has positive investment when the weighting parameter is α_1. From Proposition 3.4.2, we have

$$B > \sum_{i=1}^{k-1} x_{ik}^*(\alpha_1) > \sum_{i=1}^{k-1} x_{ik}^*(\alpha_2).$$

Thus, by Lemma 3, we see that node k would also have positive investment when the parameter is α_2. Thus, the number of nodes that have positive investment under α_2 is at least as large as the number of nodes that have positive investment under α_1. □

The above result shows that a behavioral defender may choose to leave lower valued nodes vulnerable, and instead concentrate their investments on the high-valued nodes. This will have implications for the (true) expected loss faced by the defender. We illustrate the phenomenon identified by the above results and the resulting impact on the defender's true loss in the next section.

3.5 Numerical Simulations

3.5.1 Effect of Perception on Investments

In this subsection, we show the effects of probability misperception identified in the previous sections on the defense investment decisions in the Multi-Target Behavioral Security Problem. In this context, consider a setting with four critical assets (or targets). The first asset has very high loss (i.e., $L_1 = 1000$) while the second, third, and fourth assets have progressively lower losses (with $L_2 = 250$, $L_3 = 60$, and $L_4 = 15$). We let the total defense budget for defending the four critical assets be $B = 10$. The probability of successful attack on each of the assets is given by

$$p(x) = \mathrm{e}^{-x-1}$$

where x is the investment on that asset. The above function satisfies the conditions in Assumption 2. The optimal investments in the following scenarios were calculated using Matlab Optimization toolbox [57]. Fig. 3.1 shows the difference in the defense investments for each of the assets as α changes for the defender. We observe that the phenomena identified in Propositions 3.4.1, 3.4.2, and 3.4.3 are indeed manifested in these plots. First, for each value of α, the investments are ordered by the value of the assets. Second, as α gets smaller (i.e., the defender becomes more behavioral), the investments are shifted to a smaller number of higher-valued assets. For example, the non-behavioral defender (with $\alpha = 1$) puts nonzero investments on all of the four assets, a behavioral defender (with

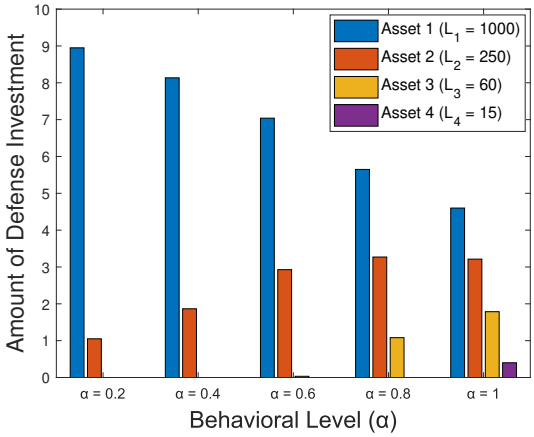


Figure 3.1. Effect of behavioral probability weighting on the defense investments on four assets. The asset with the highest loss takes a higher portion of the defense investments as the defender becomes more behavioral (i.e., α decreases). Moreover, the number of assets with positive investment decreases as the defender becomes more behavioral.

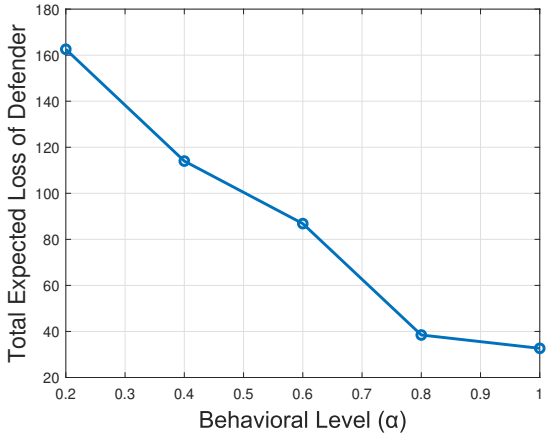


Figure 3.2. Effect of behavioral probability weighting on the true expected loss of the defender. The true expected loss of the defender is higher as the defender becomes more behavioral. In particular, the true expected loss of a highly behavioral defender (with $\alpha = 0.4$) is approximately 3.5 times that for the non-behavioral defender (with $\alpha = 1$).

$\alpha = 0.6$) puts nonzero investments on the first three assets, and a highly behavioral defender (with $\alpha = 0.4$) puts nonzero investments only on the first two assets.

3.5.2 Effect of Behavioral Investments on Real Loss

We further consider the total expected system loss E_T of the defender under their optimal investments, given by the sum of the true expected losses of all assets. As shown in Fig. 3.2, when the defender is non-behavioral (i.e., $\alpha = 1$) $E_T = 32.67$, while $E_T = 114.01$ when $\alpha = 0.4$. This considerable increase in the total real loss of the behavioral defender shows that probability weighting induces the defender to invest in a sub-optimal manner, specifically when some assets are much more valuable than others.

3.6 Summary of Findings

This chapter presented a framework that accounts for behavioral attitudes of the defender in a Multi-Target Security Problem where the defender places her investments to protect the target assets. Specifically, we considered the scenario where the (human) defender misperceives the probabilities of successful attack in each asset. We first established the convexity of the objective function of the defender. We then studied the impacts of probability weighting on the investment decisions made by the defender; in particular, we showed that nonlinear perceptions of probability can induce the defender to invest more on the assets with higher values. Moreover, nonlinear perceptions of probability can induce the defender to put nonzero investments on fewer assets. Finally, we provided numerical simulations to show the effect of probability misperceptions on the investment decisions. Future avenues of research include considering strategic attackers and exploring other factors in prospect theory such as subjective assessments of outcomes.

4. A Game-Theoretic Analysis to Protect Heterogeneous Common Pool Resources under Behavioral Probability Weighting

In this chapter, we introduce prospect theory into a game-theoretic framework involving multiple players protecting multiple shared assets with heterogeneous valuations from failure. Specifically, we consider a setting consisting of many common-pool assets, and assume that each player misperceives the probabilities of failure of each asset. We characterize the impacts of such misperceptions on the investments made by the players both in a game-theoretic setting (Section 4.6 and Section 4.7).

We first establish the convexity of the objective function of each player in this setting, even under nonlinear probability weighting (subject to appropriate conditions on the probability of failure on the nodes). We then characterize the optimal investments in the assets. We then show the existence of a Pure Strategy Nash Equilibrium (PNE) in this game, and characterize properties of the investment profiles at the PNE. In particular, we show that the total investment in each asset is unique across all PNE. Furthermore, we show that in settings where the probability of failure is sufficiently low, behavioral probability weighting by the players causes the PNE investments to shift to higher-valued assets compared to a setting with players that correctly perceive the failure probabilities. In particular, the number of nodes that have positive investment decreases as the players become more behavioral, which increases the (true) expected cost (loss) of each player. We also provide numerical simulations to illustrate our findings, and to explore additional features such as heterogeneity in behavioral levels.

This chapter extends our previous chapter (Chapter 3) as follows:

- While Chapter 3 only considered a setting with a single player, our work in this chapter considers the general common pool resources (CPR) game-theoretic setting with multiple players. We show the existence of PNE in those games, characterize the uniqueness of the total investments on each asset at any PNE, and identify the impacts of probability weighting on the PNE investments.

- We consider a more general class of probability weighting functions (incorporating both S-shaped and inverse S-shaped functions), in contrast to Chapter 3 which only considered inverse S-shape probability weighting.

- We quantify the effect of heterogeneity of behavioral levels on the investments at PNE, compare different possible training policies for enhancing social cost, and illustrate our theoretical findings via numerical simulations.

4.1 Related Literature

4.1.1 Prospect-theoretic preferences in experimental studies on CPR games

Several prior experimental works that explored CPR games and related settings have shown evidence of prospect-theoretic risk preferences. In particular, the level of cooperation among users (players) in CPR games and public goods (PG) games with identical utilities have been observed to differ in experimental studies [58]–[60]. In those studies, the experiments have shown that loss averse players tend to cooperate more in the CPR game. Other experimental works focused on the rate of convergence to Nash equilibrium in CPR games [61]. Moreover, the effects of loss aversion, reference dependence, and framing effects have been investigated in threshold PG games with deterministic threshold values in [62] and [63]. In [63], the authors studied the effect of probability weighting on users' strategies. Our analysis provides a theoretical characterization of the impact of behavioral risk misperception on investing on the shared resource(s).

4.1.2 Theoretical analysis of prospect-theoretic behavior in games

The theoretical investigations of the effect of prospect theoretic attributes (i.e., reference dependence, loss aversion and probability weighting) on decision-making in multi-player settings has been relatively limited [64]. The work [65] explored equilibria in strategic games with finite action sets when players have prospect-theoretic risk preferences. This further motivates investigations of prospect-theoretic preferences in strategic multi-player settings. In particular, the impacts of the probability weighting function and loss aversion

have been examined in the contest theory literature in [66] and [67], respectively. Butler studied the impact of prospect theory in an ultimatum game [68]. The work [69] focused only on the effect of the value function on players' strategies and did not explore the effect of probability weighting functions to model uncertainty in a common-pool resource game. Recently, multiple works [31], [32], [36], [70] have modeled the effect of behavioral decision-making on the players' investments, and its effects on shared system's security and robustness. However, these works focused on understanding the role of the network structure [31], [32], [71] and settings with only single target [36]. In contrast to these works, here we consider the effects of behavioral decision-making in a setting with multiple players and multiple targets with *heterogeneous* values to the players and model such setting via a CPRs game.

4.1.3 Total Effort Games and Group Contests

Total effort games have the characteristic that investments of each player can help the other players by improving their utilities (here, reducing their costs) in a non-direct manner, similar to public good provision with positive externalities. Thus, some players can free ride (i.e., under-invest in the assets) and depend on the investments by other players. This leads to a reduction in social welfare [39], [40]. This motivates the study of mechanisms for improving social welfare, and ideally, incentivizing user cooperation and driving the system to a socially optimal state (e.g., [41], [72]). Such lines of work have considered quasi-linear costs and Nash equilibrium solutions of the mechanisms, but have not investigated behavioral decision-making effects that we consider here in our current work. Another related line of work is the group contests that has different applications such as competition between political parties, team-incentives within firms, and rent-seeking. Experimental research has investigated incentives to induce members of the same group to cooperate with each other by expending effort [73]. However, the cost of cooperation and group asymmetry can also incentivize members to abstain from expending any effort and instead free ride on efforts of other members [74]. These works have not explored behavioral decision-making effects in such settings.

4.2 Outline of Chapter

The remainder of this chapter is organized as follows. We introduce the game framework in Section 4.3, followed by the Behavioral Multi-Target CPR Game in Section 4.4. We show the convexity of players' costs and prove the existence of a PNE in the game in Section 4.5. We show the properties of the PNE in Section 4.6. We characterize impacts of probability weighting on the PNE investments in our multi-player game in Section 4.7. We provide numerical simulations in Section 4.8 and conclude the chapter in Section 4.9.

4.3 The Multi-Target CPR Game

In this section, we describe our general game framework, including the multi-target setup and the characteristics of the players.

4.3.1 Assets and Strategic Players

Let $\mathcal{D}$ be the set of all players who are responsible for protecting a set $V = \{v_1, v_2, \ldots, v_n\}$ of assets. For each failed asset $v_m \in V$, player D_k will incur a financial loss $L_m^k \in \mathbb{R}_{>0}$. To reduce the failure probabilities on assets, a player can allocate resources on these assets, subject to the constraints described below.

Let $n = |V|$. We assume that each player $D_k \in \mathcal{D}$ has a budget $B_k \in \mathbb{R}_{>0}$. Let x_{i}^k denote the investment of player D_k on the asset v_{i}. Thus, we define the strategy space of each player $D_k \in \mathcal{D}$ by

$$X_k \triangleq \{[x_1^k, x_2^k, \ldots, x_n^k] \in \mathbb{R}_{\geq 0}^n : \sum_{\mathrm{i}=1}^{n} x_{\mathrm{i}}^k \leq B_k\}. \tag{4.1}$$

In other words, the strategy space for player D_k consists of all non-negative investments on the assets such that the sum of all investments does not exceed the player's budget B_k. We denote any particular set of investments by player D_k by $\mathbf{x}_k \in X_k$ where $\mathbf{x}_k = \left[x_1^k, x_2^k, \ldots, x_n^k\right]$.

Let $\mathbf{x} = \left[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{|\mathcal{D}|}\right] \in X_1 \times X_2 \times \cdots \times X_{|\mathcal{D}|}$ be a joint investment strategy of all players, with $\mathbf{x}_k \in X_k$ for player D_k. Under a joint investment strategy $\mathbf{x}$, we denote the total investment on asset v_{i} by $x_{\mathrm{i}}^T \triangleq \sum_{D_k \in \mathcal{D}} x_{\mathrm{i}}^k$. Let the scalar $y_{\mathrm{i}} \triangleq \sum_{D_l \in \mathcal{D} \setminus \{D_k\}} x_{\mathrm{i}}^l$ denote the sum

of the investments of all players except D_k on asset v_i. Thus, $x_\mathrm{i}^T \triangleq x_\mathrm{i}^k + y_\mathrm{i}$. We denote any particular set of investments by players other than D_k by $\mathbf{x}_{-k}$ where $\mathbf{x}_{-k} = [y_1, y_2, \ldots, y_n]$.

4.3.2 Player's Cost

The investments made by the players on each asset change the probability of failure of that asset. Specifically, for each $v_\mathrm{i} \in V$, let $p_\mathrm{i} : \mathbb{R}_{\geq 0} \to [0, 1]$ be a function mapping the total investment x_i^T to a failure probability on node v_i.

The goal of each player $D_k \in \mathcal{D}$ is to choose her investment vector $\mathbf{x}_k$ in order to best protect her assets from failure. Mathematically, for a given vector of investments $\mathbf{x} \in X_1 \times X_2 \times \cdots \times X_\mathcal{D}$, the cost faced by player $D_k \in \mathcal{D}$ is given by

$$\overline{C}_k(\mathbf{x}) = \sum_{v_\mathrm{i} \in V} L_\mathrm{i}^k \; p_\mathrm{i}(x_\mathrm{i}^T). \tag{4.2}$$

In particular, player D_k chooses her investment $\mathbf{x}_k \in X_k$ to minimize $\overline{C}_k(\mathbf{x})$, given the investments of the other players.

As discussed above, problems of this flavor have been studied in a variety of decision- and game-theoretic settings [7], [25]–[27]. However, as also mentioned throughout the thesis, humans have been shown to systematically misperceive probabilities, which can impact the decisions that players make in the presence of risk. We next review certain classes of probability weighting functions that capture this phenomenon, and subsequently introduce such functions into the above multi-target CPR game formulation.

4.4 The Behavioral Multi-Target CPR Game

4.4.1 Nonlinear Probability Weighting

Inverse S-shape Behavior: The behavioral economics and psychology literature has shown that humans consistently misperceive probabilities by overweighting low probabilities and underweighting high probabilities [14], [47]. More specifically, humans perceive a "true" probability $p \in [0, 1]$ as $w(p) \in [0, 1]$, where $w(\cdot)$ is a probability weighting function. A

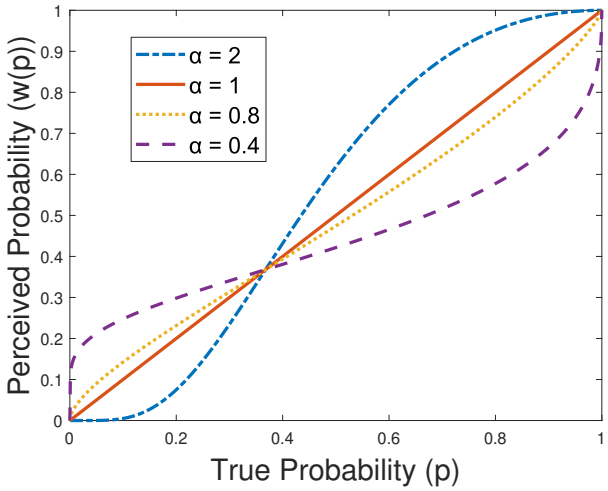


Figure 4.1. Prelec probability weighting function which transforms true probabilities p into perceived probabilities $w(p)$. The parameter α controls the extent of overweighting and underweighting.

commonly studied probability weighting function was proposed by Prelec in [47], and is given by

$$w(p) = \exp\Big[-(-\log(p))^{\alpha}\Big], \quad p \in [0,1], \tag{4.3}$$

where $\alpha \in (0,1]$ is a parameter that controls the extent of overweighting and underweighting. When $\alpha = 1$, we have $w(p) = p$ for all $p \in [0,1]$, which corresponds to the situation where probabilities are perceived correctly. Smaller values of α lead to a greater amount of overweighting and underweighting, as illustrated in Fig. 4.1.

S-shape Behavior: There are also a few papers [75], [76] that have observed the opposite of prospect theory in terms of how humans weigh probabilities in security scenarios (i.e., players' probability weighting functions were found to be S-shaped in those security experiments). One way to capture this behavior is by using the Prelec function and setting $\alpha \in \mathbb{R}_{>1}$. Here, higher values of α lead to a greater amount of overweighting high probabilites and underweighting low probabilities, as shown in Fig. 4.1.

Recall that in our setting, each player seeks to protect a set of assets. The probability of failure of each asset is itself determined by the investments on that asset by the player. This motivates a game that incorporates probability weighting, as defined below. Due to the

fact that both the (classical) inverse S-shaped and S-shaped probability weighting functions can be captured by choosing α appropriately in the Prelec function (4.3), we will provide a unified treatment of both cases by allowing α to take any value in $(0, \infty)$ in our analysis.

4.4.2 The Multi-Target Behavioral CPR Game

Definition 4.4.1. *We define a Multi-Target Behavioral CPR Game as a game between multiple players with a set of assets, where each player $D_k \in \mathcal{D}$ misperceives the failure probability on each asset according to the probability weighting function defined in (4.3). Specifically, for any given total investment $x_{\mathrm{i}}^T \in \mathbb{R}_{\geq 0}$, the perceived failure probability on asset $v_{\mathrm{i}} \in V$ by player $D_k \in \mathcal{D}$ is given by*

$$w_k(p_{\mathrm{i}}(x_{\mathrm{i}}^T)) = \exp\Big[-\Big(-\log\big(p_{\mathrm{i}}(x_{\mathrm{i}}^T)\big)\Big)^{\alpha_k} \Big], \tag{4.4}$$

where $p_{\mathrm{i}}(x_{\mathrm{i}}^T) \in [0,1]$, $\alpha_k \in (0, \infty)$. Thus, each behavioral player D_k allocates her investments to minimize the expected perceived cost function, given by

$$\begin{aligned} C_k(\mathbf{x}_k, \mathbf{x}_{-k}) &= \sum_{\mathrm{i}=1}^{n} L_{\mathrm{i}}^k w_k(p_{\mathrm{i}}(x_{\mathrm{i}}^T)) \\ &= \sum_{\mathrm{i}=1}^{n} L_{\mathrm{i}}^k w_k(p_{\mathrm{i}}(x_{\mathrm{i}}^k + y_{\mathrm{i}})) \end{aligned} \tag{4.5}$$

subject to $\mathbf{x}_k \in X_k$.

Remark 6. The subscript k in α_k and $w_k(\cdot)$ allows each player in the Multi-Target Behavioral CPR Game to have a different level of mis-perception. However, for ease of notation, we will drop the subscript k for most of our analysis, when it is clear from the context. ■

We formally define the notion of best response and a Pure Strategy Nash Equilibrium (PNE) in our CPR game as follows.

Definition 4.4.2. *The best response of player D_k at a given investment profile $\mathbf{x}_{-k} = [y_1, y_2, \ldots, y_n]$ by other players is the set* $\operatorname{argmin}_{\mathbf{x}_k \in X_k} C_k(\mathbf{x}_k, \mathbf{x}_{-k})$.

Definition 4.4.3. *A strategy profile* $\{\mathbf{x}_1^*, \mathbf{x}_2^*, \ldots, \mathbf{x}_{|\mathcal{D}|}^*\} \in X_1 \times X_2 \times \cdots \times X_{|\mathcal{D}|}$ *is a pure strategy Nash equilibrium (PNE) of the Multi-Target Behavioral CPR Game if and only if* $\mathbf{x}_k^* \in \operatorname{argmin}_{\mathbf{x_k} \in X_k} C_k(\mathbf{x}_k, \mathbf{x}_{-k}^*)$ *for every player* $D_k \in \mathcal{D}$ *where* $\mathbf{x}_{-k}^*$ *is the aggregate best responses by other players other than* D_k.

4.4.3 Assumptions on the Probabilities of Failure

Recall that the function $p_{\mathrm{i}}(x_{\mathrm{i}}^T)$ represents the true probability of failure on an asset $v_{\mathrm{i}} \in V$ when the total investment on that asset is x_{i}^T. We make the following assumption on $p_{\mathrm{i}}(x_{\mathrm{i}}^T)$ throughout our analysis.

Assumption 4. *The probability of failure on each asset* $v_{\mathrm{i}} \in V$, $p_{\mathrm{i}}(x_{\mathrm{i}}^T)$, *has the following properties.*

- $p_{\mathrm{i}}(x_{\mathrm{i}}^T)$ *is twice differentiable with* $\lim_{x_{\mathrm{i}}^T \to \infty} p_{\mathrm{i}}(x_{\mathrm{i}}^T) = 0$ *and* $0 < p_{\mathrm{i}}(x_{\mathrm{i}}^T) < 1$ *for all* $x_{\mathrm{i}}^T \in [0, \infty)$.
- $p_{\mathrm{i}}(x_{\mathrm{i}}^T)$ *is strictly decreasing and log-convex*[1] *in* x_{i}^T.
- $\frac{p_{\mathrm{i}}(x_{\mathrm{i}}^T)}{p_{\mathrm{i}}(x_{\mathrm{i}}^T)}$ *is bounded in* $x_{\mathrm{i}}^T \in \mathbb{R}_{\geq 0}$.

In other words, the larger the investment on a target, the less likely that the target will be experiencing failure. See Chapter 3 for probability functions that satisfy the conditions in Assumption 4.

Now, we establish the convexity of the cost functions and the existence of PNE in our CPR game.

4.5 Convexity of Cost Functions and Existence of PNE

The nonlinear (and nonconvex) nature of the probability weighting function (as shown in Fig. 4.1) leads to a complicated form for the utility function (4.5) for each player. Nevertheless, we will show in this section that this optimization problem is convex under

[1]↑This is a common assumption in the literature. In particular, [28] shows that log-convexity of the failure probability functions is a necessary and sufficient condition for the optimal investment result of the seminal paper [25] to hold.

mild conditions, and subsequently prove the existence of a PNE in the game. We start with the following result.

Lemma 5. *Under Assumption 4, for every player $D_k \in \mathcal{D}$, for every asset $v_\mathrm{i} \in V$, and for all $y_\mathrm{i} \in \mathbb{R}_{\geq 0}$, the perceived probability of failure $w_k(p_\mathrm{i}(x_\mathrm{i}^k + y_\mathrm{i}))$ is strictly convex in the investment x_i^k in the following cases:*

i. if $\alpha_k \in (0, 1]$;

ii. if $\alpha_k \in \mathbb{R}_{>1}$ and $p_\mathrm{i}(x_\mathrm{i}^T) \leq \frac{1}{\mathrm{e}}\ \forall x_\mathrm{i}^T \in [0, \infty)$.

Proof. For ease of notation, we drop the indices i (corresponding to the asset) and k (corresponding to the player) in the following analysis, and denote x_i^k as x, y_i as y, and α_k as α.

i) First, note that if $\alpha = 1$, we have $w(p(x+y)) = p(x+y)$. Since $p(\cdot)$ is strictly decreasing and log-convex in its argument, it is also strictly convex, and thus $w(p(x+y))$ is strictly convex in x for $\alpha = 1$. Thus, we will focus on the case where $\alpha \in (0, 1)$ in the rest of the proof of the first part of the proposition.

Note from Assumption 4 that $0 < p(x+y) < 1$, and so we have $0 < -\log(p(x+y)) < \infty$ for all $x \in \mathbb{R}_{\geq 0}$. We prove this part by calculating the second derivative of $w(p(x+y))$ with respect to x as follows:

$$\frac{d}{dx} w(p(x+y)) = \alpha(-\log(p(x+y)))^{\alpha-1} \frac{p(x+y)}{p(x+y)} w(p(x+y)). \tag{4.6}$$

$$\frac{d^2}{dx^2} w(p(x+y)) = \alpha(-\log(p(x+y)))^{\alpha-1} \frac{w(p(x+y))}{p(x+y)} \times \left[\frac{p(x+y)\frac{d}{dx} w(p(x+y))}{w(p(x+y))} - \frac{(\alpha-1)(p(x+y))^2}{p(x+y)(-\log(p(x+y)))} + \frac{p(x+y)p(x+y) - (p(x+y))^2}{(p(x+y))} \right] \tag{4.7}$$

From Assumption 4, $p(\cdot)$ is strictly decreasing and thus $\frac{d}{dx} w(p(x+y))$ is strictly negative based on the expression given above. Thus, the first term on the R.H.S. of $\dfrac{d^2}{dx^2} w(p(x))$ is strictly positive. Next, since $\alpha \in (0, 1)$ and $0 < -\log(p(x+y)) < \infty$, the second term is positive.

Finally, since $p(\cdot)$ is twice-differentiable and log-convex with a convex domain $\mathbb{R}_{\geq 0}$, $(p(x+y))^2 \leq p(x+y)p(x+y)$ [52], which ensures that the third term is non-negative. Thus, $\frac{d^2}{dx^2}w(p(x+y))$ is strictly positive, and hence strictly convex in x.

ii) We prove this part also from the calculated second derivative of $w(p(x+y))$ (shown above). First, the third term on the RHS of (4.7) is non-negative (as argued in the previous case, by the fact that $p(\cdot)$ is twice-differentiable and log-convex). Now, we show that $\frac{p(x+y)\left(\frac{d}{dx}w(p(x+y))\right)}{w(p(x+y))} > \frac{(\alpha-1)(p(x+y))^2}{p(x+y)(-\log(p(x+y)))}$ when $\alpha \in \mathbb{R}_{>1}$ and $p(x+y) \leq \frac{1}{\mathrm{e}}$; this will then cause the first two terms on the RHS of (4.7) to together be positive, which will then yield $\frac{d^2}{dx^2}w(p(x+y)) > 0$.

First note from (4.7) that

$$\frac{p(x+y)\left(\frac{d}{dx}w(p(x+y))\right)}{w(p(x+y))} = \frac{\alpha(p(x+y))^2(-\log(p(x+y)))^{\alpha}}{p(x+y)(-\log(p(x+y)))}. \tag{4.8}$$

Moreover, we have

$$\begin{aligned} p(x+y) \leq \frac{1}{\mathrm{e}} &\iff -\log(p(x+y)) \geq 1 \\ &\implies \alpha(-\log(p(x+y)))^{\alpha} > \alpha - 1. \end{aligned}$$

Together with (4.8), we have

$$\frac{p(x+y)\left(\frac{d}{dx}w(p(x+y))\right)}{w(p(x+y))} > \frac{(\alpha-1)(p(x+y))^2}{p(x+y)(-\log(p(x+y)))}.$$

Thus, $\frac{d^2}{dx^2}w(p(x+y)) > 0$ and therefore $w(p(x+y))$ is strictly convex in the investment x. □

Based on the above result, we will make the following assumption throughout the rest of the chapter.

Assumption 5. *At least one of the following conditions holds.*

i. For all $D_k \in \mathcal{D}$, $\alpha_k \in (0,1]$.

ii. For all $v_{\mathrm{i}} \in V$, $p_{\mathrm{i}}(x_{\mathrm{i}}^T) \leq \frac{1}{\mathrm{e}}$, $\forall x_{\mathrm{i}}^T \in [0, \infty)$.

We now have the following corollary of Lemma 5.

Corollary 1. *Consider any player* $D_k \in \mathcal{D}$. *For all* $\alpha_k \in (0, \infty)$ *and under Assumptions 4 and 5, the problem of minimizing the cost function (4.5) over the set* X_k *in (4.1) is convex in the investment* $\mathbf{x}_k$, *for any given investment vector* $\mathbf{x}_{-k}$ *by other players.*

Proof. Recall that the investment vector of all players other than D_k is given by $\mathbf{x}_{-k} = [y_1, y_2, \ldots, y_n]$. By Lemma 5, each term in $C_k(\mathbf{x}_k, \mathbf{x}_{-k})$ (in (4.5)) is strictly convex in a different variable x_{i}^k. Since the cost function is separable in the variables $x_1^k, x_2^k, \ldots, x_n^k$, $C_k(\mathbf{x}_k, \mathbf{x}_{-k})$ is convex in $\mathbf{x}_k$ for any given investment vector $\mathbf{x}_{-k}$. Finally, the result follows by noting that the constraint set X_k, as defined in (4.1), is convex. □

We can now establish the existence of a Pure Strategy Nash Equilibrium (PNE) for the class of behavioral games defined in Section 4.4.

Proposition 4.5.1. *Under Assumptions 4 and 5, the Multi-Target Behavioral CPR Game possesses a pure strategy Nash equilibrium (PNE) when* $\alpha_k \in (0, \infty)$ *for each player* D_k.

The proof follows directly by noting from Corollary 1 that the Multi-Target Behavioral CPR Game is an instance of *concave games*, which always have a PNE [54].

4.6 Properties of the PNE

Having established the existence of one or more PNE in the Multi-Target Behavioral CPR Game, we now turn our attention to characterizing properties of the equilibria. We start with some useful properties of the marginals of the cost function (4.5) for each player.

4.6.1 Properties of the Marginals

Lemma 6. *Consider any player* $D_k \in \mathcal{D}$. *Under Assumption 4 and Assumption 5, for all* $\alpha_k \in (0, \infty)$, *for all* $v_{\mathrm{i}} \in V$, *and for all* $y_{\mathrm{i}} \in \mathbb{R}_{\geq 0}$ *the marginal* $\frac{dw_k(p_{\mathrm{i}}(x+y_{\mathrm{i}}))}{dx}$ *is negative, continuous, and increasing to* 0 *in* x.

Proof. Consider the expression for $\frac{dw_k(p_{\mathrm{i}}(x+y_{\mathrm{i}}))}{dx}$ given by (4.6). This function is strictly negative (since $p_{\mathrm{i}}(x+y_{\mathrm{i}})$ is strictly negative and $-\log(p_{\mathrm{i}}(x+y))$ is strictly positive). Furthermore it is continuous and increasing in x, since $w_k(p_{\mathrm{i}}(x+y_{\mathrm{i}}))$ is strictly convex as shown in Lemma 5, and hence $\frac{d}{dx}(\frac{dw_k(p_{\mathrm{i}}(x+y_{\mathrm{i}}))}{dx}) > 0$. To show that the marginal goes to zero as $x \to \infty$, we note that

$$\lim_{x\to\infty}\left|\frac{dw_k(p_{\mathrm{i}}(x+y_{\mathrm{i}}))}{dx}\right| = \lim_{x\to\infty}\left|\alpha_k(-\log(p_{\mathrm{i}}(x+y_{\mathrm{i}})))^{\alpha_k-1}w_k(p_{\mathrm{i}}(x+y_{\mathrm{i}}))\right|\left|\frac{p_{\mathrm{i}}(x+y)}{p_{\mathrm{i}}(x+y)}\right| = 0,$$

since $p_{\mathrm{i}}(x+y_{\mathrm{i}}) \to 0$ as $x \to \infty$ (which means $w_k(p_{\mathrm{i}}(x+y_{\mathrm{i}})) \to 0$ and $-\log(p_{\mathrm{i}}(x+y_{\mathrm{i}})) \to \infty$), and $\frac{p_{\mathrm{i}}(x+y_{\mathrm{i}})}{p_{\mathrm{i}}(x+y_{\mathrm{i}})}$ is bounded by Assumption 4. □

We will also use this straightforward property of the investments at any PNE.

Lemma 7. *Consider a set of players $\mathcal{D}$ and a set of n assets V, under Assumption 4 and Assumption 5. Consider a PNE $\mathbf{x}^*$, and let the total investment vector on each node under that PNE be given by $\mathbf{x}^{*T} = \begin{bmatrix} x_1^{*T} & x_2^{*T} & \dots & x_n^{*T}\end{bmatrix}^\intercal$. Then, for every player $D_k \in \mathcal{D}$, for each pair of nodes v_{i} and v_{j}:*

i. If D_k has nonzero investments in both of v_{i} and v_{j} at the PNE, then the marginals satisfy $L_{\mathrm{i}}^k \frac{dw_k(p_{\mathrm{i}}(x))}{dx}\Big|_{x=x_{\mathrm{i}}^{*T}} = L_{\mathrm{j}}^k \frac{dw_k(p_{\mathrm{j}}(x))}{dx}\Big|_{x=x_{\mathrm{j}}^{*T}}$.

ii. If D_k has a nonzero investment on v_{i} but a zero investment in v_{j} at the PNE, then the marginals would satisfy $L_{\mathrm{i}}^k \frac{dw_k(p_{\mathrm{i}}(x))}{dx}\Big|_{x=x_{\mathrm{i}}^{*T}} \leq L_{\mathrm{j}}^k \frac{dw_k(p_{\mathrm{j}}(x))}{dx}\Big|_{x=x_{\mathrm{j}}^{*T}}$.

The above result follows by noting that if the given conditions are not satisfied, then player D_k can reduce their perceived cost (4.5) by transferring a small amount of their investment from one of the assets to the other. This would contradict the fact that the player is playing her best response at the PNE.

We now show some properties of the PNE. First, we show the uniqueness of the total investments at all PNEs.

4.6.2 Uniqueness of Total Investments at the PNE

Proposition 4.6.1. *Consider a set of players $\mathcal{D}$ and a set of n assets V, under Assumption 4 and Assumption 5. Then, the total investment in each asset is unique for all PNEs.*

Proof. Suppose by way of contradiction that there are two different PNEs $\mathbf{x}^*$ and $\bar{\mathbf{x}}$ with two different total investment vectors $\mathbf{x}^{*T}$ and $\bar{\mathbf{x}}^T$. Define

$$\mathcal{H} = \left\{ v_{\mathrm{i}} \in V \mid x_{\mathrm{i}}^{*T} > \bar{x}_{\mathrm{i}}^T \right\}$$

to be the set of assets that have a larger total investment in PNE $\mathbf{x}^*$ than in PNE $\bar{\mathbf{x}}$. Let $\mathcal{D}_{\mathcal{H}} \subseteq \mathcal{D}$ be the set of players that have invested a nonzero amount in at least one asset in $\mathcal{H}$ in the PNE $\mathbf{x}^*$. We now argue that each player in $\mathcal{D}_{\mathcal{H}}$ must have invested zero in all assets in $V \setminus \mathcal{H}$ in the PNE $\bar{\mathbf{x}}$.

To show this, suppose there is a player $D_k \in \mathcal{D}_{\mathcal{H}}$ that has invested a nonzero amount in some asset $v_{\mathrm{j}} \in V \setminus \mathcal{H}$ in the PNE $\bar{\mathbf{x}}$. Then, from Lemma 7, we have

$$L_{\mathrm{i}}^k \frac{dw_k(p_{\mathrm{i}}(x))}{dx}\bigg|_{x=\bar{x}_{\mathrm{i}}^T} \geq L_{\mathrm{j}}^k \frac{dw_k(p_{\mathrm{j}}(x))}{dx}\bigg|_{x=\bar{x}_{\mathrm{j}}^T}$$

for all assets $v_{\mathrm{i}} \in \mathcal{H}$. Since $x_{\mathrm{i}}^{*T} > \bar{x}_{\mathrm{i}}^T$, and $x_{\mathrm{j}}^{*T} \leq \bar{x}_{\mathrm{j}}^T$ (from the definition of the set $\mathcal{H}$), and since the marginal for each node is increasing in the total investment in that node, we have

$$\begin{aligned} L_{\mathrm{i}}^k \frac{dw_k(p_{\mathrm{i}}(x))}{dx}\bigg|_{x=x_{\mathrm{i}}^{*T}} &> L_{\mathrm{i}}^k \frac{dw_k(p_{\mathrm{i}}(x))}{dx}\bigg|_{x=\bar{x}_{\mathrm{i}}^T} \\ &\geq L_{\mathrm{j}}^k \frac{dw_k(p_{\mathrm{j}}(x))}{dx}\bigg|_{x=\bar{x}_{\mathrm{j}}^T} \\ &\geq L_{\mathrm{j}}^k \frac{dw_k(p_{\mathrm{j}}(x))}{dx}\bigg|_{x=x_{\mathrm{j}}^{*T}}. \end{aligned}$$

However, this contradicts the fact that $D_k \in \mathcal{D}_{\mathcal{H}}$ has invested in asset v_{i} in the PNE $\mathbf{x}^*$ (since the above expressions state that asset $v_{\mathrm{j}} \in V \setminus \mathcal{H}$ has a lower marginal than asset $v_{\mathrm{i}} \in \mathcal{H}$ in the PNE $\mathbf{x}^*$). Thus, in the PNE $\bar{\mathbf{x}}$, each player in $\mathcal{D}_{\mathcal{H}}$ only invests in nodes in $\mathcal{H}$.

Thus, the sum of the investments in nodes in $\mathcal{H}$ in the PNE $\bar{\mathbf{x}}$ is at least $\sum_{D_k \in \mathcal{D}_{\mathcal{H}}} B_k$. However, the sum of the investments in nodes in $\mathcal{H}$ in the PNE $\mathbf{x}^*$ is at most $\sum_{D_k \in \mathcal{D}_{\mathcal{H}}} B_k$, since $\mathcal{D}_{\mathcal{H}}$ is the set of all players that have a nonzero investment in nodes in $\mathcal{H}$ in the PNE $\mathbf{x}^*$. This indicates that the sum of the investments in the nodes in $\mathcal{H}$ in the PNE $\bar{\mathbf{x}}$ is at least as large as the sum of the investments in the nodes in $\mathcal{H}$ in the PNE $\mathbf{x}^*$. However, this contradicts the fact that the total investment in each node in $\mathcal{H}$ in the PNE $\mathbf{x}^*$ is greater than the total investment in that node in the PNE $\bar{\mathbf{x}}$. Thus, it must be that the set $\mathcal{H}$ is empty, when then shows that the total investment in each node must be the same under both PNEs. □

The above result shows that the total investments are unique at any PNE. In other words, each asset $v_{\mathrm{i}} \in V$ has the same total investments, $x_{\mathrm{i}}^{T^*}$, at any PNE.

Remark 7. Note that the investments by each player can be different at any PNE but with the property that the total investments (i.e., the summation of all players' investments) on each asset is the same at any PNE. ■

After showing the uniqueness of the total investments at any PNE, we will make the following assumption to show additional properties at the PNE.

Assumption 6. *The players share the same ordering of assets (i.e., $L_1^k > L_2^k > \cdots > L_n^k$) for every player $D_k \in \mathcal{D}$. Furthermore, the probabilities of failure satisfy $p_1(x) = p_2(x) = \cdots = p_n(x) = p(x)$, where $p(x)$ satisfies Assumption 4.*

As we will see, interesting phenomena arise even under the above assumption of identical probability functions at each node (note that failure of each node is still independent of failure of any other node, and only depends on the amount of investment on that node).

4.6.3 Ordering of Total Investments at PNE

We now show that the total investments at any PNE are non-increasing in the asset index (i.e., an asset with higher loss would have higher total investment at any PNE compared to an asset with lower loss).

Proposition 4.6.2. *Consider a set of players $\mathcal{D}$ and a set of n assets satisfying Assumption 6. Consider a PNE $\mathbf{x}^{\mathbf{T}^*}$, denoted $\mathbf{x}^{\mathbf{T}^*} = \begin{bmatrix} x_1^{T^*} & x_2^{T^*} & \dots & x_n^{T^*} \end{bmatrix}^\intercal$. Then, $\mathbf{x}^{\mathbf{T}^*}$ has the property that $x_1^{T^*} \geq x_2^{T^*} \geq \cdots \geq x_n^{T^*}$.*

Proof. We prove this result by contradiction. Suppose that there exists two assets v_{i} and v_{j} with $\mathrm{i} < \mathrm{j}$ where $x_{\mathrm{i}}^{T^*} < x_{\mathrm{j}}^{T^*}$. Then, there must exist a player $D_k \in \mathcal{D}$ who has invested less in v_{i} than in v_{j}. From Lemma 6, since the marginal is increasing in the total investment x, the marginal of asset v_{i} would be more negative compared to the marginal of asset v_{j} for defender D_k. Formally, we have

$$L_{\mathrm{i}}^k \frac{dw(p_{\mathrm{i}}(x))}{dx}\bigg|_{x=x_{\mathrm{i}}^{T^*}} < L_{\mathrm{j}}^k \frac{dw(p_{\mathrm{j}}(x))}{dx}\bigg|_{x=x_{\mathrm{j}}^{T^*}},$$

However, since $\mathbf{x}^{\mathbf{T}^*}$ is a PNE, from Lemma 7 the marginals must satisfy

$$L_{\mathrm{i}}^k \frac{dw(p_{\mathrm{i}}(x))}{dx}\bigg|_{x=x_{\mathrm{i}}^{T^*}} \geq L_{\mathrm{j}}^k \frac{dw(p_{\mathrm{j}}(x))}{dx}\bigg|_{x=x_{\mathrm{j}}^{T^*}},$$

for the player $D_k \in \mathcal{D}$ since she invested in v_{j} (with equality if she puts non-zero investments in both of assets v_{i} and v_{j}) which yields a contradiction. □

The above result shows that at the PNE the players will invest more in higher-valued assets (and this is true for all α and $p(x)$ satisfying Assumption 5).

4.7 Impact of Probability Weighting on the PNE

In this section, we study the impact of probability weighting on the PNE investments.

To gain further insights into the PNE investments of multiple players, we can leverage Lemma 6 to introduce the following quantities for each player D_k.

Definition 4.7.1. *Suppose the nodes satisfy Assumption 6. For all $\mathrm{i} \in \{1, 2, \dots, n\}$ and $\mathrm{j} \in \{1, 2, \dots, n\}$ with $\mathrm{i} < \mathrm{j}$, define the quantity $x_{\mathrm{ij}k}^* \in \mathbb{R}_{\geq 0}$ for player D_k to be such that*

$$L_{\mathrm{i}}^k \frac{dw(p_{\mathrm{i}}(x))}{dx}\bigg|_{x=x_{\mathrm{ij}k}^*} = L_{\mathrm{j}}^k \frac{dw(p_{\mathrm{j}}(x))}{dx}\bigg|_{x=0}. \tag{4.9}$$

We will use the notation $x^*_{ijk}(\alpha_k)$ when needed to explicitly indicate the dependence of x^*_{ijk} on α_k.

Note that by Lemma 6, the quantity x^*_{ijk} exists and is unique for each $i < j$. Based on the above definition, we now present the following result.

Proposition 4.7.1. *Under Assumption 6, consider a PNE $\mathbf{x}^{\mathbf{T}^*}$. If $x_i^{T^*} > x^*_{ijk} \forall i \in \{1, \ldots, j-1\}$ and $y^*_j < x^*_{j(j+1)k}$, then a player $D_k \in \mathcal{D}$ would put nonzero investment on asset v_j.*

Proof. Suppose that $x_i^{T^*} > x^*_{ijk} \forall i \in \{1, \ldots, j-1\}$ and $y^*_j < x^*_{j(j+1)k}$, and suppose by way of contradiction that the player D_k puts zero investment on the asset v_j. Now, since $x_i^{T^*} > x^*_{ijk} \forall i \in \{1, \ldots, j-1\}$, we have (from Lemma 6 and Definition 4.7.1)

$$L_i^k \frac{dw_k(p_i(x))}{dx}\bigg|_{x=x_i^{T^*}} > L_j^k \frac{dw_k(p_j(x))}{dx}\bigg|_{x=0}.$$

Now, since $y^*_j < x^*_{j(j+1)k}$ and since D_k puts zero investment on the asset v_j, we have $x_j^{T^*} < x^*_{j(j+1)k}$. Therefore, from Definition 4.7.1, we have

$$L_j^k \frac{dw_k(p_j(x))}{dx}\bigg|_{x=x_j^{T^*}} < L_{j+1}^k \frac{dw_k(p_{j+1}(x))}{dx}\bigg|_{x=0}.$$

From Assumption 3, we have

$$L_{j+1}^k \frac{dw_k(p_{j+1}(x))}{dx}\bigg|_{x=0} < L_j^k \frac{dw_k(p_j(x))}{dx}\bigg|_{x=0}.$$

Therefore, we have

$$L_i^k \frac{dw_k(p_i(x))}{dx}\bigg|_{x=x_i^{T^*}} > L_j^k \frac{dw_k(p_j(x))}{dx}\bigg|_{x=x_j^{T^*}}.$$

which yields a contradiction with Lemma 7 (case ii). □

The above result shows that the investment decision of any player D_k to put investments on an asset v_j depends on the PNE total investments by all players on all assets v_i with lower index than v_j (i.e., with $i < j$). Moreover, the above results held irrespective of the particular

value of α_k. Recall that α_k controlled the extent of underweighting and overweighting in the Prelec probability weighting function (4.3) (see Fig. 4.1).

We now study the impact of probability weighting on the PNE investments (i.e., how the investments change as α_k changes).

Lemma 8. *Suppose Assumption 6 holds, and let* $p(0) \leq \frac{1}{\mathrm{e}}$. *Then,* $\forall \mathrm{i} \in \{1, \ldots, n\}$ *and* $\mathrm{j} \in \{1, \ldots, n\}$ *with* $\mathrm{i} < \mathrm{j}$, *the quantity* $x^*_{\mathrm{ij}k}(\alpha_k)$ *is decreasing in* α_k *for any* $\alpha_k \in \mathbb{R}_{>0}$.

Proof. For ease of notation, we remove the index k in α_k and w_k in the following analysis.

For a player D_k, from Definition 4.7.1, the value of $x^*_{\mathrm{ij}k}(\alpha)$ is given by (4.9) for all $\mathrm{i} < \mathrm{j}$. Since that the perceived expected loss at node v_{i} is given by $L^k_{\mathrm{i}} w(p_{\mathrm{i}}(x))$, differentiating (3.3) with respect to the player's investment in that node, we obtain

$$L^k_{\mathrm{i}} \tfrac{dw(p_{\mathrm{i}}(x))}{dx} = \alpha L^k_{\mathrm{i}} (-\log(p_{\mathrm{i}}(x)))^{\alpha-1} w(p_{\mathrm{i}}(x)) \frac{p_{\mathrm{i}}(x)}{p_{\mathrm{i}}(x)}. \tag{4.10}$$

Using the expression for the marginals given by (4.10), and noting that $p_{\mathrm{i}}(x) = p_{\mathrm{j}}(x) = p(x)$ from Assumption 6, from (4.9) $x^*_{\mathrm{ij}k}(\alpha)$ satisfies the equation

$$L^k_{\mathrm{i}} (-\log\Big(p(x^*_{\mathrm{ij}k}(\alpha))\Big))^{\alpha-1} w(p(x^*_{\mathrm{ij}k}(\alpha))) \frac{p(x^*_{\mathrm{ij}k}(\alpha))}{p(x^*_{\mathrm{ij}k}(\alpha))} = L^k_{\mathrm{j}} (-\log(p(0)))^{\alpha-1} w(p(0)) \frac{p(0)}{p(0)}. \tag{4.11}$$

In (4.11), taking the logarithm of both sides and differentiating yields that $\frac{dx^*_{\mathrm{ij}k}}{d\alpha}$ is given by:

$$\frac{dx^*_{\mathrm{ij}k}}{d\alpha} = \frac{\Big[\Big(-\log\Big(p(x^*_{\mathrm{ij}k})\Big)\Big)^{\alpha} - 1\Big] \log\Big(-\log\Big(p(x^*_{\mathrm{ij}k})\Big)\Big)}{z(x^*_{\mathrm{ij}k})} - \frac{[(-\log(p(0)))^{\alpha} - 1] \log(-\log(p(0)))}{z(x^*_{\mathrm{ij}k})}$$

where

$$z(x^*_{\mathrm{ij}k}) = \Big(\alpha - 1 - \alpha(-\log\Big(p(x^*_{\mathrm{ij}k})\Big))^{\alpha}\Big) \frac{p(x^*_{\mathrm{ij}k})}{p(x^*_{\mathrm{ij}k}) \log\Big(p(x^*_{\mathrm{ij}k})\Big)} + \frac{p(x^*_{\mathrm{ij}k}) p(x^*_{\mathrm{ij}k}) - (p(x^*_{\mathrm{ij}k}))^2}{p(x^*_{\mathrm{ij}k}) p(x^*_{\mathrm{ij}k})}.$$

From Assumption 4, we have $p(x^*_{\mathrm{ij}k}) < 0$, $\log\Big(p(x^*_{\mathrm{ij}k})\Big) < 0$ and $p(x)$ is log-convex, thus $p(x^*_{\mathrm{ij}k}) p(x^*_{\mathrm{ij}k}) - (p(x^*_{\mathrm{ij}k}))^2 \geq 0$. Moreover, note that $\alpha - 1 - \alpha(-\log\Big(p(x^*_{\mathrm{ij}k})\Big))^{\alpha}$ is negative in the following two cases i) if $\alpha \in (0, 1]$ ii) if $\alpha \in \mathbb{R}_{>1}$ and $p(x^*_{\mathrm{ij}k}) \leq \frac{1}{\mathrm{e}}$ (as shown earlier in the proof of Lemma 5). Thus, the denominator $z(x^*_{\mathrm{ij}k})$ of $\frac{dx^*_{\mathrm{ij}k}}{d\alpha}$ is negative.

Now, from Assumption 4 and the assumption that $p(0) \leq \frac{1}{\mathrm{e}}$, we have $-\log\Big(p(x^*_{\mathrm{ij}k})\Big) > 1$ and $-\log(p(0)) \geq 1$. Thus, we have $\log\Big(-\log\Big(p(x^*_{\mathrm{ij}k})\Big)\Big) > 0$ and $\log(-\log(p(0))) \geq 0$. Moreover, we have

$$\begin{aligned} x^*_{\mathrm{ij}k} > 0 &\iff p(x^*_{\mathrm{ij}k}) < p(0) \\ &\iff -\log\Big(p(x^*_{\mathrm{ij}k})\Big) > -\log(p(0)) \\ &\iff (-\log\Big(p(x^*_{\mathrm{ij}k})\Big))^{\alpha} > (-\log(p(0)))^{\alpha} \\ &\iff (-\log\Big(p(x^*_{\mathrm{ij}k})\Big))^{\alpha} - 1 > (-\log(p(0)))^{\alpha} - 1. \end{aligned}$$

Thus, the numerator of $\frac{dx^*_{\mathrm{ij}k}}{d\alpha}$ is positive and hence the derivative $\frac{dx^*_{\mathrm{ij}k}}{d\alpha}$ is negative, yielding that $x^*_{\mathrm{ij}k}(\alpha)$ is decreasing in α. □

The above result leads to the following key outcome, showing that if $p(0) \leq \frac{1}{\mathrm{e}}$, behavioral players will generally invest in fewer nodes at PNE than rational players (given the same budget).

Proposition 4.7.2. *Suppose Assumption 6 holds, and furthermore that $p(0) \leq \frac{1}{\mathrm{e}}$. Let $\boldsymbol{\alpha_1} \in \mathbb{R}^{|D|}_{>0}$ and $\boldsymbol{\alpha_2} \in \mathbb{R}^{|D|}_{>0}$ denote two different vectors of behavioral levels of the players, given by $\boldsymbol{\alpha_1} = [\alpha_1, \alpha_2, \cdots, \alpha_k, \cdots, \alpha_{|D|}]$ and $\boldsymbol{\alpha_2} = [\alpha_1, \alpha_2, \cdots, \bar{\alpha}_k, \cdots, \alpha_{|D|}]$, with $\alpha_k < \bar{\alpha}_k$ and $\boldsymbol{\alpha_1}(\mathrm{i}) = \boldsymbol{\alpha_2}(\mathrm{i}) \forall \mathrm{i} \neq k$. Then, the number of nodes that have positive total investment at PNE under $\boldsymbol{\alpha_2}$ is at least as large as those at PNE under $\boldsymbol{\alpha_1}$.*

Proof. As stated, consider two different behavioral level vectors $\boldsymbol{\alpha_1}$ and $\boldsymbol{\alpha_2}$, where all the players have the same behavioral levels in both vectors except an arbitrary player $D_k \in \mathcal{D}$ where $\alpha_k \in \mathbb{R}_{>0}$ and $\bar{\alpha}_k \in \mathbb{R}_{>0}$ represent the player D_k's behavioral level under $\boldsymbol{\alpha_1}$ and $\boldsymbol{\alpha_2}$, respectively and $\alpha_k < \bar{\alpha}_k$. Let $\{x^*_{\mathrm{ij}k}(\alpha_k)\}$ and $\{x^*_{\mathrm{ij}k}(\bar{\alpha}_k)\}$ be the corresponding sets of investment thresholds for each of those values of α for the arbitrary player D_k, given by Definition 4.7.1.

Suppose by way of contradiction that the number of assets that have positive total investment at PNE under $\alpha_{\boldsymbol{2}}$ is lower than the number of assets that have positive total investment at PNE under $\alpha_{\boldsymbol{1}}$. Now, let v_{j} be the last asset that has positive total PNE investment under $\alpha_{\boldsymbol{1}}$. Then, we have $x^{T^*}_{\mathrm{j}}(\alpha_{\boldsymbol{1}}) > 0$ and $x^{T^*}_{\mathrm{j}}(\alpha_{\boldsymbol{2}}) = 0$. Since the summation of

budgets of all players, denoted by $\sum_{D_k \in \mathcal{D}} B_k$ is fixed for both cases of $\alpha_{\mathbf{1}}$ and $\alpha_{\mathbf{2}}$, thus there must exist at least one asset v_{i} with $\mathrm{i} < \mathrm{j}$ in which the total PNE investment under $\alpha_{\mathbf{2}}$ is larger than the total PNE investment under $\alpha_{\mathbf{1}}$. In other words, we have $x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{2}}) > x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{1}})$ for that asset v_{i}.

From the fact that $x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{1}})$ is the total investment on the asset v_{i}, we have

$$x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{1}}) \geq x_{\mathrm{ij}k}^*(\alpha_{\mathbf{1}}). \tag{4.12}$$

Now, since $p(0) \leq \frac{1}{\mathrm{e}}$ and $\alpha_k < \bar{\alpha}_k$, from Lemma 8 we have

$$x_{\mathrm{ij}k}^*(\bar{\alpha}_k) < x_{\mathrm{ij}k}^*(\alpha_k) \iff x_{\mathrm{ij}k}^*(\alpha_2) < x_{\mathrm{ij}k}^*(\alpha_1) \tag{4.13}$$

Since we have $x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{2}}) > x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{1}})$ and using (4.12) and (4.13), we thus have

$$x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{2}}) > x_{\mathrm{ij}k}^*(\alpha_{\mathbf{2}}).$$

Therefore, comparing the marginals and using Definition 4.7.1 we have the following

$$\begin{aligned}
x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{2}}) > x_{\mathrm{ij}k}^*(\alpha_{\mathbf{2}}) \\
&\iff L_{\mathrm{i}}^k \frac{dw_k(p_{\mathrm{i}}(x))}{dx}\bigg|_{x=x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{2}})} > L_{\mathrm{i}}^k \frac{dw_k(p_{\mathrm{i}}(x))}{dx}\bigg|_{x=x_{\mathrm{ij}k}^*(\alpha_{\mathbf{2}})} \\
&\iff L_{\mathrm{i}}^k \frac{dw_k(p_{\mathrm{i}}(x))}{dx}\bigg|_{x=x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{2}})} > L_{\mathrm{j}}^k \frac{dw_k(p_{\mathrm{j}}(x))}{dx}\bigg|_{x=0} \\
&\iff L_{\mathrm{i}}^k \frac{dw_k(p_{\mathrm{i}}(x))}{dx}\bigg|_{x=x_{\mathrm{i}}^{T^*}(\alpha_{\mathbf{2}})} > L_{\mathrm{j}}^k \frac{dw_k(p_{\mathrm{j}}(x))}{dx}\bigg|_{x=x_{\mathrm{j}}^{T^*}(\alpha_{\mathbf{2}})},
\end{aligned}$$

which contradicts the case (ii) in Lemma 7 which yields a contradiction. Therefore, the number of assets that have positive total investment under $\alpha_{\mathbf{2}}$ is at least as large as the number of assets that have positive investment under $\alpha_{\mathbf{1}}$. □

The above result shows that at the PNE, behavioral players would choose to leave lower valued nodes vulnerable, and instead the total investments on the high-valued nodes would

be higher if $p(0) \leq \frac{1}{\mathrm{e}}$. This will have implications for the (true) expected loss faced by each player which will increase the total expected loss faced by all of the players. We illustrate the phenomenon identified by the above results and the resulting impact on the player's true loss in our numerical simulations in Section 4.8.

Now, we give a more general case that follows from the above result

Corollary 2. *Suppose Assumption 3 holds, and let* $p(0) \leq \frac{1}{\mathrm{e}}$. *Let* $\boldsymbol{\alpha_1} \in \mathbb{R}_{>0}^{|D|}$ *and* $\boldsymbol{\alpha_2} \in \mathbb{R}_{>0}^{|D|}$ *denote two different vectors of behavioral levels of the players, given by* $\boldsymbol{\alpha_1} = [\alpha_1^1, \alpha_2^1, \cdots, \alpha_k^1, \cdots, \alpha_{|D|}^1]$ *and* $\boldsymbol{\alpha_2} = [\alpha_1^2, \alpha_2^2, \cdots, \alpha_k^2, \cdots, \alpha_{|D|}^2]$, *with* $\boldsymbol{\alpha_1}(\mathrm{i}) \leq \boldsymbol{\alpha_2}(\mathrm{i}) \forall \mathrm{i}$. *Then, the number of assets that have positive total investment at PNE under* $\boldsymbol{\alpha_2}$ *is at least as large as those at PNE under* $\boldsymbol{\alpha_1}$.

The proof of the above general corollary follows directly from Proposition 4.7.2 by considering each corresponding players from the two groups at a time.

4.7.1 Homogeneous Behavioral Levels

We emphasize that the case in which all the players have homogeneous behavioral levels follows from the above result as shown below.

Proposition 4.7.3. *Under Assumption 6, and furthermore that* $p(0) \leq \frac{1}{\mathrm{e}}$. *Then, for any* $\alpha \in \mathbb{R}_{>0}$, *the number of nodes that have positive total investment at PNE is nondecreasing in* α.

Now, we present the effect of the behavioral probability weighting on the PNE total investment on highest valued asset.

Lemma 9. *Suppose Assumption 6 holds, and let* $p(0) \leq \frac{1}{\mathrm{e}}$. *Then,* $\forall \mathrm{i} \in \{1, \ldots, n\}$ *and* $\mathrm{j} \in \{1, \ldots, n\}$ *with* $\mathrm{i} < \mathrm{j}$, *if the total investment* $x_{\mathrm{j}}^{T^*}$ *is nonincreasing in* α, *then the total investment* $x_{\mathrm{i}}^{T^*}$ *is nonincreasing in* α *for any* $\alpha \in \mathbb{R}_{>0}$.

Proof. For any player $D_k \in \mathcal{D}$, from Lemma 7, $x_{\mathrm{i}}^{T^*}(\alpha)$ and $x_{\mathrm{j}}^{T^*}(\alpha)$ satisfies the inequality

$$L_{\mathrm{i}}^k \left(-\log\Big(p(x_{\mathrm{i}}^{T^*}(\alpha))\Big)\right)^{\alpha-1} w(p(x_{\mathrm{i}}^{T^*}(\alpha))) \frac{p(x_{\mathrm{i}}^{T^*}(\alpha))}{p(x_{\mathrm{i}}^{T^*}(\alpha))}$$

$$\leq L_{\mathrm{j}}^{k}\left(-\log\Big(p(x_{\mathrm{j}}^{T^*}(\alpha))\Big)\right)^{\alpha-1} w(p(x_{\mathrm{j}}^{T^*}(\alpha)))\frac{p(x_{\mathrm{j}}^{T^*}(\alpha))}{p(x_{\mathrm{j}}^{T^*}(\alpha))}.$$

Similar to the proof of Lemma 8, and with using the expression for the marginals given by (4.10), and noting that $p_{\mathrm{i}}(x) = p_{\mathrm{j}}(x) = p(x)$, taking the logarithm of both sides and differentiating yields that $\frac{dx_{\mathrm{i}}^{T^*}}{d\alpha}$ is given by:

$$\begin{aligned}\frac{dx_{\mathrm{i}}^{T^*}}{d\alpha} \leq & \frac{\left[\left(-\log\Big(p(x_{\mathrm{i}}^{T^*})\Big)\right)^{\alpha}-1\right]\log\Big(-\log\Big(p(x_{\mathrm{i}}^{T^*})\Big)\Big)}{z(x_{\mathrm{i}}^{T^*})} \\ & - \frac{\left[\left(-\log\Big(p(x_{\mathrm{j}}^{T^*})\Big)\right)^{\alpha}-1\right]\log\Big(-\log\Big(p(x_{\mathrm{j}}^{T^*})\Big)\Big)}{z(x_{\mathrm{i}}^{T^*})} \\ & + \frac{z(x_{\mathrm{j}}^{T^*})}{z(x_{\mathrm{i}}^{T^*})}\frac{dx_{\mathrm{j}}^{T^*}}{d\alpha}.\end{aligned}$$

where

$$z(x) = (\alpha - 1 - \alpha(-\log(p(x)))^{\alpha})\frac{p(x)}{p(x)\log(p(x))} + \frac{p(x)p(x) - (p(x))^2}{p(x)p(x)}.$$

Now, from Proposition 4.6.2, $x_{\mathrm{i}}^{T^*} \geq x_{\mathrm{j}}^{T^*}$. Thus, we have

$$\begin{aligned}x_{\mathrm{i}}^{T^*} \geq x_{\mathrm{j}}^{T^*} & \iff p(x_{\mathrm{i}}^{T^*}) \leq p(x_{\mathrm{j}}^{T^*}) \\ & \iff -\log\Big(p(x_{\mathrm{i}}^{T^*})\Big) \geq -\log\Big(p(x_{\mathrm{j}}^{T^*})\Big) \\ & \iff \Big(-\log\Big(p(x_{\mathrm{i}}^{T^*})\Big)\Big)^{\alpha} \geq \Big(-\log\Big(p(x_{\mathrm{j}}^{T^*})\Big)\Big)^{\alpha}.\end{aligned}$$

Moreover, since $x_{\mathrm{i}}^{T^*} \geq x_{\mathrm{j}}^{T^*}$, we have $\log\Big(-\log\Big(p(x_{\mathrm{i}}^{T^*})\Big)\Big) \geq \log\Big(-\log\Big(p(x_{\mathrm{j}}^{T^*})\Big)\Big)$. Thus, the summation of the first two terms of $\frac{dx_{\mathrm{i}}^{T^*}}{d\alpha}$ is nonpositive. Moreover, similar to the argument in the proof of Lemma 8, we have that both $z(x_{\mathrm{i}}^{T^*})$ and $z(x_{\mathrm{j}}^{T^*})$ are negative. Thus, $\frac{z(x_{\mathrm{j}}^{T^*})}{z(x_{\mathrm{i}}^{T^*})}$ is positive. Finally, since the total investment $x_{\mathrm{j}}^{T^*}$ is nonincreasing in α, we have $\frac{dx_{\mathrm{j}}^{T^*}}{d\alpha}$ is nonpositive, hence the derivative $\frac{dx_{\mathrm{i}}^{T^*}}{d\alpha}$ is nonpositive, yielding that $x_{\mathrm{i}}^{T^*}(\alpha)$ is nonincreasing in α. □

The above result shows that the nonincreasing nature of total PNE investment with players' behavioral level in an asset implies same nature for assets with higher losses. This is

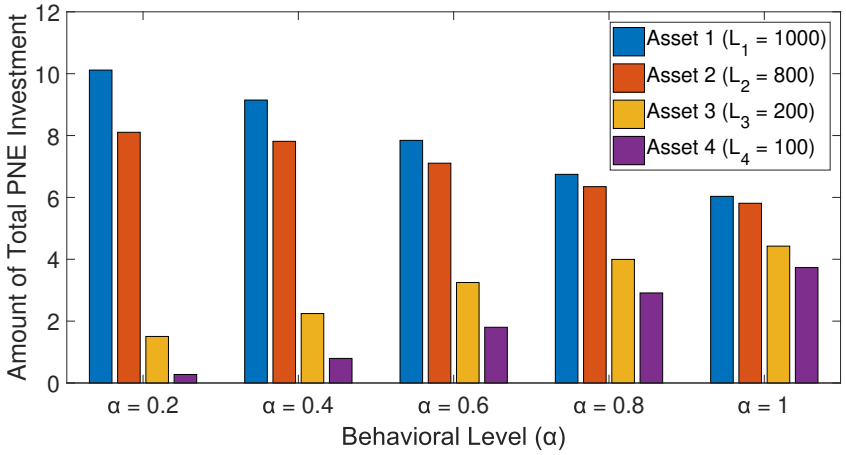


Figure 4.2. An example that illustrates Lemma 9. The highest two valued assets (Asset 1 and Asset 2) have higher total investments as the two players becomes more behavioral.

illustrated in Fig. 4.2, where the first two assets (with the highest losses) have nonincreasing PNE total investment with the behavioral level. In other words, since the second asset has nonincreasing nature of total investments with behavioral level, the first asset would have such nature as well.

To generate that figure, we consider two players with symmetric budgets ($B_1 = B_2 = 10$), and use $p_{\mathrm{i}}(x_{\mathrm{i}}^T) = \exp\Big(-x_{\mathrm{i}}^T - 1\Big)$. We then run the best response dynamics to reach the PNE.

Now, we provide the more explicit over-investment nature of total PNE investment on the highest valued asset as the player becomes more behavioral.

Proposition 4.7.4. *Under Assumption 6, and furthermore that* $p(0) \leq \frac{1}{\mathrm{e}}$. *Then, the total investment of the highest valued asset, denoted by* v_1, *at the PNE is decreasing in the behavioral level* $\alpha \in \mathbb{R}_{>0}$.

Proof. Consider a PNE $\mathbf{x}^{\mathbf{T}^*}$, denoted $\mathbf{x}^{\mathbf{T}^*} = \begin{bmatrix} x_1^{T^*} & x_2^{T^*} & \dots & x_n^{T^*} \end{bmatrix}^{\intercal}$. Suppose by way of contradiction that the total investment of the highest valued asset v_1 at PNE, dentoed by $x_1^{T^*}$, is non decreasing in α. Then, for any two groups of behavioral players with two behavioral levels α_1 and α_2, with $\alpha_1 < \alpha_2$, we have

$$x_1^{T^*}(\alpha_1) \leq x_1^{T^*}(\alpha_2).$$

Since the summation of budgets of all players, denoted by $\sum_{D_k \in \mathcal{D}} B_k$ is fixed for both groups of α_1 and α_2. Then, there must exist an asset v_{j} with $\mathrm{j} > 1$ where we have

$$x_{\mathrm{j}}^{T^*}(\alpha_1) \geq x_{\mathrm{j}}^{T^*}(\alpha_2).$$

Therefore, now we have $x_{\mathrm{j}}^{T^*}$ nonincreasing in α and $x_1^{T^*}$ nondecreasing in α, with $\mathrm{j} > 1$, which contradicts Lemma 9, which concludes proof. □

We finalize the analysis in this section by providing the following corollary that shows that behavioral players under-invest on the last asset (with the lowest loss) in the PNE.

Corollary 3. *Under Assumption 6, , and let $p(0) \leq \frac{1}{\mathrm{e}}$. Then, there exists one asset v_{j} with $\mathrm{j} > 1$ where the total PNE investment on that asset, denoted by $x_{\mathrm{j}}^{T^*}$, is nondecreasing in the behavioral level $\alpha \in \mathbb{R}_{>0}$.*

The above result follows from Proposition 4.7.3 and Proposition 4.7.4 by noting that the total budget of all players under any behavioral level is fixed.

4.7.2 Heterogeneity vs. Homogeneity of Behavioral Levels

We devote this subsection to studying the effects of heterogeneity in behavioral levels, while keeping the number of players fixed. Specifically, we investigate how a heterogeneous society compares to its homogeneous counterpart. Specifically, we study heterogeneity in the behavioral levels effect on the social cost (which is the sum of all true costs of the players).

Example 4. In this example, we show that when players have identical loss values, heterogeneity in the behavioral level α can result in either a decrease or an increase in the social cost compared to players with homogeneous behavioral levels (i.e., $\alpha_1 = \alpha_2 = \cdots = \alpha_n$).

Consider a Multi-Target behavioral CPR game with $n = 3$ players and the mean of the three heterogeneous behavioral level values is α (which is the homogeneous behavioral level). Let the probability of failure function on asset v_{i} be given by $p(x_{\mathrm{i}}^T) = \exp\Big(-x_{\mathrm{i}}^T - 1\Big)$. The loss values of the players are chosen to be the same with values $L_1^k = 500$ and $L_2^k = 250$,

for $k \in \{1, 2, 3\}$. Each player has a symmetric budget of 5. In Table 4.1, we give two numerical examples of games for which the social cost could either increase or decrease with heterogeneity in α when compared to a game where α homogeneous across players. We show that social cost increases as players become heterogeneous in their behavioral levels. On the contrary, under different behavioral levels (with the same $p(x_{\mathrm{i}}^T)$ and loss values as above), social cost decreases with heterogeneity in α_{i}.

The insight here is that the social cost would increase if there are more behavioral players with $\alpha_{\mathrm{i}} < \alpha$. Thus, they shift more investments to the highly valued asset. By contrast, if there are more less behavioral players (with $\alpha_{\mathrm{i}} > \alpha$), they would invest better in the remaining assets keeping the social cost better than the homogeneous case.

Table 4.1. Social cost and total investments under heterogeneity in the behavioral level parameter α. We give two numerical examples of games for which the social cost could either decrease (second row) or increase (fourth row) with heterogeneity in α when compared to a game where α is homogeneous among players and is the mean of the heterogeneous values. In all of the examples in the table, $p(x_{\mathrm{i}}^T) = \exp\big(-x_{\mathrm{i}}^T - 1\big)$ and the loss values of the players are chosen to be the same with values $L_1^k = 500$ and $L_2^k = 250$, for $k \in \{1, 2, 3\}$. Each player has a symmetric budget of 5.

Behavioral Levels (α_{i})	x_1^T	x_2^T	Social Cost
$\alpha_1 = \alpha_2 = \alpha_3 = 0.4$	9.3884	5.6116	2.8680
$\alpha_1 = \alpha_2 = 0.6$ $\alpha_3 = 0.001$	8.6452	6.3548	1.5677
$\alpha_1 = \alpha_2 = \alpha_3 = 0.4$	9.3884	5.6116	2.8680
$\alpha_1 = 1$ $\alpha_2 = 0.2$ $\alpha_3 = 0.001$	9.9984	5.0016	5.1138

4.7.3 Training Policy for enhancing behavioral decision-making

We now investigate how to enhance behavioral decision-making in a community of behavioral players. Specifically, we assume that this training is translated into a total limited budget of α that can be used to decrease behavioral level (i.e., increase α) of a subset or all the players. Indeed, there are multiple training policies that can be used with such budget of α. We compare several different possible training policies in Table 4.2 and show their effect on the social cost. This can give an insight about which policy can be more efficient (i.e., gives higher reduction in the social cost of the community).

Example 5. Consider a Multi-Target behavioral CPR game with $n = 4$ players with different behavioral levels with $\alpha_1 = 0.2$, $\alpha_2 = 0.4$, $\alpha_3 = 0.6$, and $\alpha_4 = 0.8$. Let the probability of failure function on asset v_i be given by $p(x_\mathrm{i}^T) = \exp\Big(-x_\mathrm{i}^T - 1\Big)$. The loss values of the players are chosen to be the same with values $L_1^k = 5000$ and $L_2^k = 2500$, for $k \in \{1, 2, 3, 4\}$. Each player has a symmetric budget of 2.5. In Table 4.2, we give the several possible training policies with their corresponding investments and social cost. We observe that the most effective training policy (i.e., the one with the lowest social cost) is training the least two behavioral players to be rational. On the other hand, training the most two behavioral players to have moderate behavioral decision-making while keeping the other players without training is not effective.

The insight here is that the existence of more than one rational player make the assets more secure since these rational players would invest properly on the assets that behavioral players under-invest on (i.e., they shifts most of their investments to the lower valued asset that the behavioral players do not allocate their resources on due to their cognitive bias). As a result, the social cost would decrease. On the contrary, if there are more behavioral players, they would over-invest in the highest valued asset keeping the lowest valued asset less protected which increases the social cost as shown in the other policies.

4.8 Numerical Simulations

In this section, we illustrate our theoretical findings via numerical simulations.

4.8.1 Effect of Perception on Investments

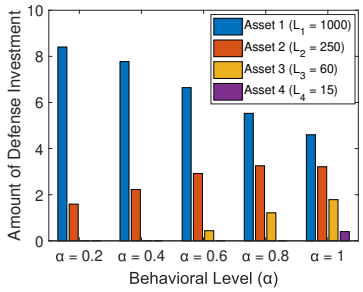
In this subsection, we show the effects of probability misperception identified in the previous sections on the investment decisions in the Multi-Target Behavioral CPR Game. In this context, consider a setting with four critical assets (or targets). We consider two players with symmetric losses on the assets (i.e., $L_\mathrm{i}^1 = L_\mathrm{i}^2 = L_\mathrm{i} \forall \mathrm{i} \in \{1, 2, 3, 4\}$).[2] The first asset has very high loss (i.e., $L_1 = 1000$) while the second, third, and fourth assets have

[2]↑Note that all of our results and simulations follows for the case in which the players have different loss valuations as long as they share the same ordering given in Assumption 6.

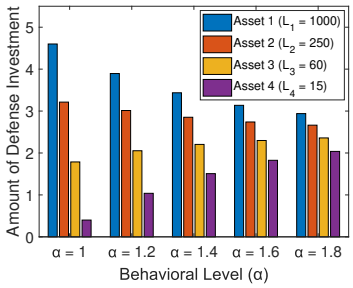
Table 4.2. Social cost and total investments under different training policies where the total available budget of α for training is 0.6. The loss values of the players are chosen to be the same with values $L_1^k = 5000$ and $L_2^k = 2500$, for $k \in \{1, 2, 3, 4\}$. Each player has a symmetric budget of 2.5.

Behavioral Levels (α_i)	x_1^T	x_2^T	Social Cost
[0] The base case (without any training) $\boldsymbol{\alpha} = \begin{bmatrix} 0.2 & 0.4 & 0.6 & 0.8 \end{bmatrix}$	5.9602	4.0398	83.655
[1] Train all players by equal amount $\boldsymbol{\alpha} = \begin{bmatrix} \mathbf{0.35} & \mathbf{0.55} & \mathbf{0.75} & \mathbf{0.95} \end{bmatrix}$	5.6646	4.3354	73.684
[2] Train the most behavioral player only $\boldsymbol{\alpha} = \begin{bmatrix} \mathbf{0.8} & 0.4 & 0.6 & 0.8 \end{bmatrix}$	5.5848	4.4152	72.109
[3] Train the two moderate behavioral only $\boldsymbol{\alpha} = \begin{bmatrix} 0.2 & \mathbf{0.8} & \mathbf{0.8} & 0.8 \end{bmatrix}$	5.5847	4.4153	72.107
[4] Train the highest two behavioral only $\boldsymbol{\alpha} = \begin{bmatrix} \mathbf{0.6} & \mathbf{0.6} & 0.6 & 0.8 \end{bmatrix}$	5.9600	4.0400	83.719
[5] Training the least two behavioral only $\boldsymbol{\alpha} = \begin{bmatrix} 0.2 & 0.4 & \mathbf{1} & \mathbf{1} \end{bmatrix}$	5.3465	4.6535	**70.109**
[6] Train the second most behavioral only $\boldsymbol{\alpha} = \begin{bmatrix} 0.2 & \mathbf{1} & 0.6 & 0.8 \end{bmatrix}$	5.5848	4.4152	72.109
[7] Train the most and the least behavioral $\boldsymbol{\alpha} = \begin{bmatrix} \mathbf{0.6} & 0.4 & 0.6 & \mathbf{1} \end{bmatrix}$	5.9602	4.0398	83.655
[8] Train most and second least behavioral $\boldsymbol{\alpha} = \begin{bmatrix} \mathbf{0.5} & 0.4 & \mathbf{0.9} & 0.8 \end{bmatrix}$	5.5848	4.4152	72.109
[9] Train least and second most behavioral $\boldsymbol{\alpha} = \begin{bmatrix} 0.2 & \mathbf{0.8} & 0.6 & \mathbf{1} \end{bmatrix}$	5.5848	4.4152	72.109
[10] Train most three behavioral players $\boldsymbol{\alpha} = \begin{bmatrix} \mathbf{0.5} & \mathbf{0.6} & \mathbf{0.7} & 0.8 \end{bmatrix}$	5.7541	4.2459	76.011

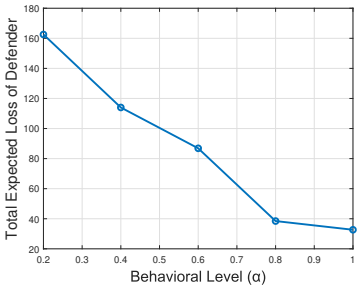
progressively lower losses (with $L_2 = 250$, $L_3 = 60$, and $L_4 = 15$). The PNE investments in the following scenarios were calculated using Matlab CVX toolbox [56]. We let the total budget for protecting the four critical assets for each player be $B_1 = B_2 = 5$. The probability of failure on each of the assets is given by $p(x) = \mathrm{e}^{-x-1}$ where x is the investment on that asset. The above function satisfies the conditions in Assumption 4.



(a) The effect of inverse S-shape behavioral probability weighting on total investments on four assets. The asset with the highest loss takes a higher portion of the investments as the players becomes more behavioral (α decreases). Moreover, the number of assets with positive investment decreases as the players becomes more behavioral.



(b) The effect of behavioral probability weighting on the total investments for S-shape probability weighting. The asset with the highest loss takes a less portion of the investments as the players becomes more behavioral (i.e., α increases). Moreover, the non-increasing order of assets' investments is kept as the players becomes more behavioral.



(c) The effect of behavioral probability weighting on the true expected loss of each player. The true expected loss of the player is higher as the players becomes more behavioral. In particular, the true expected loss of two highly behavioral players (with $\alpha_1 = \alpha_2 = 0.2$) is approximately 3.15 times that for the rational players (with $\alpha_1 = \alpha_2 = 1$).

Figure 4.3. The effect of behavioral bias on total investments on each node (asset) and the resulting player's (true) cost.

Effect of inverse S-shape probability weighting

Fig. 4.3a shows the difference in the total investment for each of the assets as α changes for the players. These plots illustrate the phenomena identified in Propositions 4.6.2 and 4.7.2. First, for each value of α, the total investments are ordered by the value of the assets. Second, as α gets smaller (i.e., the player becomes more behavioral), the investments are shifted to a smaller number of higher-valued assets. For example, two rational players (with $\alpha_1 = \alpha_2 = 1$) have nonzero total investments on all of the four assets, two behavioral players (with $\alpha_1 = \alpha_2 = 0.6$) put nonzero total investments on the first three assets, and two highly behavioral players (with $\alpha_1 = \alpha_2 = 0.4$) put nonzero total investments only on the first two assets.

Effect of S-shape probability weighting

We repeat the above experiments while letting α_k range in the domain of S-shaped probability weighting (i.e., $\alpha_k > 1$). As α gets higher (i.e., the players becomes more behavioral), a portion of the investments are shifted from the asset with the highest loss to the assets with lower losses. For instance, as shown in Fig. 4.3b, two highly behavioral players (with $\alpha_1 = \alpha_2 = 1.8$) put higher total investments on all of the second to fourth assets compared to two rational players (with $\alpha_1 = \alpha_2 = 1$). Note that the ordering of investments is also unchanged here (Proposition 4.6.2).

4.8.2 Effect of Behavioral Investments on Real Loss

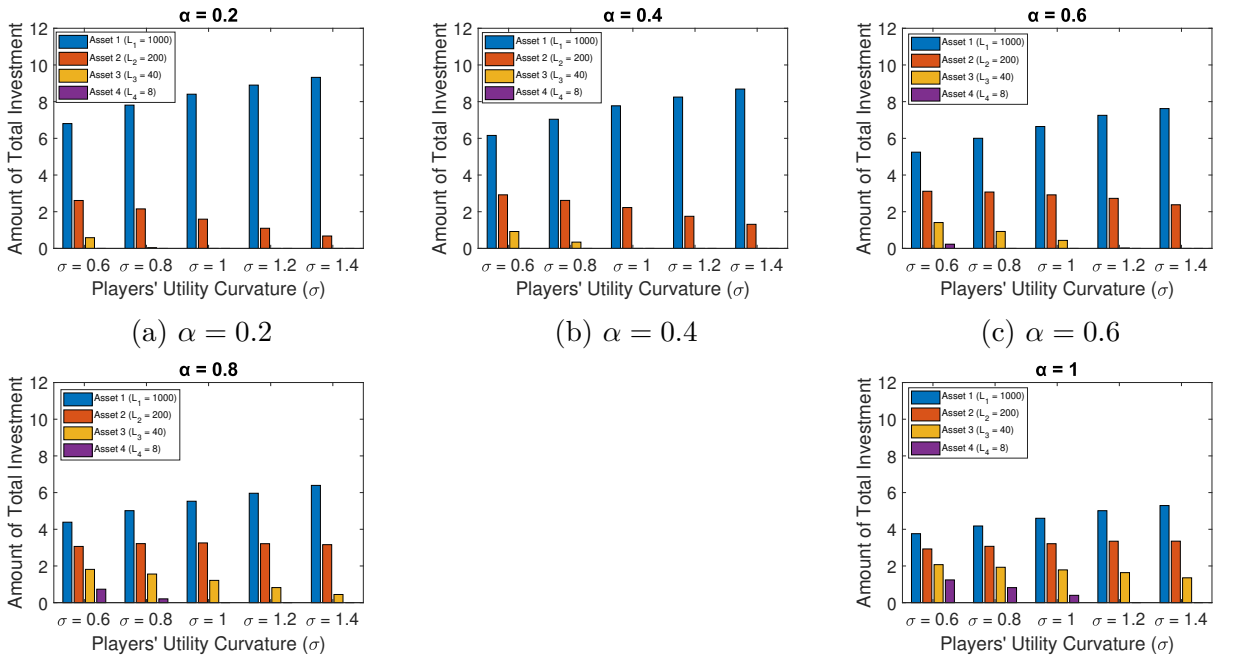
We further consider the total expected system loss E_T of each player under their optimal investments, given by the sum of the true expected losses of all assets. For inverse S-shape probability weighting range, as shown in Fig. 4.3c, when the two players are rational (i.e., $\alpha_1 = \alpha_2 = 1$) $E_T = 40.21$, while $E_T = 126.02$ when $\alpha_1 = \alpha_2 = 0.2$. This considerable increase in the total expected real loss of the behavioral players shows that probability weighting induces the players to invest in a sub-optimal manner, specifically when some assets are much more valuable than others. Similarly, we observe increase in the total real loss (but with less magnitudes) for S-shape probability weighting. For instance, $E_T = 77.95$ when $\alpha_1 = \alpha_2 = 1.8$ which is approximately 1.94 times that of the rational players.

In total, these simulations shed light on the effect of both of inverse S-shaped and S-shaped proposed models for behavioral probability weighting on the PNE investment decisions and the associated expected real loss. We emphasize that the ratio of loss magnification due to sub-optimal investments under probability weighting is expected to be higher with real-world assets that have huge financial loss when failed [71], [77].

4.8.3 Effect of Utility Curvature

We next study the effect of utility curvature on total investments on each node (asset) under different probability weighting behavioral levels. Note that the utility curvature, as

explained earlier, leads to raising the loss value L_i of each node v_i to a power σ (which is the utility curvature value). In other words, the index of utility curvature (loss aversion) only scales the constant L_i by a scalar without changing the dependence of the cost function on the investments. We consider the same setup of two players with same budget values and loss valuations (shown earlier in this Section). We sweep the values of σ to reflect different types of players (i.e., $\sigma = 1$ is risk-neutral, $\sigma < 1$ is risk-averse, and $\sigma > 1$ is risk-Seeking) while keeping players behavioral probability weighting parameter α fixed.[3] Figure 4.4 shows such experiments (each subfigure has its value of α). We observe that for a fixed behavioral level, the higher the utility curvature is (i.e., higher value of σ) the more the players over-invest on the highest valued assets. Moreover, if the players have both high probability weighting (here $\alpha = 0.2$) and high utility curvature index ($\alpha = 1.4$), they almost put all the budget on the highest valued resource (node) as shown in Fig. 4.4a.



(a) $\alpha = 0.2$ (b) $\alpha = 0.4$ (c) $\alpha = 0.6$

(d) $\alpha = 0.8$ (e) $\alpha = 1$ (No Prob. Weighting)

Figure 4.4. The effect of utility curvature on total investments on each node (asset) under different probability weighting behavioral levels. We observe that for a fixed behavioral level, the higher the utility curvature is (i.e., higher value of σ) the more the players over-invest on the highest valued assets.

[3] The values of the utility curvature index σ used in our experiments follow the prior work [69] and our initial subject experiments.

4.9 Summary of Findings

This chapter presented a framework that accounts for behavioral attitudes of the players in a Multi-Target CPR Game where the players places their investments to protect the shared assets. Specifically, we considered the scenario where each (human) player misperceives the probabilities of failure in each asset. We first established the convexity of the objective function of each player. We then studied multi-player game-theoretic setting and showed the existence of Pure Nash Equilibrium (PNE) in these multi-player games. We also characterized the uniqueness of the total investments on each asset at any PNE. We then studied the impacts of probability weighting on the investment decisions made by the players; in particular, we showed that nonlinear perceptions of probability can induce players to invest more on the assets with higher values. This leads to leaving the assets with lower losses unprotected. We then quantified the effect of heterogeneity of behavioral levels on the investments at PNE. We also compared different possible policies for enhancing behavioral levels. Finally, we provided numerical simulations to show the effect of probability misperceptions on the investment decisions.

Future avenues of research include performing human subject experiments (similar to the controlled experiments on defense investments on interdependent attack graphs in [78]) to test our predictions. Moreover, exploring other setups with other factors in prospect theory such as subjective assessments of outcomes would be another avenue for future research.

5. The Effect of Behavioral Probability Weighting in a Sequential Defender-Attacker Game

In this chapter, we consider a setting consisting of two sites, and a sequential game between a defender and an attacker who are responsible for securing and attacking the sites, respectively. Each site has a value to the defender, and an associated probability of successful attack, which can be reduced via security investments in that site by the defender. The attacker targets the site that maximizes the expected loss for the defender (after the investments). While prior work has studied the security investments in such scenarios, in this work we consider what happens when the defender exhibits characteristics of bounded-rationality that have been identified by behavioral economics. In particular, humans have been shown to perceive probabilities in a nonlinear manner, typically overweighting low probabilities and underweighting high probabilities. We characterize how such nonlinear probability weighting affects the security investments made by the defender, and bound the inefficiency of the equilibrium investments under behavioral decision-making, compared to a non-behavioral optimal solution.

5.1 The Defender-Attacker Sequential Game

In this section, we describe our general game framework, which builds upon the model introduced in [30]. We consider a sequential game consisting of two players, a defender and an attacker. There are two *sites*, denoted site 1 and site 2, which the defender is trying to protect (and the attacker is trying to compromise). The defender has a budget $R \in \mathbb{R}_{>0}$ that she can spend on defending the sites. In particular, the defender moves first and allocates an amount $r \in [0, R]$ to site 1 and an amount $R - r$ to site 2. We assume that the attacker can observe the allocations made by the defender to each of the sites, after which he targets one of the two sites.

The probability that the attacker successfully compromises the site that he targets is a decreasing function of the amount invested in protecting that site by the defender. The probability of successful attack on site 1, when the defense investment on that site is r, is

denoted by $p_1(r)$. We assume $p_1 < 0$ and $p_1 > 0$. Similarly, for site 2, let $p_2(x)$ be the probability that an attack on site 2 succeeds if the defender spends $x = R - r$ defending that site. Once again, we assume that $p_2 < 0$ and $p_2 > 0$. We note that these assumptions are common in the literature (e.g., [28], [30]).

The defender suffers a loss of one if site 1 is successfully attacked, and a loss of $A > 0$ if site 2 is successfully attacked. After the defender allocates her resources, the attacker targets the site that will maximize the defender's expected loss. Thus, the defender's expected loss if it allocates r to site 1 is given by

$$L(r) = \max\left\{p_1(r), Ap_2(R-r)\right\}. \tag{5.1}$$

This is also the attacker's expected gain.

As one might expect, the optimal strategy for the defender is to choose r in order to equalize the expected loss from both sites (if possible). The paper [30] studied this game when both the defender and the attacker are perfectly rational, but did not investigate the impacts of behavioral biases of the defender and the attacker, which are the focus of the present work. We describe this extension in the next section, and then subsequently analyze the outcomes of those behavioral biases.

5.2 Nonlinear Probability Weighting and the Behavioral Defender-Attacker Sequential Game

Next, we incorporate the probability weighting function into the security game defined in Section 5.1, and define the Behavioral Defender-Attacker Sequential Game that is the focus of this chapter.

5.2.1 The Behavioral Defender-Attacker Sequential Game

Recall that the defender seeks to protect a set of two sites, and the probability of each site being successfully attacked is determined by the corresponding investment in that site. This motivates us to study a *Behavioral Defender-Attacker Sequential Game* that incorporates probability weighting, as defined below.

In the *Behavioral Defender-Attacker Sequential Game*, the players, sites, actions, and probabilities are as defined in Section 5.1. However, we now define a behavioral probability weighting parameter $\alpha_{\mathcal{D}} \in (0, 1]$ for the defender, capturing the extent of her behavioral misperception of probabilities.[1] Thus, using the Prelec function (2.3), the defender's *perceived* attack probability on a site $\mathrm{i} \in \{1, 2\}$ is given by:

$$w_{\mathcal{D}}(p_{\mathrm{i}}(\cdot)) = \exp\Big[-(-\log(p_{\mathrm{i}}(\cdot)))^{\alpha_{\mathcal{D}}}\Big],$$

where $p_{\mathrm{i}}(\cdot) \in [0, 1]$, $\alpha_{\mathcal{D}} \in (0, 1]$.

Based on these misperceptions, the behavioral defender attempts to minimize her perceived expected loss

$$L_w(r) = \max\left\{w_{\mathcal{D}}(p_1(r)), A w_{\mathcal{D}}(p_2(R - r))\right\}. \tag{5.2}$$

In particular, note that the defender may not be aware of her own behavioral biases, and thus will not anticipate that the attacker will have a different perception than her. In other words, the defender assumes that the attacker will target the site that has the largest perceived expected loss for the defender.

On the other hand, the (non-behavioral) attacker chooses which site to attack in order to maximize the defender's *true* expected loss. Thus, the attacker's action under a defense investment of r on site 1 will yield the utility (payoff)

$$U(r) = \max\{p_1(r), A p_2(R - r)\}. \tag{5.3}$$

Remark 8. *For ease of notation, we will drop the subscript $\mathcal{D}$ for most of our analysis, when it is clear from the context (i.e., any result for the defender has $\alpha = \alpha_{\mathcal{D}}$).*

We now study the impacts of the probability weighting parameter α on the decisions made by the players.

[1] One can also consider a behavioral attacker; however, in this chapter, we focus only on behavioral decision-making by the defender in order to better understand its impact on the game, and leave the consideration of a behavioral attacker for future work.

5.3 Properties of the Behavioral Defender-Attacker Sequential Game

5.3.1 Uniqueness of defender's (perceived) optimal investment strategy

First, we prove that the behavioral defender's allocation that minimizes her perceived loss (as captured by (5.2)) is unique. We later use this to understand how behavioral probability weighting affects the investments of the defender.

Proposition 5.3.1. *For any $\alpha \in (0, 1]$, the defender's optimal allocation to site 1 in order to minimize $L_w(r)$ in (5.2) is unique, and denoted by $\hat{r}$.*

Proof. First, note that since $w(p)$ is strictly increasing in p, and by our assumption that $p_1(r)$ is strictly decreasing in r, we have that $w(p_1(r))$ is strictly decreasing in r. Similarly, by our assumption that $p_2(x)$ is strictly decreasing in its argument, the function $p_2(R-r)$ is strictly increasing in r. Thus, $Aw(p_2(R-r))$ is strictly increasing in r.

First, consider the case where $w(p_1(r)) < Aw(p_2(R-r)) \forall r \in [0, R]$. Then, $\hat{r} = 0$ is the unique solution that minimizes the defender's perceived expected loss (since if the defender deviates to any investment $r > 0$, the defender's perceived expected loss $Aw(p_2(R-r))$ would be larger as $Aw(p_2(R-r))$ is increasing in r).

Second, consider the case in which $w(p_1(r)) > Aw(p_2(R-r)) \forall r \in [0, R]$. Then, $\hat{r} = R$ is the unique solution that minimizes the defender's perceived expected loss (since if the defender deviates to any investment $r < R$, the defender's perceived expected loss $w(p_1(r))$ would increase as $w(p_1(r))$ is decreasing in r as shown earlier).

Now, consider the cases that are not considered by the above two (corner) cases. Note that since $w(p_1(r))$ is strictly decreasing in r, and since $Aw(p_2(R-r))$ is strictly increasing in r, and since neither function is always larger than the other (which was captured by the previous two cases), there must be a unique value of r at which $w(p_1(r)) = Aw(p_2(R-r))$. This will be the unique solution to the problem of minimizing (5.2), which we denote by $\hat{r}$. □

Fig. 5.1 illustrates $\hat{r}$, i.e., the allocation that minimizes the maximum perceived expected loss for the defender.

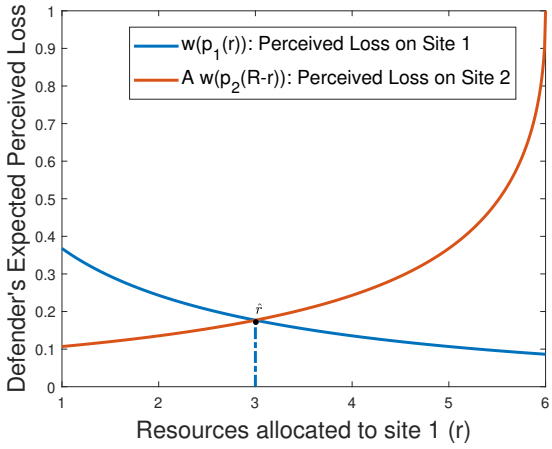


Figure 5.1. An illustration of the defender's minmax problem under misperception of the probabilities of successful attack on each site.

5.3.2 Effect of probability weighting on the defender's investment strategy

We now characterize the impact of probability weighting on the defender's investments in each of the two sites. To aid in our analysis, let us define the difference function between the defender's losses in the two sites as $D(r) = w(p_1(r)) - Aw(p_2(R-r))$. As argued earlier, since the first term is strictly decreasing in r and the second term $(Aw(p_2(R-r)))$ is strictly increasing in r, we see that $D(r)$ is strictly decreasing in r. In particular, $D(r)$ is positive if $w(p_1(r)) > Aw(p_2(R-r))$, negative if $w(p_1(r)) < Aw(p_2(R-r))$, and zero if $w(p_1(r)) = Aw(p_2(R-r))$.

Now, we show how the investment by the defender in site 1 changes under behavioral probability weighting. In order to keep the exposition clear, we will make the following assumption on the probabilities and site values for the case where there is no probability weighting (this assumption rules out the two corner cases where a non-behavioral defender invests entirely in only one of the two sites). This assumption was also made in [30].

Assumption 7. *The quantities $p_1(r)$ and $Ap_2(R-r)$ are such that $p_1(0) > Ap_2(R)$ and $p_1(R) < Ap_2(0)$, i.e., there is a unique quantity r^* such that $p_1(r^*) = Ap_2(R-r^*)$.*

Theorem 5.3.1. *Consider a behavioral defender (with $\alpha \in (0,1)$) that faces losses of 1 and A if the sites 1 and 2 are successfully compromised, respectively. Let $\hat{r}$ be the*

defender's allocation that minimizes its loss (5.2), where $\hat{r}$ is defined in Proposition 5.3.1. Moreover, let r^* be the non-behavioral (with $\alpha = 1$) defender's optimal allocation that satisfies Assumption 7. We have the following cases.

i. If $\hat{r}$ does not satisfy $w(p_1(\hat{r})) = Aw(p_2(R - \hat{r}))$, and

(a) If $w(p_1(r)) < Aw(p_2(R - r))\forall r \in [0, R]$, then $\hat{r} \leq r^*$.

(b) If $w(p_1(r)) > Aw(p_2(R - r))\forall r \in [0, R]$, then $\hat{r} \geq r^*$.

ii. If $\hat{r}$ satisfies $w(p_1(\hat{r})) = Aw(p_2(R - \hat{r}))$, and

(a) If $A = 1$, then $\hat{r} = r^*$,

(b) If $p_1(r^*) < \frac{1}{\mathrm{e}}$ and $A < 1$, then $\hat{r} > r^*$,

(c) If $p_1(r^*) < \frac{1}{\mathrm{e}}$ and $A > 1$, then $\hat{r} < r^*$.

Proof. We begin with the cases in which the behavioral defender cannot equalize the perceived losses. In the case i(a) where $w(p_1(r)) < Aw(p_2(R - r))\forall r \in [0, R]$, we have $\hat{r} = 0$ from Proposition 5.3.1. Thus, we have $r^* \geq \hat{r}$. In the case i(b) in which $w(p_1(r)) > Aw(p_2(R - r))\forall r \in [0, R]$, we have $\hat{r} = R$ from Proposition 5.3.1. Thus, we have $r^* \leq \hat{r}$.

Now, consider the remaining cases, that are not considered by the above (corner) cases, where $\hat{r}$ uniquely satisfies $w(p_1(\hat{r})) = Aw(p_2(R - \hat{r}))$.

Recall that $D(r) = w(p_1(r)) - Aw(p_2(R - r))$ and thus we have $D(\hat{r}) = 0$. Also, from Assumption 7, r^* satisfies the relation $p_1(r^*) = Ap_2(R - r^*)$. Thus,

$$\begin{aligned} D(r^*) &= w(p_1(r^*)) - Aw(p_2(R - r^*)) \\ &= w(p_1(r^*)) - Aw\left(\frac{p_1(r^*)}{A}\right). \end{aligned} \tag{5.4}$$

Now, we prove the following three cases:

Case ii(a): If $A = 1$, we have $D(r^*) = 0$. However, from Proposition 5.3.1, $\hat{r}$ is the defender's unique investment strategy that satisfies $w(p_1(r)) = Aw(p_2(R - r))$ (i.e., $\hat{r}$ is the

only investment that satisfies $D(\hat{r}) = 0$). Therefore, $\hat{r} = r^*$. In other words, the defense allocations of behavioral and non-behavioral defenders are identical if $A = 1$.

Now, for the other cases in ii(b) and ii(c), we show that $\hat{r} \neq r^*$ (i.e., the optimal defense allocations are different for behavioral and non-behavioral defenders). Recall that since $w(p_1(\hat{r})) = Aw(p_2(R - \hat{r}))$, we have $D(\hat{r}) = 0$. To show that $\hat{r} > r^*$, it is sufficient to show that $D(r^*) > 0$ (since $D(r)$ is strictly decreasing in r). Similarly, to show that $\hat{r} < r^*$, it is sufficient to show that $D(r^*) < 0$.

For ease of notation, we will drop the argument r^* of p_1 in the following steps of the proof. We first substitute the form of the Prelec function from (2.3) into (5.4) to obtain

$$D(r^*) = \mathrm{e}^{-(-\log(p_1))^\alpha} - A\mathrm{e}^{-(\log(A)-\log(p_1))^\alpha} = \mathrm{e}^{-(-\log(p_1))^\alpha}\left[1 - Ay(\alpha)\right],$$

where $y(\alpha) = \mathrm{e}^{-(\log(A)-\log(p_1))^\alpha + (-\log(p_1))^\alpha}$.

Case ii(b): We prove this case by dividing it into two sub-cases as follows. First, we consider the sub-case where $p_1 < \frac{1}{\mathrm{e}}$ and $A \in (\mathrm{e}p_1, 1)$. We first differentiate $y(\alpha)$ w.r.t. α to get

$$\begin{aligned}\frac{dy(\alpha)}{d\alpha} = y(\alpha)\Big[&- \left(\log\left(\frac{A}{p_1}\right)\right)^\alpha \log\left(\log\left(\frac{A}{p_1}\right)\right) \\ &+ \left(\log\left(\frac{1}{p_1}\right)\right)^\alpha \log\left(\log\left(\frac{1}{p_1}\right)\right)\Big].\end{aligned}$$

Note since $p_1 < \frac{1}{\mathrm{e}}$, we have $\log\left(\frac{1}{p_1}\right) > 1$ and $\log\left(\log\left(\frac{1}{p_1}\right)\right) > 0$. Moreover, since $A \in (\mathrm{e}p_1, 1)$, we have $\log\left(\frac{A}{p_1}\right) > 1$ and $\log\left(\log\left(\frac{A}{p_1}\right)\right) > 0$. Furthermore,

$$\begin{aligned}A \in (\mathrm{e}p_1, 1) &\iff \log\left(\frac{A}{p_1}\right) < \log\left(\frac{1}{p_1}\right) \\ &\iff \left(\log\left(\frac{A}{p_1}\right)\right)^\alpha < \left(\log\left(\frac{1}{p_1}\right)\right)^\alpha \\ &\iff \log\left(\log\left(\frac{A}{p_1}\right)\right) < \log\left(\log\left(\frac{1}{p_1}\right)\right).\end{aligned}$$

From the above inequalities and the fact that $y(\alpha) > 0$, we see that $\frac{dy(\alpha)}{d\alpha}$ is positive. In other words, $y(\alpha)$ is increasing in α and upper bounded at $\alpha = 1$ and therefore $y(\alpha) < y(1) = \frac{1}{A}$ for any $\alpha \in (0, 1)$. Therefore, $D(r^*) > 0$. Finally, since $D(r)$ is strictly decreasing in r and we have $D(\hat{r}) = 0$, we have $\hat{r} > r^*$.

Now, we consider the second sub-case where $p_1 < \frac{1}{\mathrm{e}}$ and $A \in (0, \mathrm{e}p_1]$. In this sub-case, we use (5.4) to prove that $D(r^*) > 0$ as follows:

$$\begin{aligned} D(r^*) &= w(p_1) - Aw\left(\frac{p_1}{A}\right) \\ &\overset{(a)}{>} p_1 - Aw\left(\frac{p_1}{A}\right) \\ &\overset{(b)}{\geq} p_1 - A\frac{p_1}{A} = 0. \end{aligned}$$

Note that (a) holds since $p_1 < \frac{1}{\mathrm{e}}$ and thus $w(p_1) > p_1$. Also, (b) holds since $A \in (0, \mathrm{e}p_1]$, we have $\frac{p_1}{A} \geq \frac{1}{\mathrm{e}}$ and thus we have $w\left(\frac{p_1}{A}\right) \leq \frac{p_1}{A}$. Therefore, $D(r^*) > 0$, and thus we have $\hat{r} > r^*$.

Case ii(c): We now prove the case when $A > 1$ as follows. In the derivative $\frac{dy(\alpha)}{d\alpha}$ (which always exists here since $A > 1$ and $p_1 < \frac{1}{\mathrm{e}}$), since $p_1 < \frac{1}{\mathrm{e}}$, we have $\log\left(\frac{1}{p_1}\right) > 1$ and $\log\left(\log\left(\frac{1}{p_1}\right)\right) > 0$. Moreover, since $A > 1$ and $p_1 < \frac{1}{\mathrm{e}}$, we have $\log\left(\frac{A}{p_1}\right) > 1$ and $\log\left(\log\left(\frac{A}{p_1}\right)\right) > 0$. Moreover,

$$\begin{aligned} A > 1 &\iff \log\left(\frac{A}{p_1}\right) > \log\left(\frac{1}{p_1}\right) \\ &\iff \left(\log\left(\frac{A}{p_1}\right)\right)^{\alpha} > \left(\log\left(\frac{1}{p_1}\right)\right)^{\alpha} \\ &\iff \log\left(\log\left(\frac{A}{p_1}\right)\right) > \log\left(\log\left(\frac{1}{p_1}\right)\right). \end{aligned}$$

From the above inequalities and the fact that $y(\alpha) > 0$, we have $\frac{dy(\alpha)}{d\alpha}$ is negative. In other words, $y(\alpha)$ is decreasing in α and lower bounded at $\alpha = 1$ and therefore $y(\alpha) > y(1) = \frac{1}{A}$ for any $\alpha \in (0, 1)$.

Therefore, $D(r^*) < 0$. Again, since $D(r)$ is strictly decreasing in r, and we know that $D(\hat{r}) = 0$, we have $\hat{r} < r^*$. That concludes the proof. □

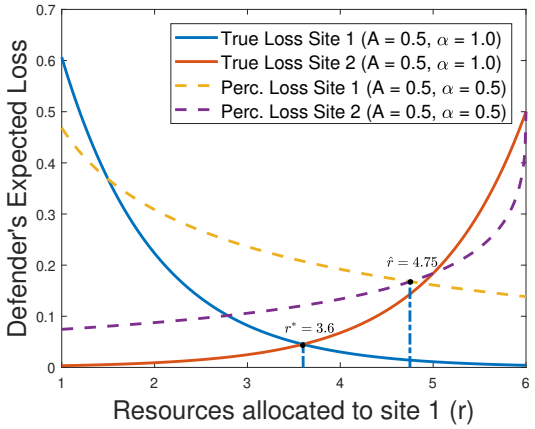


Figure 5.2. The effect of behavioral probability weighting on the defender's investments with $A < 1$.

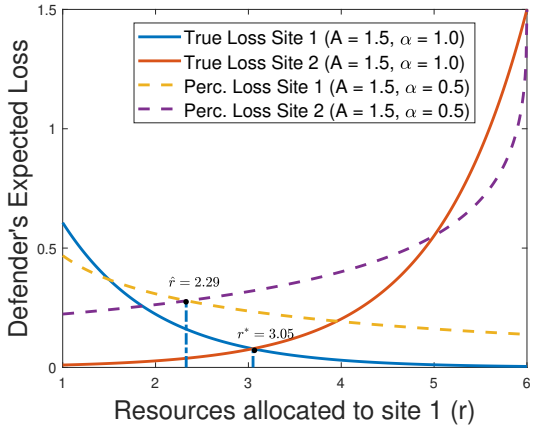


Figure 5.3. The effect of behavioral probability weighting on the defender's investments with $A > 1$.

The above result shows that the optimal defense allocations for both behavioral and non-behavioral defenders are different if $A \neq 1$ (i.e., the sites have different financial losses when compromised). In other words, the behavioral defender allocates more resources to the higher valued site compared to the non-behavioral defender (recall that $\hat{r}$ is the amount of defense resources allocated by the behavioral defender on site 1). This is illustrated in Fig. 5.2, where the second site has a smaller value and therefore $\hat{r} > r^*$ (i.e., the behavioral defender allocates more resources on site 1). On the other hand, if $A > 1$ (as shown in Fig. 5.3) the second site has a higher value and therefore $\hat{r} < r^*$. To generate those figures, we use $p_1(r) = \exp(0.5 - r)$, $p_2(r) = \exp(-(R - r))$ and $R = 6$.

5.3.3 Effect of defender's misperception on the attacker's choice

The above result of Theorem 5.3.1 brings us to the following result, establishing the effect of the behavioral defender's investment on the attacker's choice of targets. In this context, we study that effect by considering the attacker's move in the sequential game. We will show that when facing a behavioral defender and under the scenarios (mentioned in Theorem 5.3.1) where the two sites have different loss values to the defender, the attacker always has a strict preference on which site to strike (in contrast to the situation with a non-behavioral

defender, where the defense investments make the attacker indifferent between the sites). Correspondingly, we show that the behavioral defender's investment strategy shown in Theorem 5.3.1 yields an increase in her true expected loss (i.e., the attacker's payoff would be higher against a behavioral defender, when compared to a non-behavioral defender).

Recall from the Behavioral Defender-Attacker Sequential Game in Section 5.2.1 that the attacker observes the defender's investment on site 1 and then chooses to hit the site that offers her a higher payoff. Let us define the function $E(r) = p_1(r) - Ap_2(R-r)$. Note that if $E(r) > 0$, the non-behavioral attacker would hit site 1, if $E(r) < 0$, the non-behavioral attacker would hit site 2, and if $E(r) = 0$, the non-behavioral attacker is indifferent between the sites. It is easy to see that $E(r)$ is strictly decreasing with r.

Proposition 5.3.2. *Consider a behavioral defender (with $\alpha < 1$), and suppose the allocation $\hat{r}$ on site 1 is such that $w(p_1(\hat{r})) = Aw(p_2(R-\hat{r}))$. Let the losses on sites 1 and 2 (when compromised) be 1 and A, respectively. Moreover, let r^* be the non-behavioral (with $\alpha = 1$) defender's optimal allocation that satisfies Assumption 7. Then,*

i. If $p_1(r^*) < \frac{1}{\mathrm{e}}$ and $A < 1$, the attacker would hit site 2.

ii. If $p_1(r^*) < \frac{1}{\mathrm{e}}$ and $A > 1$, the attacker would hit site 1.

iii. In both of (i) and (ii), the attacker would have higher payoff compared to facing a non-behavioral defender (with $\alpha = 1$). Formally, $U(\hat{r}) > U(r^*)$.

Proof. (i) If $p_1(r^*) < \frac{1}{\mathrm{e}}$ and $A < 1$, we have $\hat{r} > r^*$ (from Theorem 5.3.1). By our assumptions that $p_1(r)$ is strictly decreasing in r and $p_2(R-r)$ is strictly increasing in r, we have $p_1(\hat{r}) < p_1(r^*)$ and $Ap_2(R-\hat{r}) > Ap_2(R-r^*)$. Thus, we have $Ap_2(R-\hat{r}) > p_1(\hat{r})$ (from the fact that $Ap_2(R-r^*) = p_1(r^*)$). Therefore, $E(\hat{r}) < 0$ and the attacker would hit site 2.

(ii) Second, if $p_1(r^*) < \frac{1}{\mathrm{e}}$ and $A > 1$, we have $\hat{r} < r^*$ (from Theorem 5.3.1). With a similar argument to (i), we have $Ap_2(R-\hat{r}) < p_1(\hat{r})$. Thus, $E(\hat{r}) > 0$ and the attacker would hit site 1.

(iii) Now, we compare the attacker's payoff under the defense investments r^* and $\hat{r}$ by the non-behavioral and behavioral defender, respectively.

If $p_1(r^*) < \frac{1}{e}$ and $A < 1$, we have

$$\begin{aligned} \hat{r} > r^* &\iff Ap_2(R - \hat{r}) > Ap_2(R - r^*) \\ &\iff U(\hat{r}) \overset{(a)}{>} U(r^*). \end{aligned}$$

Note that (a) holds since $Ap_2(R - r^*) = p_1(r^*)$ (from Assumption 7) and $Ap_2(R - \hat{r}) > p_1(\hat{r})$ (from (i)) and by substituting in (5.3).

Second, if $p_1(r^*) < \frac{1}{e}$ and $A > 1$, we have

$$\begin{aligned} \hat{r} < r^* &\iff p_1(\hat{r}) > p_1(r^*) \\ &\iff U(\hat{r}) \overset{(b)}{>} U(r^*). \end{aligned}$$

Similarly, (b) holds since $Ap_2(R - r^*) = p_1(r^*)$ and $Ap_2(R - \hat{r}) < p_1(\hat{r})$ (from (ii)). □

The above result shows that under loss asymmetry, the non-behavioral attacker benefits (i.e., has a higher payoff) from the behavioral defender's investment decisions. In the next section, we will seek to quantify this increase in the attacker's payoff (or equivalently, the increase in the defender's *true* expected loss).

5.4 Bound on Behavioral Inefficiency

In this section, we seek to define a measure to capture the inefficiency of the security investments due to the defender's behavioral decision-making. We thus define the Price of Behavioral Probability Weighting (PoBW) as the ratio of the *true* expected loss of the behavioral defender (under the behavioral investments) to the true expected loss of a non-behavioral defender. This notion is similar to the Price of Behavioral Anarchy (PoBA) metric introduced in [77], which measured the inefficiency of game-theoretic equilibria with multiple behavioral defenders (similar to how the classical notion of Price of Anarchy measures the inefficiency of game-theoretic equilibria compared to a socially optimal solution [55]). Here, PoBW measures only the inefficiency of the single defender due

to her behavioral decision-making. Specifically, we define the Price of Behavioral Probability Weighting (PoBW) as

$$PoBW = \frac{L(\hat{r})}{L(r^*)}, \tag{5.5}$$

where $\hat{r} = \min_{r\in[0,R]} \max\{w(p_1(r)), Aw\,(p_2(R-r))\}$ and $r^* = \min_{r\in[0,R]} \max\{p_1(r), Ap_2(R-r)\}$ denote the behavioral and non-behavioral defender's investments, respectively. We emphasize that the expected losses in both the numerator and the denominator are the *true* (rather than perceived) expected losses (defined in (5.1)) of the defender.

Now, we will establish the upper bound on the PoBW. We show that the PoBW is bounded if the total budget is bounded (regardless of the defender's behavioral level).

Proposition 5.4.1. *Let the budget available to the defender be R, and let the probability of successful attack on sites 1 and 2 be given by $p_1(r) = \mathrm{e}^{-r}$ and $p_2(r) = \mathrm{e}^{-(R-r)}$, respectively. Then, for any A and any behavioral level $\alpha \in (0, 1]$, $PoBW \leq \max\{A, \frac{1}{A}\}\exp(R)$.*

Proof. Substituting from (5.1) into (5.5) yields

$$PoBW = \frac{\max\{p_1(\hat{r}), Ap_2(R-\hat{r})\}}{\max\{p_1(r^*), Ap_2(R-r^*)\}}.$$

We consider the following four possible sub-cases. To get the upper bound of PoBW, we will leverage the fact that $\mathrm{e}^{-R} \leq p_1(r) \leq 1$ and $\mathrm{e}^{-R} \leq p_2(r) \leq 1$ (from the proposition statement) as follows.

i) If $p_1(\hat{r}) > Ap_2(R-\hat{r})$ and $p_1(r^*) > Ap_2(R-r^*)$, then we have

$$PoBW = \frac{p_1(\hat{r})}{p_1(r^*)} \overset{(a)}{=} \frac{\exp(-\hat{r})}{\exp(-r^*)} \overset{(b)}{\leq} \exp(R).$$

Note that (a) holds from the proposition statement and (b) holds since the numerator is upper bounded by 1 and the denominator is lower bounded by e^{-R}.

ii) If $p_1(\hat{r}) \leq Ap_2(R-\hat{r})$ and $p_1(r^*) \leq Ap_2(R-r^*)$, then we have

$$PoBW = \frac{Ap_2(R-\hat{r})}{Ap_2(R-r^*)} = \frac{A\exp(-R+\hat{r})}{A\exp(-R+r^*)} \leq \exp(R).$$

iii) If $p_1(\hat{r}) > Ap_2(R-\hat{r})$ and $p_1(r^*) \leq Ap_2(R-r^*)$, then we have

$$PoBW = \frac{p_1(\hat{r})}{Ap_2(R-r^*)} = \frac{\exp(-\hat{r})}{A\exp(-R+r^*)} \overset{(c)}{\leq} \frac{\exp(R)}{A}.$$

Note that (c) holds since the numerator is upper bounded by 1 and the denominator is lower bounded by $A\mathrm{e}^{-R}$.

iv) If $p_1(\hat{r}) \leq Ap_2(R-\hat{r})$ and $p_1(r^*) > Ap_2(R-r^*)$, then we have

$$PoBW = \frac{Ap_2(R-\hat{r})}{p_1(r^*)} = \frac{A\exp(-R+\hat{r})}{\exp(-r^*)} \overset{(d)}{\leq} A\exp(R).$$

Similarly, (d) holds since the numerator is upper bounded by A and the denominator is lower bounded by e^{-R}.

In all of the possible scenarios (as shown above), $PoBW \leq \max\{A, \frac{1}{A}\}\exp(R)$, which concludes the proof. □

Now, we illustrate our above characterizations of the impacts of behavioral decision-making via numerical simulations.

5.5 Numerical Simulations

5.5.1 Effect of perception on payoffs

In this subsection, we show the effect of misperception on the defender's true expected loss in the Behavioral Defender-Attacker Sequential Game. We consider the sequential game described in Section 5.2.1 with a behavioral defender and a non-behavioral attacker. We let the probability of successful attack on sites 1 and 2 be given by $p_1(r) = \mathrm{e}^{-r}$ and $p_2(r) = \mathrm{e}^{-(R-r)}$, respectively (similar to Proposition 5.4.1). For the defender, the first site has a unit loss while second site has a loss of A when compromised. We consider the values $A = 0.5$ and $A = 1.5$ to represent the two possible scenarios of loss asymmetry. We let the total defense budget for defending the two sites be $R = 10$. The optimal investments in the following scenarios were calculated using CVX toolbox [56].

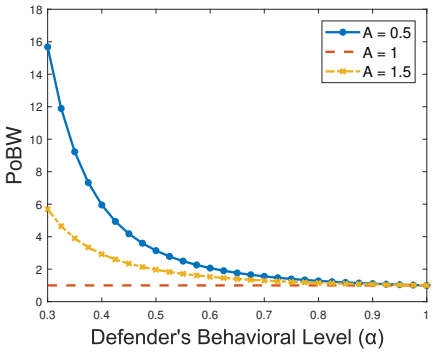


Figure 5.4. Effect of behavioral probability weighting on the defender's true expected loss. The PoBW increases from one as the defender becomes more behavioral (i.e., α decreases) under asymmetric loss values ($A \neq 1$).

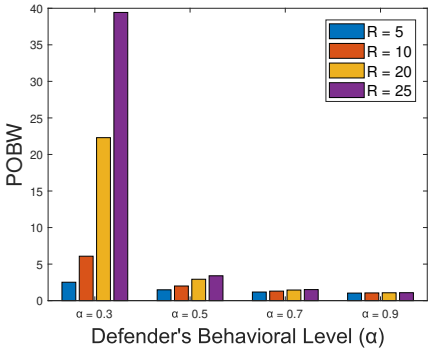


Figure 5.5. The PoBW for different security budgets (i.e., different R). We observe that the PoBW increases non-linearly as the security budget increases when the defender becomes more behavioral (i.e., as α decreases).

Fig. 5.4 shows the PoBW ratio given by (5.5) to measure the inefficiency of the defender's investments, compared to the investments of a non-behavioral defender. It shows the value of this ratio as we sweep α from 0.3 to 1 (non-behavioral), for different values of the loss A.[2] As the figure shows, the PoBW increases from 1 as α changes for the defender for both $A = 0.5$ and $A = 1.5$ (which is consistent with Proposition 5.4.1). This considerable increase in the PoBW shows that the behavioral defender's investments are beneficial to the attacker, especially under loss asymmetries (i.e., one site is more valuable to the defender).

5.5.2 Effect of Security Budget

Similarly, we let the probability of successful attack on sites 1 and 2 be given by $p_1(r) = \mathrm{e}^{-r}$ and $p_2(r) = \mathrm{e}^{-(R-r)}$ and let $A = 1.5$. Fig. 5.5 shows the value of the PoBW ratio as we sweep α from 0.3 to 0.9 (almost non-behavioral), for different values of the total budget R. Fig. 5.5 shows that the inefficiency due to behavioral decision-making becomes exacerbated

[2]↑Prior experimental studies have shown that the probability weighting parameter α tends to fall within this range (e.g., [15], [79]).

as the defense budget R increases. This happens as the behavioral defender shifts higher amounts of her budget to the site with higher loss, leaving the other site vulnerable and thus the attacker hits that vulnerable site (i.e., here site 1 since $A > 1$). We also note that this effect is more noticeable when the defender becomes more behavioral (i.e., as α decreases).

5.6 Summary of Findings

In this chapter, we presented a game-theoretic framework that takes account of behavioral biases of the defender in a defender-attacker sequential game. Specifically, we first showed uniqueness of the (behavioral) defender's investments (under appropriate conditions on the probabilities of successful attack on each of the defender's sites). We also showed how nonlinear perceptions of attack probabilities affect the security investments made by defender to protect her sites. In this context, the behavioral defender finds it optimal to invest more on the site with the higher loss (leaving the site with lower loss more vulnerable compared to the non-behavioral defender). As a result, this changes the attacker's choice of site to hit, and increases the defender's real expected loss. An avenue for future research would be consider the setup of multiple sites (more than 2). Moreover, studying properties of the setup of a non-behavioral defender and a behavioral attacker would be another avenue for future research.

6. The Effect of Behavioral Probability Weighting in a Simultaneous Multi-Target Attacker-Defender Game

In this chapter, we consider a simultaneous security game in a setting consisting of two players (an attacker and a defender), each with a given budget to allocate towards attack and defense, respectively, of a set of nodes. Each node has a certain value to the attacker and the defender, along with a probability of being successfully compromised, which is a function of the investments in that node by both players. For such games, we characterize the optimal investment strategies by the players at the (unique) Nash Equilibrium. We then investigate the impacts of behavioral probability weighting on the investment strategies; such probability weighting, where humans overweight low probabilities and underweight high probabilities, has been identified by behavioral economists to be a common feature of human decision-making. We show via numerical experiments that behavioral decision-making by the defender causes the Nash Equilibrium investments in each node to change (where the defender overinvests in the high-value nodes and underinvests in the low-value nodes).

6.1 The Multi-Target Security Game Framework

In this section, we introduce the defender model, the adversary model, and the players' utilities considered in this chapter.

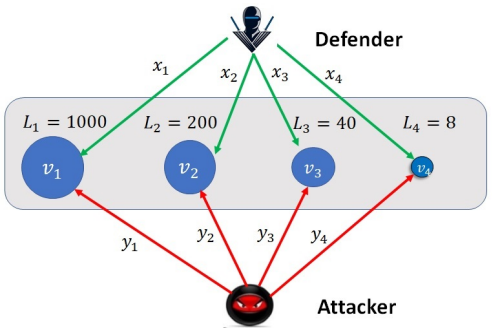


Figure 6.1. A simple visualization of our Multi-Target Game Setup. The green arrows are the defense resources while the red arrows are the attack efforts on the assets. The quantities x_i and y_i denote the amount of resources allocated to defending and attacking asset v_i, respectively.

6.1.1 Strategic Defender

Let $\mathcal{D}$ be a defender who is responsible for defending a set $V = \{v_1, v_2, \ldots, v_n\}$ of assets. For each compromised asset $v_m \in V$, defender $\mathcal{D}$ will incur a financial loss $L_m \in \mathbb{R}_{>0}$. To reduce the attack success probabilities on assets, the defender can allocate security resources on these assets, subject to the constraints described below.

Let $n = |V|$. We assume that defender $\mathcal{D}$ has a security budget $B \in \mathbb{R}_{\geq 0}$. Thus, we define the defense strategy space of the defender by

$$X \triangleq \{\mathbf{x} \in \mathbb{R}^n_{\geq 0} : \sum_{v_i \in V} x_i \leq B\}. \tag{6.1}$$

In other words, the defense strategy space for defender $\mathcal{D}$ consists of all non-negative investments on assets such that the sum of all investments does not exceed the budget B. We denote any particular vector of investments by defender $\mathcal{D}$ by $\mathbf{x} \in X$.

6.1.2 Strategic Attacker

Let $\mathcal{A}$ be an attacker who is attempting to compromise the set V of assets.[1] For each compromised asset $v_m \in V$, the attacker $\mathcal{A}$ will incur a financial gain $G_m \in \mathbb{R}_{>0}$. To increase the attack success probabilities on assets, the attacker can allocate attack resources on these assets, subject to a budget constraint $P \in \mathbb{R}_{\geq 0}$. Thus, we define the attack strategy space of the attacker by

$$Y \triangleq \{\mathbf{y} \in \mathbb{R}^n_{\geq 0} : \sum_{v_i \in V} y_i \leq P\}. \tag{6.2}$$

In other words, the attack strategy space for attacker $\mathcal{A}$ consists of all non-negative attack investments on assets, with the sum of all these investments not exceeding P. We denote the attacker's investment vector by $\mathbf{y} \in Y$.

[1] ↑It is realistic to assume that multiple targets could be attacked at one time. Therefore, we allow the attacker to launch simultaneous attacks on different multiple targets.

6.1.3 Defender's and Attacker's Utilities

The investments made by the defender and the attacker on each asset changes the probability that the asset can be successfully compromised by the attacker. Specifically, let $p_{\mathrm{i}} : \mathbb{R}^2_{\geq 0} \to [0,1]$ be a function mapping the total defense investment x_{i} and the total attack investment y_{i} on the asset v_{i} to an attack success probability.

The goal of defender $\mathcal{D}$ is to choose her investment vector $\mathbf{x}$ in order to best protect her assets from being attacked. Mathematically, this is captured via the cost function

$$\overline{C}_{\mathcal{D}}(\mathbf{x}, \mathbf{y}) = \sum_{v_{\mathrm{i}} \in V} L_{\mathrm{i}}\, p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}}) \tag{6.3}$$

subject to $\mathbf{x} \in X$. In particular, for any given $\mathbf{y} \in Y$, defender $\mathcal{D}$ chooses her investment $\mathbf{x} \in X$ to minimize $\overline{C}_{\mathcal{D}}(\mathbf{x}, \mathbf{y})$.

The goal of the attacker $\mathcal{A}$ is to choose her attack investment vector $\mathbf{y}$ in order to compromise her target assets. Mathematically, this is captured via the utility function

$$\overline{U}_{\mathcal{A}}(\mathbf{x}, \mathbf{y}) = \sum_{v_{\mathrm{i}} \in V} G_{\mathrm{i}}\, p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}}) \tag{6.4}$$

subject to $\mathbf{y} \in Y$. For any given $\mathbf{x} \in X$, attacker $\mathcal{A}$ chooses $\mathbf{y} \in Y$ to maximize $\overline{U}_{\mathcal{A}}(\mathbf{x}, \mathbf{y})$.

Note that $\overline{C}_{\mathcal{D}}(\mathbf{x}, \mathbf{y})$ and $\overline{U}_{\mathcal{A}}(\mathbf{x}, \mathbf{y})$ are functions of both the defense investments $\mathbf{x}$ of the defender and the attack investments $\mathbf{y}$ by the attacker.

The recent work [7] studies this setting and provides a method to calculate the optimal investments (with respect to the cost (6.3) and utility (6.4) functions, respectively). However, as mentioned in the introduction, humans have been shown to systematically misperceive probabilities, which can impact the decisions that defenders and attackers make in the presence of risk. In the next section, we will review certain classes of probability weighting functions that capture this phenomenon, and then subsequently introduce such functions into the above Multi-Target Security Game formulation.

6.2 The Behavioral Multi-Target Security Game

In this section, we incorporate behavioral biases into the two player simultaneous move game formulation between the defender $\mathcal{D}$, and the attacker $\mathcal{A}$.

Recall that the defender seeks to protect a set of assets, while the attacker is seeking to compromise them. The probability of each asset being successfully compromised is itself determined by the corresponding investments on that asset by both the attacker and the defender. This motivates a broad class of games that incorporate probability weighting, as defined below.

6.2.1 Behavioral Multi-Target Security Game Formulation

Definition 6.2.1. *We define a Behavioral Multi-Target Security Game as a game between an attacker and a defender for a set of targets, where both defender and attacker misperceive the attack probability on each asset according to the probability weighting function defined in (2.3). Specifically, the perceived attack probability on an asset $v_{\mathrm{i}} \in V$ by player $k \in \{\mathcal{A}, \mathcal{D}\}$ is given by:*

$$w_k(p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}})) = \exp\Big[-(-\log(p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}})))^{\alpha_k} \Big],$$

where $p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}}) \in [0, 1]$, $\alpha_k \in (0, 1]$.

Remark 9. *The subscript k in α_k and $w_k(\cdot)$ allows each player (i.e., attacker and defender) in the Behavioral Multi-Target Security Game to have a different level of mis-perception. However, for ease of notation, we will drop the subscript k for most of our analysis, when it is clear from the context (i.e., any result for the defender has $\alpha = \alpha_{\mathcal{D}}$ and any result for the attacker has $\alpha = \alpha_{\mathcal{A}}$).*

Now, we present the optimization problem perceived by the behavioral defender and the behavioral attacker, respectively.

Defender Cost Function Minimization Problem

$$\underset{\mathbf{x}\in X}{\text{minimize}} \quad C_{\mathcal{D}}(\mathbf{x},\mathbf{y}) = \sum_{\mathrm{i}=1}^{n} L_{\mathrm{i}} \;\; w_{\mathcal{D}}(p_{\mathrm{i}}(x_{\mathrm{i}},y_{\mathrm{i}})). \tag{6.5}$$

Attacker Utility Function Maximization Problem

$$\underset{\mathbf{y}\in Y}{\text{maximize}} \quad U_{\mathcal{A}}(\mathbf{x},\mathbf{y}) = \sum_{\mathrm{i}=1}^{n} G_{\mathrm{i}} \;\; w_{\mathcal{A}}(p_{\mathrm{i}}(x_{\mathrm{i}},y_{\mathrm{i}})). \tag{6.6}$$

In a Behavioral Multi-Target Security Game, a collection of best response strategies $(\mathbf{x}^*,\mathbf{y}^*)$ is a Pure-strategy Nash Equilibrium (PNE) if and only if both equations (6.7) and (6.8) below are satisfied simultaneously:

$$\mathbf{x}^* \in \underset{\mathbf{x}\in X}{\text{argmin}} \;\; C_{\mathcal{D}}(\mathbf{x},\mathbf{y}^*) \tag{6.7}$$

$$\mathbf{y}^* \in \underset{\mathbf{y}\in Y}{\text{argmax}} \;\; U_{\mathcal{A}}(\mathbf{x}^*,\mathbf{y}). \tag{6.8}$$

We will start by proving the existence of a PNE in the Behavioral Multi-Target Security Game, and then subsequently characterize properties of the investments by the players. In particular, we focus on the simultaneous move game in this chapter (e.g., as considered in [7] and the literature on Colonel Blotto games [34]).

6.3 Existence of Pure Strategy Nash Equilibrium

In this section, we prove the existence of a PNE for the Behavioral Multi-Target Security Game defined in Section 6.2. Throughout, let the function $p_{\mathrm{i}}(x_{\mathrm{i}},y_{\mathrm{i}})$ represent the true probability of successful attack on an asset $v_{\mathrm{i}} \in V$ when the total defense and attack investments on that asset are x_{i} and y_{i}, respectively. We make the following assumption on $p_{\mathrm{i}}(x_{\mathrm{i}},y_{\mathrm{i}})$.

Assumption 8. *The probability of successful attack on asset $v_i \in V$, $p_i(x_i, y_i)$, has the following properties.*

- $p_i(x_i, y_i)$ *is twice differentiable with* $p_i(x_i, 0) = 0$ *and* $\lim_{x_i \to \infty} p(x_i, y_i) = 0 \ \forall y_i \in \mathbb{R}_{\geq 0}$.
- $p_i(x_i, y_i)$ *is decreasing and log-convex*[2] *in* x_i.
- $p_i(x_i, y_i)$ *is increasing and concave in* y_i.
- $p_i(x_i, y_i)\dfrac{\partial^2 p(x_i, y_i)}{\partial x_i \partial y_i} \leq \dfrac{\partial p_i(x_i, y_i)}{\partial x_i}\dfrac{\partial p_i(x_i, y_i)}{\partial y_i}$.

In other words, the larger the defensive security investment on a target, the less likely that the target will be successfully attacked. On the other hand, the larger the attack resources used to attack a target, the higher the chance that the target is compromised successfully. The assumptions of concavity and twice-differentiability are common in literature [7], [33].

A particular success function which we will focus on throughout this work is

$$p_i(x_i, y_i) = \exp(-x_i - a_i)(1 - \exp(-y_i)), \tag{6.9}$$

where $a_i \in \mathbb{R}_{\geq 0}$ in (6.9) represents the pre-existing (or inherent) security investments on a node, which decrease the successful attack probability even under no additional defense investment. Such probability functions fall within the class commonly considered in security economics [25], [28], and satisfy the conditions in Assumption 8.

Lemma 10. *For every asset $v_i \in V$, the perceived probability of attack $w(p_i(x_i, y_i))$ is convex in the defense investment x_i under Assumption 8.*

Proof. For ease of notation, we drop the subscript i in the following analysis. First note that since $0 \leq p(x, y) \leq 1$, we have $0 \leq -\log(p(x, y)) \leq \infty$ for all x and y. Substituting $p(x, y)$ into the probability weighting function defined in (2.3), we have

$$w(p(x, y)) = \exp\Big[-(-\log(p(x, y)))^{\alpha}\Big].$$

[2]↑This is a common assumption in the literature [25], [28].

Now, calculating the second partial derivative of $w(p(x,y))$ w.r.t x yields

$$\frac{\partial w(p(x,y))}{\partial x} = \alpha w(p(x,y))(-\log(p(x,y)))^{\alpha-1}\frac{\frac{\partial p(x,y)}{\partial x}}{p(x,y)},$$

$$\begin{aligned}\frac{\partial^2 w(p(x,y))}{\partial x^2} = \alpha\frac{w(p(x,y))(-\log(p(x,y)))^{\alpha-1}}{(p(x,y))^2} \\ \Bigg[(1-\alpha)\left(\frac{\partial p(x,y)}{\partial x}\right)^2(-\log(p(x,y)))^{-1} \\ +\alpha\left(\frac{\partial p(x,y)}{\partial x}\right)^2(-\log(p(x,y)))^{\alpha-1} \\ +\left(p(x,y)\frac{\partial^2 p(x,y)}{\partial x^2}-\left(\frac{\partial p(x,y)}{\partial x}\right)^2\right)\Bigg].\end{aligned}$$

Since $0 < \alpha \leq 1$, the first term on the R.H.S. of $\frac{\partial^2 w(p(x,y))}{\partial x^2}$ is always non-negative. The second term is also non-negative. Also, $p(x,y)$ is twice-differentiable and log-convex in x, and the feasible defense strategy domain X is convex. Therefore, $p(x,y)\frac{\partial^2 p(x,y)}{\partial x^2} \geq (\frac{\partial p(x,y)}{\partial x})^2$ [52] which ensures that the third term is also non-negative. Therefore, $w(p_{\mathrm{i}}(x_{\mathrm{i}},y_{\mathrm{i}}))$ is convex in the defense investment x_{i}. □

Lemma 11. *Under Assumption 8, if* $p_{\mathrm{i}}(x_{\mathrm{i}},y_{\mathrm{i}}) \in [0,\frac{1}{\mathrm{e}})\forall x_{\mathrm{i}},y_{\mathrm{i}} \in \mathbb{R}_{\geq 0}$, *then*

i. The perceived probability $w(p_{\mathrm{i}}(x_{\mathrm{i}},y_{\mathrm{i}}))$ *will be concave in the attack investment* y_{i}.

ii. The partial derivative $\dfrac{\partial^2 w(p(x_{\mathrm{i}},y_{\mathrm{i}}))}{\partial x_{\mathrm{i}}\partial y_{\mathrm{i}}}$ *is negative.*

Proof. (i) Beginning with $\frac{\partial^2 w(p(x,y))}{\partial y^2}$ (which has the same form as $\frac{\partial^2 w(p(x,y))}{\partial x^2}$ in the proof of Lemma 10), we have

$$\begin{aligned}\frac{\partial^2 w(p(x,y))}{\partial y^2} = \alpha\frac{w(p(x,y))(-\log(p(x,y)))^{\alpha-1}}{(p(x,y))^2} \\ \Bigg[(1-\alpha)\left(\frac{\partial p(x,y)}{\partial y}\right)^2(-\log(p(x,y)))^{-1}+\alpha\left(\frac{\partial p(x,y)}{\partial y}\right)^2(-\log(p(x,y)))^{\alpha-1} \\ +\left(p(x,y)\frac{\partial^2 p(x,y)}{\partial y^2}-\left(\frac{\partial p(x,y)}{\partial y}\right)^2\right)\Bigg].\end{aligned}$$

Since $p(x,y) < \frac{1}{\mathrm{e}}$, $(-\log(p(x,y)))^{-1} < 1$ and $(-\log(p(x,y)))^{\alpha-1} < 1$. Moreover, we have $\alpha(-\log(p(x,y)))^{\alpha-1} + (1-\alpha)(-\log(p(x,y)))^{-1} < 1$. Therefore, the summation of the first, second and fourth term is negative. From Assumption 8, $\frac{\partial^2 p(x,y)}{\partial y^2} < 0$ which implies that the third term is also negative. Therefore, $\frac{\partial^2 w(p(x,y))}{\partial y^2} < 0$, i.e., $w(p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}}))$ is concave in the attacker investment y_{i}.

(ii) The proof of (ii) is similar to that of part (i) and Lemma 10 by using the second partial derivative formula and Assumption 8, and thus we omit its steps. □

Note that for attack success probabilities given by (6.9), the condition $p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}}) \in [0, \frac{1}{\mathrm{e}})$ is guaranteed when the inherent defenses of the asset (given by parameter a_{i}) satisfy $a_{\mathrm{i}} \geq 1$.

This brings us to the following result, establishing the existence of a PNE in the Behavioral Multi-Target Security Games.

Theorem 6.3.1. *Under Assumption 8, if* $p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}}) \in [0, \frac{1}{\mathrm{e}}) \forall x_{\mathrm{i}}, y_{\mathrm{i}} \in \mathbb{R}_{\geq 0}$*, a PNE exists in the Behavioral Multi-Target Security Game.*

Proof. From (6.1) and (6.2), the strategy spaces X and Y are compact and convex. Let the Hessian matrices of $C_{\mathcal{D}}(\mathbf{x}, \mathbf{y})$ (in (6.5)) and $U_{\mathcal{A}}(\mathbf{x}, \mathbf{y})$ (in (6.6)) be $H_{\mathcal{D}}$ and $H_{\mathcal{A}}$, respectively. Both $H_{\mathcal{D}}$ and $H_{\mathcal{A}}$ are diagonal by definition since $p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}})$ for each asset only depends on x_{i} and y_{i}. Moreover, from Lemma 10, each diagonal element in $H_{\mathcal{D}}$ is non-negative and therefore $C_{\mathcal{D}}(\mathbf{x}, \mathbf{y})$ is continuous and convex in $\mathbf{x}$. Similarly, Lemma 11 shows that each diagonal element in $H_{\mathcal{A}}$ is non-positive and thus $U_{\mathcal{A}}(\mathbf{x}, \mathbf{y})$ is continuous and concave in $\mathbf{y}$. Therefore, a pure-strategy Nash equilibrium exists for our Behavioral Multi-Target Security Game [54], [80]. □

After establishing the existence of a PNE in our Behavioral Multi-Target Security Game, we study the characteristics of the investments of the players (the defender and the attacker) in the game.

6.4 Properties of the Optimal Investment Decisions

In this section, we characterize properties of the optimal investment decisions by the players.

6.4.1 Uniqueness of PNE

We first show the uniqueness of the PNE for the Behavioral Multi-Target Security Game (defined in Section 6.2).

Theorem 6.4.1. *Suppose that the asset values for the defender and attacker share a common ordering (i.e., $L_1 \geq L_2 \geq \cdots \geq L_n$ and $G_1 \geq G_2 \geq \cdots \geq G_n$). Under Assumption 8, if $p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}}) \in [0, \frac{1}{\mathrm{e}})\forall x_{\mathrm{i}}, y_{\mathrm{i}} \in \mathbb{R}_{\geq 0}$, then the PNE of the Behavioral Multi-Target Security Game is unique.*

Proof. To prove the uniqueness of the PNE, we follow the argument of Rosen [54] by proving that the weighted non-negative sum of our payoff functions is diagonally strictly concave.

Let us denote the payoff functions of the defender and attacker as $\phi_1(\mathbf{x}, \mathbf{y})$ and $\phi_2(\mathbf{x}, \mathbf{y})$, respectively. Note that $\phi_1(\mathbf{x}) = -C_{\mathcal{D}}(\mathbf{x}, \mathbf{y})$ and $\phi_2(\mathbf{x}) = U_{\mathcal{A}}(\mathbf{x}, \mathbf{y})$. Now, define $\mathbf{r} = [r_1 \;\; r_2]$, and let us define $\sigma(\mathbf{x}, \mathbf{y}, \mathbf{r})$ as the weighted non-negative sum of the two payoff functions $\phi_1(\mathbf{x}, \mathbf{y})$ and $\phi_2(\mathbf{x}, \mathbf{y})$ as follows:

$$\sigma(\mathbf{x}, \mathbf{y}, \mathbf{r}) = \sum_{\mathrm{i}=1}^{2} r_{\mathrm{i}}\, \phi_{\mathrm{i}}(\mathbf{x}, \mathbf{y}) = -r_1 \sum_{\mathrm{i}=1}^{n} L_{\mathrm{i}}\, w_{\mathcal{D}}(p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}})) + r_2 \sum_{\mathrm{i}=1}^{n} G_{\mathrm{i}}\, w_{\mathcal{A}}(p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}})).$$

Now, let us define the function $g(\mathbf{x}, \mathbf{y}, \mathbf{r})$ as follows:

$$g(\mathbf{x}, \mathbf{y}, \mathbf{r}) = \begin{bmatrix} r_1\, \nabla_{\mathbf{x}}\, \phi_1(\mathbf{x}, \mathbf{y}) \\ r_2\, \nabla_{\mathbf{y}}\, \phi_2(\mathbf{x}, \mathbf{y}) \end{bmatrix} = \begin{bmatrix} -r_1\, \nabla_{\mathbf{x}}\, C_{\mathcal{D}}(\mathbf{x}, \mathbf{y}) \\ r_2\, \nabla_{\mathbf{y}}\, U_{\mathcal{A}}(\mathbf{x}, \mathbf{y}) \end{bmatrix}$$

$$= \begin{bmatrix} -r_1\, L_1\, \frac{\partial(w_{\mathcal{D}}(p_1(x_1, y_1)))}{\partial x_1} \\ -r_1\, L_2\, \frac{\partial(w_{\mathcal{D}}(p_2(x_2, y_2)))}{\partial x_2} \\ \vdots \\ -r_1\, L_n \frac{\partial(w_{\mathcal{D}}(p_n(x_n, y_n)))}{\partial x_n} \\ r_2\, G_1\, \frac{\partial(w_{\mathcal{A}}(p_1(x_1, y_1)))}{\partial y_1} \\ \vdots \\ r_2\, G_n\, \frac{\partial(w_{\mathcal{A}}(p_n(x_n, y_n)))}{\partial y_n} \end{bmatrix}.$$

To show that $\sigma(\mathbf{x}, \mathbf{y}, \mathbf{r})$ is diagonally strictly concave, it is sufficient to show that the symmetric matrix $[G(\mathbf{x}, \mathbf{y}, \mathbf{r}) + G^T(\mathbf{x}, \mathbf{y}, \mathbf{r})]$ is negative definite for some $\mathbf{r} > \mathbf{0}$ where $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{y} \in \mathbb{R}^n$, where $G(\mathbf{x}, \mathbf{y}, \mathbf{r})$ is the Jacobian with respect to $\mathbf{x}$ and $\mathbf{y}$ of $g(\mathbf{x}, \mathbf{y}, \mathbf{r})$ [54].

Now, we can write $G(\mathbf{x}, \mathbf{y}, \mathbf{r})$ as

$$G(\mathbf{x}, \mathbf{y}, \mathbf{r}) = \begin{bmatrix} G_1(\mathbf{x}, \mathbf{y}, \mathbf{r}) & G_2(\mathbf{x}, \mathbf{y}, \mathbf{r}) \\ G_3(\mathbf{x}, \mathbf{y}, \mathbf{r}) & G_4(\mathbf{x}, \mathbf{y}, \mathbf{r}) \end{bmatrix},$$

where $G_1(\mathbf{x}, \mathbf{y}, \mathbf{r})$, $G_2(\mathbf{x}, \mathbf{y}, \mathbf{r})$, $G_3(\mathbf{x}, \mathbf{y}, \mathbf{r})$, and $G_4(\mathbf{x}, \mathbf{y}, \mathbf{r})$ each have dimension $n \times n$ and are given by:

$$G_1(\mathbf{x}, \mathbf{y}, \mathbf{r}) = r_1 \operatorname{diag}(-L_1 \frac{\partial^2 w_{\mathcal{D}}(p(x_1, y_1))}{\partial x_1^2}, \cdots, -L_n \frac{\partial^2 w_{\mathcal{D}}(p(x_n, y_n))}{\partial x_n^2}),$$

$$G_2(\mathbf{x}, \mathbf{y}, \mathbf{r}) = r_1 \operatorname{diag}(-L_1 \frac{\partial^2 w_{\mathcal{D}}(p(x_1, y_1))}{\partial x_1 \partial y_1}, \cdots, -L_n \frac{\partial^2 w_{\mathcal{D}}(p(x_n, y_n))}{\partial x_n \partial y_n}),$$

$$G_3(\mathbf{x}, \mathbf{y}, \mathbf{r}) = r_2 \operatorname{diag}(G_1 \frac{\partial^2 w_{\mathcal{A}}(p(x_1, y_1))}{\partial y_1 \partial x_1}, \cdots, G_n \frac{\partial^2 w_{\mathcal{A}}(p(x_n, y_n))}{\partial y_n \partial x_n}),$$

$$G_4(\mathbf{x}, \mathbf{y}, \mathbf{r}) = r_2 \operatorname{diag}(G_1 \frac{\partial^2 w_{\mathcal{A}}(p(x_1, y_1))}{\partial y_1^2}, \cdots, G_n \frac{\partial^2 w_{\mathcal{A}}(p(x_n, y_n))}{\partial y_n^2}).$$

Now, define the symmetric real matrix $M(\mathbf{x}, \mathbf{y}, \mathbf{r})$ as

$$M(\mathbf{x}, \mathbf{y}, \mathbf{r}) = [G(\mathbf{x}, \mathbf{y}, \mathbf{r}) + G^T(\mathbf{x}, \mathbf{y}, \mathbf{r})].$$

Now, we prove that $M(\mathbf{x}, \mathbf{y}, \mathbf{r})$ is negative definite by showing that $\mathbf{u}^T M(\mathbf{x}, \mathbf{y}, \mathbf{r})\mathbf{u} < 0$ for all non-zero vectors $\mathbf{u} = \begin{bmatrix} u_1 & u_2 & \dots & u_{2n} \end{bmatrix}^\intercal$ as follows:

$$\mathbf{u}^T M(\mathbf{x}, \mathbf{y}, \mathbf{r})\mathbf{u} = -2r_1 \left(\sum_{\mathrm{i}=1}^{n} u_{\mathrm{i}}^2 L_{\mathrm{i}} \frac{\partial^2 w_{\mathcal{D}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial x_{\mathrm{i}}^2} \right) + 2r_2 \left(\sum_{\mathrm{i}=1}^{n} u_{n+\mathrm{i}}^2 G_{\mathrm{i}} \frac{\partial^2 w_{\mathcal{A}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial y_{\mathrm{i}}^2} \right)$$

$$+ 2\sum_{\mathrm{i}=1}^{n} u_{\mathrm{i}} u_{n+\mathrm{i}} \left(-r_1 L_{\mathrm{i}} \frac{\partial^2 w_{\mathcal{D}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial x_{\mathrm{i}} \partial y_{\mathrm{i}}} + r_2 G_{\mathrm{i}} \frac{\partial^2 w_{\mathcal{A}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial y_{\mathrm{i}} \partial x_{\mathrm{i}}} \right). \quad (6.10)$$

In (6.10), we have $\frac{\partial^2 w_{\mathcal{D}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial x_{\mathrm{i}}^2} > 0 \forall \mathrm{i} = 1, \ldots, n$ (since $p_{\mathrm{i}}(x_{\mathrm{i}}, y_{\mathrm{i}}) \in [0, \frac{1}{\mathrm{e}})$, it follows directly from the proof of Lemma 10), $L_{\mathrm{i}} > 0$ (from defender's financial loss definition), and $u_{\mathrm{i}}^2 \geq 0$. Moreover, since $\frac{\partial^2 w_{\mathcal{A}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial y_{\mathrm{i}}^2} < 0 \forall \mathrm{i} = 1, \ldots, n$ (from Lemma 11), $G_{\mathrm{i}} > 0$ (from attacker's financial gain definition), the summation of the first and second term is always negative. Moreover, from Lemma 11(ii), we have $\frac{\partial^2 w_{\mathcal{D}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial x_{\mathrm{i}} \partial y_{\mathrm{i}}} < 0$ and $\frac{\partial^2 w_{\mathcal{A}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial y_{\mathrm{i}} \partial x_{\mathrm{i}}} < 0$. Thus, choosing

$$r_1 = \frac{1}{L_1 \left| \frac{\partial^2 w_{\mathcal{D}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial x_{\mathrm{i}} \partial y_{\mathrm{i}}} \Big|_{(x_{\mathrm{i}}^*, y_{\mathrm{i}}^*) \in \operatorname{argmin}_{x_{\mathrm{i}}, y_{\mathrm{i}}} \frac{\partial^2 w_{\mathcal{D}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial x_{\mathrm{i}} \partial y_{\mathrm{i}}}} \right|},$$

$$r_2 = \frac{1}{G_n \left| \frac{\partial^2 w_{\mathcal{A}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial y_{\mathrm{i}} \partial x_{\mathrm{i}}} \Big|_{(\bar{x}_{\mathrm{i}}, \bar{y}_{\mathrm{i}}) \in \operatorname{argmax}_{x_{\mathrm{i}}, y_{\mathrm{i}}} \frac{\partial^2 w_{\mathcal{A}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial y_{\mathrm{i}} \partial x_{\mathrm{i}}}} \right|}$$

where $(x_{\mathrm{i}}^*, y_{\mathrm{i}}^*)$ denote the investments on asset v_{i} with minimum $\frac{\partial^2 w_{\mathcal{D}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial x_{\mathrm{i}} \partial y_{\mathrm{i}}}$ across the n assets and $(\bar{x}_{\mathrm{i}}, \bar{y}_{\mathrm{i}})$ denote the investments on asset v_{i} with maximum $\frac{\partial^2 w_{\mathcal{A}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial y_{\mathrm{i}} \partial x_{\mathrm{i}}}$ across the n assets. Note that this choice minimizes r_1 by choosing the maximum possible value of its denominator since $\frac{\partial^2 w_{\mathcal{D}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial x_{\mathrm{i}} \partial y_{\mathrm{i}}} < 0$. Similarly, this choice maximizes r_2 by choosing the minimum possible value of its denominator since $\frac{\partial^2 w_{\mathcal{A}}(p(x_{\mathrm{i}}, y_{\mathrm{i}}))}{\partial y_{\mathrm{i}} \partial x_{\mathrm{i}}} < 0$. Therefore, this ensures that the third term is non-positive. Therefore, we have $\mathbf{u}^T M(\mathbf{x}, \mathbf{y}, \mathbf{r})\mathbf{u} < 0$ and thus $\sigma(\mathbf{x}, \mathbf{y}, \mathbf{r})$ is diagonally strictly concave for some $\mathbf{r} > \mathbf{0}$.

From Theorem 2 in [54], since $\sigma(\mathbf{x}, \mathbf{y}, \mathbf{r})$ is diagonally strictly concave for some $\mathbf{r} > \mathbf{0}$, the equilibrium point of the Behavioral Multi-Target Security Game is unique. □

6.4.2 Locations of Optimal Investments

We next characterize the optimal investments by the defender for a given set of investments by the attacker, and then do the same for the attacker. In particular, we denote the optimal investments by $\mathbf{x}^*(\alpha_{\mathcal{D}})$ and $\mathbf{y}^*(\alpha_{\mathcal{A}})$ to indicate that such investments will depend on the probability weighting parameters $\alpha_{\mathcal{D}}$ and $\alpha_{\mathcal{A}}$, respectively.

Proposition 6.4.1. *Consider a defender $\mathcal{D}$. Let the true probability of successful attack on each asset be given by (6.9). Consider a set of n assets whose losses can be put in the descending order $L_1 \geq L_2 \geq \cdots \geq L_n$. Suppose $y_1 \geq y_2 \geq \cdots \geq y_n \geq 0$, and that the pre-existing defense investments on each asset satisfy $a_1 = a_2 = \cdots = a_n$. Then, the optimal defense allocation of (6.5), denoted $\mathbf{x}^*(\alpha_\mathcal{D}) = \begin{bmatrix} x_1^*(\alpha_\mathcal{D}) & x_2^*(\alpha_\mathcal{D}) & \dots & x_n^*(\alpha_\mathcal{D}) \end{bmatrix}^\intercal$, has the property that $x_1^*(\alpha_\mathcal{D}) \geq x_2^*(\alpha_\mathcal{D}) \geq \cdots \geq x_n^*(\alpha_\mathcal{D})$.*

Proof. From the KKT conditions for the defender's best response, for every pair of nodes i and j with nonzero optimal investments by the defender, the marginals must satisfy

$$L_\mathrm{i} \frac{\partial(w_\mathcal{D}(p_\mathrm{i}(x_\mathrm{i}, y_\mathrm{i})))}{\partial x_\mathrm{i}}|_{x_\mathrm{i}=x_\mathrm{i}^*} = L_\mathrm{j} \frac{\partial(w_\mathcal{D}(p_\mathrm{j}(x_\mathrm{j}, y_\mathrm{j})))}{\partial x_\mathrm{j}}|_{x_\mathrm{j}=x_\mathrm{j}^*}.$$

If the probability of successful attack on the asset v_i is given by (6.9), then using the Prelec probability weighting function (2.3), the defender's perceived probability of successful attack on v_i would be

$$w_\mathcal{D}(p_\mathrm{i}(x_\mathrm{i}, y_\mathrm{i})) = \exp\left(-(x_\mathrm{i} + a_\mathrm{i} - \log\left(1 - \mathrm{e}^{-y_\mathrm{i}}\right))^{\alpha_\mathcal{D}}\right).$$

Denoting $k_\mathrm{i} = a_\mathrm{i} - \log(1 - \mathrm{e}^{-y_\mathrm{i}})$, the above marginals under the defender's best response would satisfy

$$L_\mathrm{i}(x_\mathrm{i}^* + k_\mathrm{i})^{\alpha_\mathcal{D}-1}\mathrm{e}^{-(x_\mathrm{i}^*+k_\mathrm{i})^{\alpha_\mathcal{D}}} = L_\mathrm{j}(x_\mathrm{j}^* + k_\mathrm{j})^{\alpha_\mathcal{D}-1}\mathrm{e}^{-(x_\mathrm{j}^*+k_\mathrm{j})^{\alpha_\mathcal{D}}} \tag{6.11}$$

for all nodes $v_\mathrm{i}, v_\mathrm{j}$ with nonzero optimal investments x_i^* and x_j^*, respectively.

Now, if $y_\mathrm{i} \geq y_\mathrm{j}$, we have

$$\begin{aligned} y_\mathrm{i} \geq y_\mathrm{j} &\iff 1 - \mathrm{e}^{-y_\mathrm{i}} \geq 1 - \mathrm{e}^{-y_\mathrm{j}} \\ &\iff -\log\left(1 - \mathrm{e}^{-y_\mathrm{i}}\right) \leq -\log\left(1 - \mathrm{e}^{-y_\mathrm{j}}\right) \\ &\iff a_\mathrm{i} - \log\left(1 - \mathrm{e}^{-y_\mathrm{i}}\right) \leq a_\mathrm{j} - \log\left(1 - \mathrm{e}^{-y_\mathrm{j}}\right) \\ &\iff k_\mathrm{i} \leq k_\mathrm{j}, \end{aligned}$$

where we used the assumption that $a_\mathrm{i} = a_\mathrm{j}\ \forall \mathrm{i} \neq \mathrm{j}$.

Using (6.11) and assuming without loss of generality that $\mathrm{i} < \mathrm{j}$, we obtain

$$\begin{aligned} L_{\mathrm{i}}(x_{\mathrm{i}}^* + k_{\mathrm{i}})^{\alpha_{\mathcal{D}}-1}\mathrm{e}^{-(x_{\mathrm{i}}^*+k_{\mathrm{i}})^{\alpha_{\mathcal{D}}}} &= L_{\mathrm{j}}(x_{\mathrm{j}}^* + k_{\mathrm{j}})^{\alpha_{\mathcal{D}}-1}\mathrm{e}^{-(x_{\mathrm{j}}^*+k_{\mathrm{j}})^{\alpha_{\mathcal{D}}}} \\ \Rightarrow \frac{\mathrm{e}^{-(x_{\mathrm{i}}^*+k_{\mathrm{i}})^{\alpha_{\mathcal{D}}}}}{(x_{\mathrm{i}}^* + k_{\mathrm{i}})^{1-\alpha_{\mathcal{D}}}} &= \frac{L_{\mathrm{j}}}{L_{\mathrm{i}}}\frac{\mathrm{e}^{-(x_{\mathrm{j}}^*+k_{\mathrm{j}})^{\alpha_{\mathcal{D}}}}}{(x_{\mathrm{j}}^* + k_{\mathrm{j}})^{1-\alpha_{\mathcal{D}}}} \\ &< \frac{\mathrm{e}^{-(x_{\mathrm{j}}^*+k_{\mathrm{j}})^{\alpha_{\mathcal{D}}}}}{(x_{\mathrm{j}}^* + k_{\mathrm{j}})^{1-\alpha_{\mathcal{D}}}} \end{aligned}$$

since $L_{\mathrm{i}} > L_{\mathrm{j}}$. Note that $\frac{\mathrm{e}^{-r^{\alpha_{\mathcal{D}}}}}{r^{1-\alpha_{\mathcal{D}}}}$ is a decreasing function of $r \in (0, \infty)$. Thus, from the above expression, we have

$$\begin{aligned} & x_{\mathrm{i}}^* + k_{\mathrm{i}} > x_{\mathrm{j}}^* + k_{\mathrm{j}} \\ & \Rightarrow x_{\mathrm{i}}^* = x_{\mathrm{j}}^* + k_{\mathrm{j}} - k_{\mathrm{i}} \geq x_{\mathrm{j}}^*, \end{aligned}$$

since $k_{\mathrm{i}} \leq k_{\mathrm{j}}$. This concludes the proof. □

The above result showed that the defender will invest more in higher-valued assets if the attacker has invested more in higher valued assets. We now show that a non-behavioral attacker will indeed prefer to invest more in higher-valued assets (even if the defender has invested more on those assets) under certain conditions, namely when there are significant differences in the values of the assets to the attacker.

Proposition 6.4.2. *Consider a non-behavioral attacker $\mathcal{A}$ (i.e., $\alpha_{\mathcal{A}} = 1$) and a non-behavioral defender $\mathcal{D}$ (i.e., $\alpha_{\mathcal{D}} = 1$). Let the true probability of successful attack on each asset be given by (6.9). Consider a set of n assets whose gains can be put in descending order $G_1 \geq G_2 \geq \cdots \geq G_n$ such that $\frac{G_{\mathrm{i}}}{G_{\mathrm{j}}} \geq \frac{L_{\mathrm{i}}}{L_{\mathrm{j}}}$ $\forall \mathrm{i} < \mathrm{j}$. Suppose that the pre-existing defense investments on each asset satisfy $a_1 = a_2 = \cdots = a_n$. Then,*

i. The attacker's investment at the PNE is given by $y_{\mathrm{i}}^* = y_{\mathrm{j}}^* + \log\left(\frac{G_{\mathrm{i}}}{G_{\mathrm{j}}}\right) - \log\left(\frac{L_{\mathrm{i}}}{L_{\mathrm{j}}}\right) \forall \mathrm{i}, \mathrm{j} \in \{1, \ldots, k_{\mathcal{A}}\}$ where $k_{\mathcal{A}}$ is the number of nodes that have nonzero attack investment at PNE. Formally, $k_{\mathcal{A}}$ is the largest k such that $P - \log\left(\frac{\prod_{\mathrm{i}=1}^{k} G_{\mathrm{i}}}{G_k^k}\right) + \log\left(\frac{\prod_{\mathrm{i}=1}^{k} L_{\mathrm{i}}}{L_k^k}\right) > 0$.

ii. The defender's investment at the PNE is given by $x_{\mathrm{i}}^* = x_{\mathrm{j}}^* + \log\left(\frac{L_{\mathrm{i}}}{L_{\mathrm{j}}}\right) \forall \mathrm{i}, \mathrm{j} \in \{1, \ldots, k_{\mathcal{D}}\}$ *where* $k_{\mathcal{D}}$ *is the number of nodes that have nonzero defense investment at PNE. Formally,* $k_{\mathcal{D}}$ *is the largest* k *such that* $B - \log\left(\frac{\prod_{\mathrm{i}=1}^{k} L_{\mathrm{i}}}{L_k^k}\right) > 0$.

Proof. From (6.7) and (6.8), we prove the PNE investments by showing that the defender's PNE investment is the defender's best response to the attacker's PNE investment and that the attacker's PNE investment is the attacker's best response to the defender's PNE investment.

(i) From the KKT conditions for the attacker's best response, for every pair of nodes i and j with nonzero optimal investments by the attacker, the marginals must satisfy $G_{\mathrm{i}} \frac{\partial(p_{\mathrm{i}}(x_{\mathrm{i}}^*, y_{\mathrm{i}}))}{\partial y_{\mathrm{i}}}|_{y_{\mathrm{i}}=y_{\mathrm{i}}^*} = G_{\mathrm{j}} \frac{\partial(p_{\mathrm{j}}(x_{\mathrm{j}}^*, y_{\mathrm{j}}))}{\partial y_{\mathrm{j}}}|_{y_{\mathrm{j}}=y_{\mathrm{j}}^*}$.

For the probability function (6.9), this condition becomes

$$G_{\mathrm{i}} \mathrm{e}^{-x_{\mathrm{i}}^* - a_{\mathrm{i}}} \mathrm{e}^{-y_{\mathrm{i}}^*} = G_{\mathrm{j}} \mathrm{e}^{-x_{\mathrm{j}}^* - a_{\mathrm{j}}} \mathrm{e}^{-y_{\mathrm{j}}^*}$$

for all nodes i, j with nonzero optimal investments y_{i}^* and y_{j}^*, respectively. Taking the logarithm of both sides and rearranging, we have

$$y_{\mathrm{i}}^* = y_{\mathrm{j}}^* + \log\left(\frac{G_{\mathrm{i}}}{G_{\mathrm{j}}}\right) - x_{\mathrm{i}}^* + x_{\mathrm{j}}^*, \tag{6.12}$$

where we used the assumption that $a_{\mathrm{i}} = a_{\mathrm{j}} \ \forall \mathrm{i} \neq \mathrm{j}$.

Now, substituting with the defender's investment $x_{\mathrm{i}}^* = x_{\mathrm{j}}^* + \log\left(\frac{L_{\mathrm{i}}}{L_{\mathrm{j}}}\right)$ in (6.12) yields

$$y_{\mathrm{i}}^* = y_{\mathrm{j}}^* + \log\left(\frac{G_{\mathrm{i}}}{G_{\mathrm{j}}}\right) - \log\left(\frac{L_{\mathrm{i}}}{L_{\mathrm{j}}}\right). \tag{6.13}$$

This shows that (i) is the attacker's best response to (ii).

Now, we derive the attack PNE investment on each node. First, note from (6.13) that if an asset v_{j} has nonzero attack investment at the PNE, since $\frac{G_{\mathrm{i}}}{G_{\mathrm{j}}} \geq \frac{L_{\mathrm{i}}}{L_{\mathrm{j}}} \forall \mathrm{i} < \mathrm{j}$, all assets v_{i} with $\mathrm{i} < \mathrm{j}$ would have also nonzero attack investment at the PNE as well. Formally, we have $y_1^* \geq y_2^* \geq \cdots \geq y_n^*$.

Suppose that the PNE investments are such that only the top k nodes $(v_1, v_2, \ldots, v_k)$ get nonzero investments from the attacker, and the remaining nodes $(v_{k+1}, \ldots, v_n)$ get zero investment. Substituting the PNE attack investments of all assets $y_2^*, \ldots, y_k^*$ in terms of the PNE attack investment of the first asset y_1^* from (6.13) into the budget constraint $\sum_{\mathrm{i}=1}^{k} y_{\mathrm{i}}^* = P$ yields

$$\begin{aligned}
& y_1^* + \sum_{\substack{\mathrm{i}=2 \\ \mathrm{i}\neq 1}}^{k} \left(y_1^* + \log\left(\frac{G_{\mathrm{i}}}{G_1}\right) - \log\left(\frac{L_{\mathrm{i}}}{L_1}\right)\right) = P \\
\implies & k y_1^* + \sum_{\substack{\mathrm{i}=2 \\ \mathrm{i}\neq 1}}^{k} \log\left(\frac{G_{\mathrm{i}}}{G_1}\right) - \sum_{\substack{\mathrm{i}=2 \\ \mathrm{i}\neq 1}}^{k} \log\left(\frac{L_{\mathrm{i}}}{L_1}\right) = P \\
\implies & k y_1^* + \log\left(\frac{\prod_{\mathrm{i}=2}^{k} G_{\mathrm{i}}}{G_1^{k-1}}\right) - \log\left(\frac{\prod_{\mathrm{i}=2}^{k} L_{\mathrm{i}}}{L_1^{k-1}}\right) = P \\
\implies & y_1^* = \frac{P - \log\left(\frac{\prod_{\mathrm{i}=1}^{k} G_{\mathrm{i}}}{G_1^k}\right) + \log\left(\frac{\prod_{\mathrm{i}=1}^{k} L_{\mathrm{i}}}{L_1^k}\right)}{k}.
\end{aligned}$$

Thus, the PNE attack investment on the remaining assets is calculated by substituting the derived y_1^* in (6.13) which yields

$$y_{\mathrm{i}}^* = \frac{P - \log\left(\frac{\prod_{\mathrm{i}=1}^{k} G_{\mathrm{i}}}{G_{\mathrm{i}}^k}\right) + \log\left(\frac{\prod_{\mathrm{i}=1}^{k} L_{\mathrm{i}}}{L_{\mathrm{i}}^k}\right)}{k}, \forall \mathrm{i} \in \{2, \ldots, k\}.$$

To have nonzero investment on all assets $v_1, \ldots, v_k$, we must have

$$P - \log\left(\frac{\prod_{\mathrm{i}=1}^{k} G_{\mathrm{i}}}{G_{\mathrm{i}}^k}\right) + \log\left(\frac{\prod_{\mathrm{i}=1}^{k} L_{\mathrm{i}}}{L_{\mathrm{i}}^k}\right) > 0 \forall \mathrm{i} \in \{1, \ldots, k\}.$$

However, since $y_1^* \geq y_2^* \geq \cdots \geq y_k^*$, it is sufficient to have

$$P - \log\left(\frac{\prod_{\mathrm{i}=1}^{k} G_{\mathrm{i}}}{G_k^k}\right) + \log\left(\frac{\prod_{\mathrm{i}=1}^{k} L_{\mathrm{i}}}{L_k^k}\right) > 0.$$

Thus, the number of nodes that have nonzero attack investment at PNE, denoted by $k_{\mathcal{A}}$, is the largest k such that the above inequality holds.

(ii) From part (i), since the number of nodes that have nonzero attack investment at PNE is $k_{\mathcal{A}}$, substituting (6.12) in budget constraint $\sum_{\mathrm{i}=1}^{k_{\mathcal{A}}} y_{\mathrm{i}}^* = P$ yields

$$
\begin{aligned}
& y_{\mathrm{j}}^* + \sum_{\substack{\mathrm{i}=1 \\ \mathrm{i}\neq\mathrm{j}}}^{k_{\mathcal{A}}} \left(y_{\mathrm{j}}^* + \log\left(\frac{G_{\mathrm{i}}}{G_{\mathrm{j}}}\right) - x_{\mathrm{i}} + x_{\mathrm{j}} \right) = P \\
\implies & k_{\mathcal{A}}\, y_{\mathrm{j}}^* + \sum_{\substack{\mathrm{i}=1 \\ \mathrm{i}\neq\mathrm{j}}}^{k_{\mathcal{A}}} \log\left(\frac{G_{\mathrm{i}}}{G_{\mathrm{j}}}\right) - \sum_{\substack{\mathrm{i}=1 \\ \mathrm{i}\neq\mathrm{j}}}^{k_{\mathcal{A}}} x_{\mathrm{i}} + \sum_{\substack{\mathrm{i}=1 \\ \mathrm{i}\neq\mathrm{j}}}^{k_{\mathcal{A}}} x_{\mathrm{j}} = P \\
\overset{(a)}{\implies} & k_{\mathcal{A}}\, y_{\mathrm{j}}^* + \log\left(\frac{\prod_{\mathrm{i}=1}^{k_{\mathcal{A}}} G_{\mathrm{i}}}{G_{\mathrm{j}}^{k_{\mathcal{A}}}}\right) - B + k_{\mathcal{A}}\, x_{\mathrm{j}} = P \\
\implies & y_{\mathrm{j}}^* = \frac{P + B - \log\left(\frac{\prod_{\mathrm{i}=1}^{k_{\mathcal{A}}} G_{\mathrm{i}}}{G_{\mathrm{j}}^{k_{\mathcal{A}}}}\right)}{k_{\mathcal{A}}} - x_{\mathrm{j}}
\end{aligned}
$$

for any node $v_{\mathrm{j}} \in \{v_1, \ldots, v_{k_{\mathcal{A}}}\}$. Note that (a) holds since $y_{\mathrm{i}}^* = 0 \forall \mathrm{i} > k_{\mathcal{A}}$. Thus, from Assumption 8, we have $p_{\mathrm{i}}(x_{\mathrm{i}}, 0) = 0$ and thus at the PNE, we have $x_{\mathrm{i}} = 0 \forall \mathrm{i} > k_{\mathcal{A}}$.

Now, substituting y_{j}^* in the defender's cost (6.3) yields

$$
\begin{aligned}
\overline{C}_{\mathcal{D}}(\mathbf{x}, \mathbf{y}^*) &= \sum_{\mathrm{i}=1}^{k_{\mathcal{A}}} L_{\mathrm{i}} \mathrm{e}^{-x_{\mathrm{i}} - a_{\mathrm{i}}} (1 - \mathrm{e}^{-y_{\mathrm{i}}^*}) \\
&= \sum_{\mathrm{i}=1}^{k_{\mathcal{A}}} L_{\mathrm{i}} \left(\mathrm{e}^{-x_{\mathrm{i}} - a_{\mathrm{i}}} - \mathrm{e}^{-a_{\mathrm{i}} - \frac{P + B - \log\left(\frac{\prod_{\mathrm{j}=1}^{k_{\mathcal{A}}} G_{\mathrm{j}}}{G_{\mathrm{i}}^{k_{\mathcal{A}}}}\right)}{k_{\mathcal{A}}}} \right)
\end{aligned}
$$

Now, from the KKT conditions for the defender's best response, every pair of nodes i and j with nonzero optimal investments, the marginals must satisfy

$$
\frac{\partial(\overline{C}_{\mathcal{D}}(x, y^*))}{\partial x_{\mathrm{i}}}\Big|_{x_{\mathrm{i}} = x_{\mathrm{i}}^*} = \frac{\partial(\overline{C}_{\mathcal{D}}(x, y^*))}{\partial x_{\mathrm{j}}}\Big|_{x_{\mathrm{j}} = x_{\mathrm{j}}^*}.
$$

Thus, we have $L_{\mathrm{i}} \mathrm{e}^{-x_{\mathrm{i}}^* - a_{\mathrm{i}}} = L_{\mathrm{j}} \mathrm{e}^{-x_{\mathrm{j}}^* - a_{\mathrm{j}}}$ for all nodes i, j with nonzero optimal investments x_{i}^* and x_{j}^*, respectively. Taking the logarithm of both sides and rearranging, we have

$$
x_{\mathrm{i}}^* = x_{\mathrm{j}}^* + \log\left(\frac{L_{\mathrm{i}}}{L_{\mathrm{j}}}\right), \tag{6.14}
$$

where we used the assumption that $a_{\mathrm{i}} = a_{\mathrm{j}}\ \forall \mathrm{i} \neq \mathrm{j}$. This shows that (ii) is the defender's best response to (i).

Similar to part (i), suppose that only the top k nodes get nonzero investments from the defender at the PNE. Substituting the PNE defense investments of all assets $x_2^*, \ldots, x_k^*$ in terms of the PNE defense investment of the first asset x_1^* from (6.14) into the budget constraint $\sum_{\mathrm{i}=1}^{k} x_{\mathrm{i}}^* = B$ yields

$$x_{\mathrm{i}}^* = \frac{B - \log\left(\frac{\prod_{\mathrm{i}=1}^{k} L_{\mathrm{i}}}{L_{\mathrm{i}}^k}\right)}{k}, \forall \mathrm{i} \in \{1, \ldots, k\}.$$

Thus, the number of nodes that have nonzero defense investment at PNE, denoted by $k_{\mathcal{D}}$, is the largest k such that the above inequality holds.

From the above analysis, we show that (i) and (ii) satisfies (6.8) and (6.7) simultaneously and thus (i) and (ii) are PNE investments of the attacker and the defender, respectively. □

The above results shows that if the asset values for the defender and attacker share a common ordering and if the values to the attacker are significantly different between the assets, then, in the PNE, both players invest more in their higher valued assets (noting that the attacker would invest the same in all assets if the ratio of gains are exactly the ratio of losses for any two assets within the CPS, i.e., $\frac{G_{\mathrm{i}}}{G_{\mathrm{j}}} = \frac{L_{\mathrm{i}}}{L_{\mathrm{j}}} \forall \mathrm{i} < \mathrm{j}$). We will show an example of such a PNE later (emphasizing the CPS defender's investments and the attacker's efforts) in our numerical simulations in Section 6.5.

Remark 10. *Note that if the asset values to the attacker are the same (i.e., $G_1 = G_2 = ... = G_n$) and if $L_{\mathrm{i}} \geq L_{\mathrm{j}}\ \forall \mathrm{i} < \mathrm{j}$, we have $y_{\mathrm{i}}^* \leq y_{\mathrm{j}}^*\ \forall \mathrm{i} < \mathrm{j}$. This indicates that under homogeneous valuations, the non-behavioral attacker would invest more in the assets that are less-important to the defender since they are expected to be less-protected.*

6.5 Numerical Simulations

In this section, we provide numerical simulations results to validate our findings in Section 6.4 and to show the effect of behavioral decision-making.

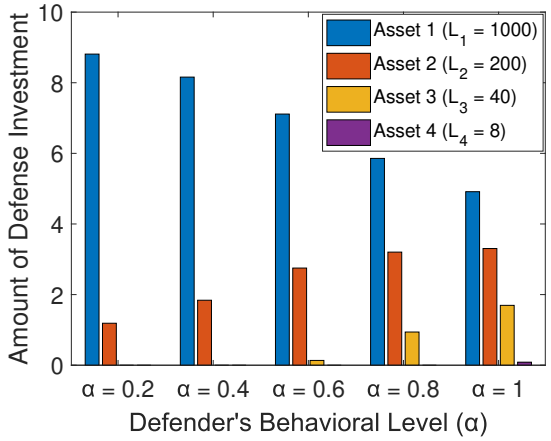


Figure 6.2. Effect of behavioral probability weighting on the defense investments on the four assets. The asset with the highest financial loss takes higher portion of the defense investments as the defender becomes more behavioral (i.e., α decreases) while the attacker is non-behavioral.

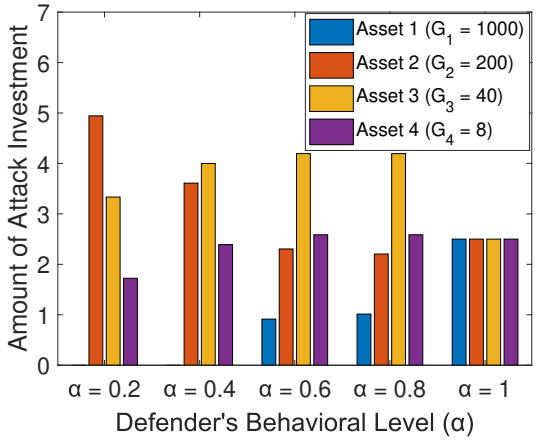


Figure 6.3. Effect of defender's behavioral probability weighting on the attack investments on the four assets. The asset with the highest financial gain takes much lower portion of the attack investments as the defender becomes more behavioral while the attacker is non-behavioral.

6.5.1 Experimental Setup

We emulated four critical assets (or targets). For the defender, the first asset has very high loss (i.e., $L_1 = 1000$) while the second and third assets have lower losses (with $L_2 = 200$, $L_3 = 40$) and the fourth asset has the least loss ($L_4 = 8$). For the attacker, we employ symmetric gains for successful attack (i.e., $G_1 = 1000$, $G_2 = 200$, $G_3 = 40$, and $G_4 = 8$). We let the total defense budget for defending the three critical assets and the total attack budget to compromise them be $B = 10$ and $P = 10$, respectively. The probability of successful attack on each of the assets is given by $p(x, y) = \mathrm{e}^{-x-1}(1 - \mathrm{e}^{-y})$ where x and y are the defense and attack investment on that asset, respectively. The above function satisfies the conditions in Assumption 2. We followed the best response dynamics notion to calculate the optimal investments of each player at the PNE. All of these optimal investments were calculated using Matlab Optimization toolbox.

6.5.2 Effect of Perception on Investments

In this subsection, we show the effect of probability misperception on the defense and attack investment decisions in the Behavioral Multi-Target Security Game. We note the ordering of defense investments on the assets (which is consistent with Proposition 3.4.1). Fig. 6.2 shows the difference in the defense investments for each of the assets as $\alpha_{\mathcal{D}}$ changes for the defender while keeping the attacker non-behavioral (with $\alpha_{\mathcal{A}} = 1$). We observe that the asset with the highest financial loss takes a higher portion of the defense investments as the defender becomes more behavioral (i.e., $\alpha_{\mathcal{D}}$ decreases). Fig. 6.3 illustrates the effect of defender's behavioral level on attacker's investment decision. The non-behavioral attacker's investments facing a non-behavioral defender is consistent with Proposition 6.4.2. Note also that when both players are non-behavioral, the PNE investments satisfy the condition for number of nodes with non-zero investments in Proposition 6.4.2 (Here, we have $k_{\mathcal{D}} = k_{\mathcal{A}} = 4$). We also observe that a non-behavioral attacker would put less resources on the first asset, with the highest gain, when facing behavioral defender who "over-protects" this asset. The insight here that the attacker would not waste attack resources on the highly-defended asset (Asset 1) but it tries to attack the remaining assets.

6.5.3 Effect of Behavioral Investments on CPS Defender's Loss

It is also worth considering the total expected system loss E_T of the defender in equilibrium, given by the sum of the real losses of all assets. First, we consider our previously considered loss valuations (i.e., $L_1 = 1000$, $L_2 = 200$, $L_3 = 40$, and $L_4 = 8$). As shown in Fig. 6.4, when the defender is non-behavioral (i.e., $\alpha = 1$) $E_T = 26.96$, while $E_T = 100.12$ when $\alpha = 0.2$ with a non-behavioral attacker in both scenarios. This considerable increase in the total real loss of the behavioral defender shows that probability weighting induces defender to invest in a sub-optimal manner, when some assets are much more valuable to the defender. Moreover, as the behavioral level increases (i.e., $\alpha_{\mathcal{D}}$ decreases), the effect of suboptimal investments is more pronounced in terms of the defender's total expected (true) loss. Fig. 6.4 also shows such insight for two alternative loss valuations scenarios.

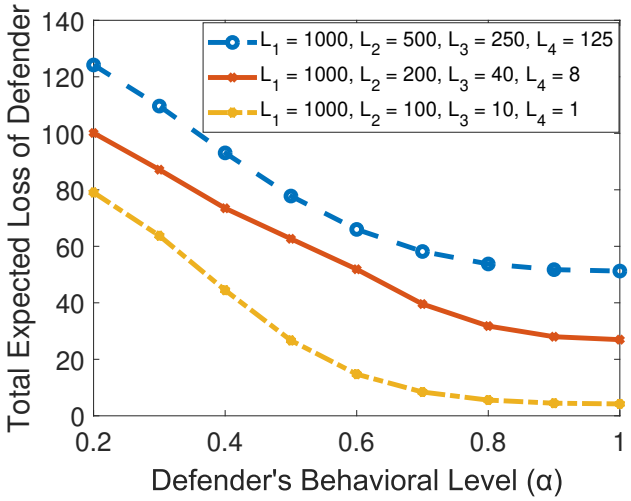


Figure 6.4. Effect of behavioral probability weighting on the true expected loss of the defender for different loss values for the assets. The cost of the defender (resp. the utility of the attacker) is worse (resp. better) if the defender becomes more behavioral while the attacker is non-behavioral

6.6 Summary of Findings

This chapter presented a game-theoretic framework that takes account of behavioral attitudes of defender and attacker in Multi-Target Security Game where the attacker and the defender place their investments to compromise and protect the target assets respectively. Specifically, we considered the scenario where the (human) defender misperceives the probabilities of successful attack in each asset. We then established the existence and uniqueness of PNE for our Behavioral Multi-Target Security Game. We then provided the optimal solutions for non-behavioral players for that game. Finally, we provided numerical simulations that validated our results and showed that nonlinear perceptions of probability can induce the defender to invest more on the assets with higher losses. An avenue for future research would be studying the setup of a behavioral attacker and its resulting properties. Moreover, considering the effect of behavioral decision-making on sequential games with multiple targets would be another avenue for future research.

7. Guiding Behavioral Decision-Makers towards Better Security Investment in Interdependent Systems

In the previous chapters, we modeled the *behavioral* biases of human decision-making in securing interdependent systems and showed that such behavioral decision-making leads to a suboptimal pattern of resource allocation compared to non-behavioral (rational) decision-making. In this chapter, we provide prospective solutions for such behavioral bias by introducing different learning algorithms. We first motivate the existence of behavioral bias in reality by providing empirical evidence for the existence of such behavioral bias model through a controlled subject study with 145 participants. We then propose three learning techniques for enhancing decision-making in multi-round setups. We illustrate the benefits of our decision-making model through multiple interdependent real-world systems and quantify the level of gain compared to the case in which the defenders are behavioral. We also show the benefit of our learning techniques against different attack models. We identify the effects of different system parameters (e.g., the defenders' security budget availability and distribution, the degree of interdependency among defenders, and collaborative defense strategies) on the degree of suboptimality of security outcomes due to behavioral decision-making.

7.1 Introduction

There are recent works [31], [36] that have started to leverage mathematical analysis to model and predict the effect of behavioral decision-making on the players' investments. However, these works have the following limitations. First, they have considered the impact of probability weighting in certain specific classes of interdependent security games. Second, these works did not consider multiple-round setups in which defenders can learn. In contrast to those, we consider general defense allocation techniques that can be applied to any system where its failure scenarios are modeled by an attack graph, and we propose multi-round learning algorithms to guide behavioral decision-makers in different setups and consider different types of attackers. The difference between our system and previous related work is shown in Table 7.1.

Our contributions:

In this chapter, we design a reasoning and security investment decision-making technique where we propose different learning-based techniques for guiding behavioral decision-makers towards optimal investment decisions for two different scenarios where each scenario represents whether the defender has knowledge of the adversary's history (i.e., chosen attack paths in previous rounds) or not. Our proposed techniques enhance the implemented security policy (in terms of reducing the total system loss when compromised by allocating limited security resources optimally). Our system has components for both single-round and multi-round setups as shown in Figure 7.1. We consider two classes of defenders.

Behavioral defenders: These defenders make security investment decisions under two types of cognitive biases. First, following prospect-theoretic, non-linear probability weighting models, they misperceive the probabilities of a successful attack on each edge of the attack graph. Second, they have a bias toward spreading their budget so that a minimum, non-zero investment is allocated to each edge of the attack graph. This second kind of bias is motivated by behavior that we observe in our human subject experiments (see Section 7.3).

Non-behavioral or rational defenders: These defenders make security investment decisions based on the classical models of fully rational decision-making. Specifically, they correctly perceive the risk on each edge within the attack graph of the system network.

On the other hand, almost all research that have considered behavioral economics in security and privacy has the common theme of considering individual choices regarding privacy and how people treat their own personal data [81] or entirely based on psychological studies [49]. To the best of our knowledge, none of these research considered the defense choices made by people in organizational contexts with interdependent system under control. On the contrary, our work considers scenarios that can be applied to critical infrastructure systems (e.g., cyber-physical systems).

We perform a human subject study with N = 145 participants where they choose defense allocations in two simple attack graphs. We then evaluate our proposed algorithms using five synthesized attack graphs that represent realistic interdependent systems and attack paths through them. These systems are DER.1 [17], (modelled by NESCOR), SCADA industrial control system, modeled using NIST guidelines for ICS [12], IEEE

Table 7.1. Comparison between the prior related work and our system in terms of the available features.

System	Multiple Defenders	Interdependent subnetworks	Analytical Framework	Behavioral Biases	Various Attack Types	Multiple Rounds
RAID08 [13], MILCOM06 [38]	✗	✓	✗	✗	✗	✗
S&P02 [16], CCS12 [11]	✗	✗	✓	✗	✗	✗
S&P09 [81], EC18 [82], ACSAC12 [49]	✗	✗	✗	✓	✗	✗
ICC17 [36]	✗	✓	✓	✓	✗	✗
TCNS20 [77], TCNS18 [31]	✓	✓	✓	✓	✗	✗
Our System	✓	✓	✓	✓	✓	✓

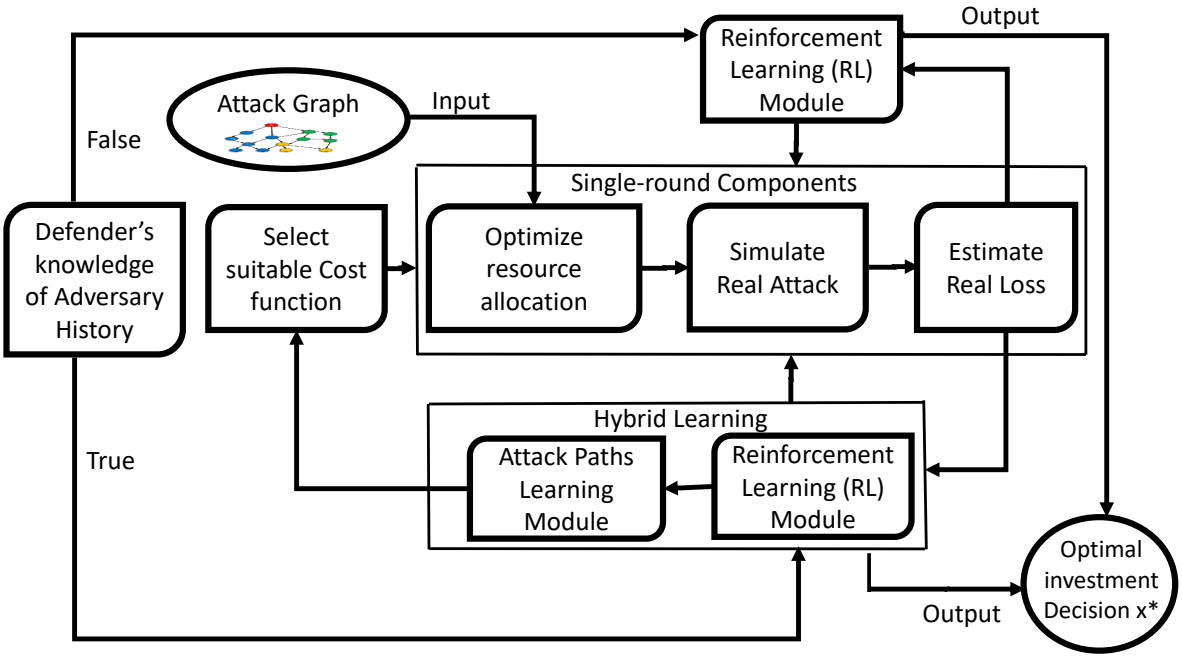
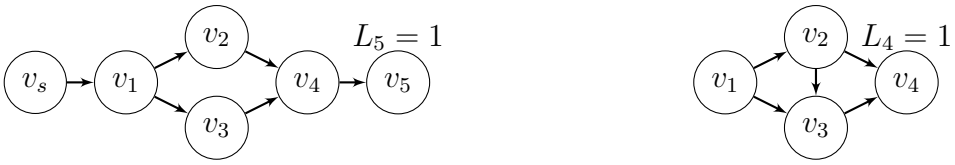


Figure 7.1. A high level overview of our system flow, available features and main components (e.g., single-round and Hybrid Learning).

300-bus smart grid [37], E-commerce [13], and VOIP [13]. We do a benchmark comparison with two prior solutions for optimal security controls with attack graphs [16], [38], and quantify the level of the underestimation of loss compared to our system's evaluation where defenders are behavioral. In conducting our analysis and obtaining these results based on a behavioral model, 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 (Equation 2.6), the estimation of baseline attack probabilities (Table 8.2) and the types of defense mechanisms (Section 7.5.5) in our formulations.



(a) An attack graph with a min-cut edge. (b) An attack graph with a cross-over edge.

Figure 7.2. The attack graph in (a) is used to illustrate the sub-optimal investment decisions of behavioral defenders. The attack graph in (b) is used in the human subject experiment to isolate the spreading effect.

In summary, this chapter makes the following contributions:

i. We propose a *security investment guiding* technique for the defenders of interdependent systems where defenders' assets have mutual interdependencies. We show the effect of *behavioral* biases of human decision-making on system security and we quantify the level of gain due to our decision-making technique where defenders are behavioral.

ii. We validate the existence of bias via a controlled subject study and illustrate the benefits of our decision-making through multiple real-world interdependent systems. We also analyze the different system parameters that affect the security of interdependent systems under our behavioral model.

iii. We propose three learning techniques to improve defense decisions in multi-round scenarios against different attack models that affect the security of interdependent systems. We incorporate such effects with behavioral decision-making.

7.2 Spreading Nature of Security Investments

Recall that each defender D_k seeks to minimize her *perceived expected cost* given by

$$C_k(x_k, \mathbf{x}_{-k}) = \sum_{v_m \in V_k} L_m \left(\max_{P \in \mathcal{P}_m} \prod_{(v_{\mathrm{i}}, v_{\mathrm{j}}) \in P} w_k \left(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) \right) \right).$$

We augment our model with another aspect of behavioral decision-making, which we call *spreading*. A defender with this characteristic spreads some of her investments on all edges of the attack graph, even when some edges are unlikely to be exploited for attacks. Spreading here is inspired by *Naïve Diversification* [83] from behavioral economics, where humans have

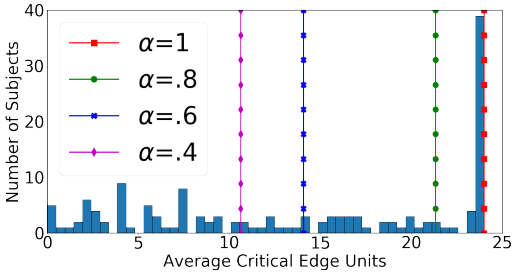


Figure 7.3. Subjects' investments on the critical edge. Vertical lines with dots show optimal allocations at specific behavioral levels (α).

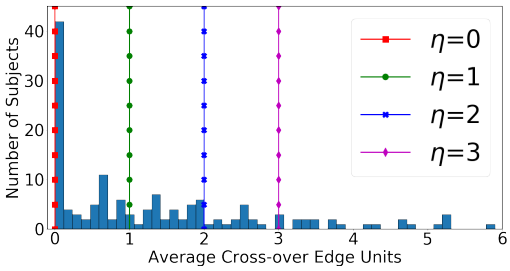


Figure 7.4. Subjects' investments on the cross-over edge. Vertical lines with dots show optimal allocations at specific spreading levels (η).

a tendency to split investments evenly over the available options. This phenomenon has not been reported earlier for security decision-making, to the best of our knowledge, and we infer this behavior from our human subject study (detailed in Section 7.3). We capture this effect by adding another constraint to our model in (2.5): for each defender D_k, we set $x^k_{i,j} \geq \eta_k$, where η_k is the minimum investment D_k makes on any edge. The value $\eta_k = 0$ gives us the behavioral decision with no spreading, i.e., with only behavioral probability weighting.

7.3 Human Subject Study

To validate the existence of behavioral bias in security allocations (captured by our model in Chapter 2.2), incentivized experiments were conducted on 145 students in an Experimental Economics Laboratory at a large public university. Subject demographics are presented below.

Human Subject Demographics: The 145 human subjects in our experiment are comprised of 78 males (53.79%) and 67 females (46.21%). They belong to various majors on campus, with the three largest being Management/Business (24.8%), Engineering (24.2%), and Science (23.5%). Regarding year in college, 6.9% are 1st year, 13.1% are 2nd year, 21.38% are 3rd year, 35.86% are 4th year, and 22.76% are graduate students. Regarding the GPA distribution, 44.83% have GPAs between 3.5 and 4, 35.17% between 3 and 3.5, and 17.93% between 2.5 and 3.

Subjects participated in the role of a defender, and allocated 24 discrete defense units over edges in each network. Subjects made their decisions on a computerized interface, and faced 10 rounds for each network, receiving feedback after each round indicating whether the attack was successful or not (i.e., the asset was compromised). Subjects received comprehensive written instructions on the decision environment that explained how their investment allocation mapped into the probability of edge defense, and what was considered a successful defense. Subjects received a base payment of $5.00 for their participation. In addition, we randomly selected one round from each network and if the subject successfully defended the critical node in that round, she received an additional payment of $7.50.

7.3.1 Network (A) with Critical Edge

This human experiment is on a network similar to Figure 7.2a, except that there is only one critical edge (v_4, v_5) i.e., $v_s = v_1$. Figure 7.3 shows the average investment allocation to the critical edge, based on 1450 investment decisions (i.e., 10 decisions from each of the 145 subjects). It shows the proportion of subjects who are non-behavioral (those at the vertical red line of $\alpha = 1$, 27%), as well as heterogeneity in α, with observations further to the left being more behavioral. Subjects to the left of the $\alpha = 0.4$ line (approximately 10 units allocated to the critical edge) are not necessarily exhibiting $\alpha < 0.4$. Those who allocate between 5 and 10 units to the critical edge could have a strong preference for spreading. We observe that after round 4, the average investment on the critical edge in each round is higher than the initial investment in round 1 (Figure 7.5). The average increase summed across the 10 rounds is one defense unit. This means that subjects become less behavioral on average through learning.

7.3.2 Network (B) with Cross-over Edge

This experiment used the attack graph from Figure 7.2b. This attack graph is suitable to separate the spreading behavioral bias from the behavioral probability weighting, since for any $0 < \alpha \leq 1$, the optimal decision is to put zero defense units on the cross-over edge (v_2, v_3). Figure 7.4 shows the average investment allocation on the cross-over edge based on

1450 investment decisions. We see that the proportion of subjects that are non-behavioral, i.e., invest nothing on the cross-over edge, is 29%. We observe that the average of subjects' investments on the cross-over edge in each round, shows a weak downward trend (Figure 7.6 below). Taken together, these human experiments provide support for our behavioral model with probability weighting and spreading factors.

7.3.3 Average Investments of Multi-rounds

We show the average investments for each round for both of the attack graphs tested in our human subject study. Note that we emulated the reinforcement learning environment where in each round as simulated attack is run and result shown to the subject [78]. In particular, after the subject allocates her investments, a simulated attack is run and we show the subject if the critical asset was compromised or not and give her experimental points if she successfully defended the asset [78].

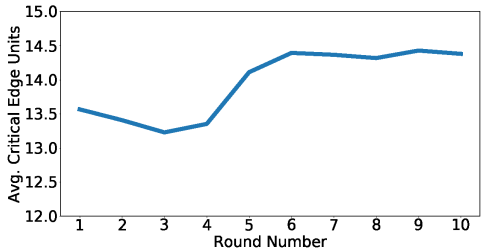


Figure 7.5. Average of all subjects' investments on the critical edge vs experiment rounds. The upward trend indicates that on average, subjects are learning.

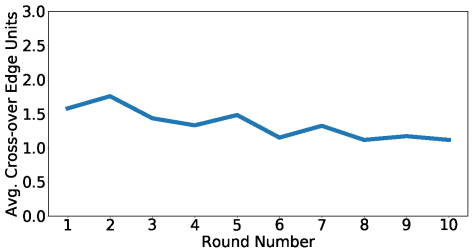


Figure 7.6. Average of all subjects' investments on the cross-over edge vs experiment rounds. There is only a weak downward trend in spreading behavior.

7.3.4 Generalizability of the study

The applicability of this subject study to security experts is motivated by the fact that numerous academic studies of even the most highly-trained specialists have shown that experts too have susceptibility to systematic failures of human cognition (e.g., [84], [85]).

In the meta-review article [85], 9 of 13 studies that make a direct comparison between student and professional subject pools find no evidence of differing behavior, and only 1 out of 13 studies finds that professionals behave more consistently with theory. Moreover, recent research has shown that cybersecurity professionals' probability perceptions are as susceptible to systematic biases as those of the general population [86], [87]. Finally, even if security experts exhibit weaker biases, this can result in sub-optimal security investments and their effects may be magnified due to the magnitude of losses associated with compromised 'real-world' assets.

7.4 Learning Over Rounds

Here we consider a defender who plays multiple rounds of the game, learning from observing the attack in each round. In each round, each defender plays the single-shot game with the attacker, allocating all her security budget. She then uses information collected during this interaction to inform her future decisions. In particular, we consider two different forms of learning: (1) what can the defender learn about an attacker over time, and (2) how can repeated interactions lead to decrease in the defenders' extent of behavioral decision-making (i.e., increase in α)? We answer these questions through casting them as repeated resource allocation and reinforcement learning problems, respectively.

7.4.1 Learning about the Attacker

Now, we assume that the defender can observe the attacker's past actions, e.g., via an intrusion detection system [13] or user metrics [88].

We propose an algorithm through which the defender learns the attack paths over time, and distributes her investments optimally accordingly over the edges. In particular, the steps of this algorithm for this defense technique, as outlined in Algorithm 1, are as follows. First, for each round, we compute the empirical frequency of the attacker's actions over the past N moves (i.e., the probability of choosing every attack path based on the most recent N choices). Then, we compute the best response of the defender to a modified version of the cost $C_k(x_k)$: this is a weighted version of the cost where each path P has a weight β_P

(computed from the previous step). The complexity of the algorithm therefore depends on the number of attack paths.

In Section 7.5, we compare the investment decisions prescribed by Algorithm 1 with those from our earlier single-shot setup where the defender exhibits no learning. In these comparisons, we consider three types of attackers: replay attackers, randomizing attackers, and adaptive attacker. Specifically, a *replay attacker* chooses the same attack path for every critical asset in every round. Such behavior may be due to limited observations [89], or when the attack process is automated. A *randomizing attacker*, on the other hand, chooses an attack path (for every critical asset v_m) randomly each round, i.e., with probability following a uniform distribution over the possible attack paths in $\mathcal{P}_m$. Such attackers have also been studied in other work using attack graph models [90]. We consider a third attacker type, the *adaptive attacker*, who chooses the least chosen attack path in the past N moves (for every critical asset).

In contrast to replay attacker and randomizing attacker, we assume that the adaptive attacker is aware that the defender's strategy considers the most recent N attacks, and thus the attacker engineers its attack history over a period of time so as to make additional gains on the future attack by choosing the least chosen attack path in the past N moves. Note that the attacker does not have a budget, he just chooses an attack path to each critical asset.

7.4.2 Reinforcement Learning for Reducing Behavioral Decision-Making

As shown in Section 7.3, the one-round investment decisions made by a behavioral defender D_k based on the decision model in Equation (2.5) are sub-optimal. It is therefore of interest to understand whether such defender can reduce her behavioral biases in a multi-round defense game by using her experience from previous rounds. In this section, we propose a learning technique through which the defender can make such progress towards a more rational model, i.e., leads to $\alpha^{\mathrm{j}} > \alpha^{\mathrm{i}}$, for some $\mathrm{j} > \mathrm{i}$, where α^{i} denotes the behavioral level in round i. Our proposed algorithm, outlined in Algorithm 2, uses a reinforcement

Algorithm 1 Learning Attack Paths

Input: Set of attack paths $\mathcal{P}_m$, number of rounds N_R and history of attack paths $(P^{t-N}, \cdots, P^{t-1})$

Output: Vector of investments over rounds, $\mathcal{O}$

Round Number = t = 0
while $t < N_R$ **do**
  for $v_m \in V_k$ **do**
    for *Path* $P \in \mathcal{P}_m$ **do**
      $\beta_P^t = \frac{1}{N} \sum_{\tau=t-N}^{t-1} [P^\tau = P]_1$
    end
  end
  $C_k^t(x_k) = \sum_{v_m \in V_k} L_m \Big(\sum_{P \in P_m} \beta_P^t \prod_{(v_\mathrm{i}, v_\mathrm{j}) \in P} w(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})) \Big)$
  $x_k^t \in argmin_{x_k \in X_k} C_k^t(x_k)$
  Append $(\mathcal{O}, x_k^t)$
end
Return $\mathcal{O}$

learning approach. Our algorithm is based on that of [91], adapted to our problem of security investment decision-making.

The algorithm proceeds as follows. Let $q^t(\alpha_\mathrm{i})$ denotes the defender's propensity to invest according to the behavioral level α_i at round t. We first initialize these propensities to the defender's initial behavioral level (i.e., $\alpha^0 = \alpha_\mathrm{i}$, $q^0(\alpha_\mathrm{i}) = A$, and $q^0(\alpha_\mathrm{j}) = B, \forall \mathrm{j} \neq \mathrm{i}$).[1] Then, for every round t, the defender does not know her behavioral level but she draws her defense budget decision in accordance to her reinforcement level. After the defender distributes her defense budget, she receives corresponding reinforcement R^t (which is the difference between the true loss $\hat{C}^t(x_k^t)$ calculated with the investments (budget allocation on edges) in round t, denoted by x_k^t, and the maximum possible true loss $\hat{C}_{max}$ (which is the initial loss). Thus, if the defender invests according to a more rational behavior (i.e., higher α) in round t, she receives higher reinforcement and thus the propensity to choose this investment again in next rounds ($q^{t+1}(\alpha_\mathrm{i})$) increases. For all other investments that are not observed in this round, the propensities of the corresponding behavioral levels do not change. Then, we

[1]↑In our evaluation, we show the convergence of Algorithm 2 under different possible values of the initial propensities of different behavioral levels (i.e., A and B in Algorithm 2). We also show that the convergence of Algorithm 2 depends on the true total loss of the investment, not the initial propensities.

update the probability distribution for the investments (resp. behavioral levels) for the next round. We repeat the process until we reach convergence (where the reinforcement learning model chooses $\alpha_{\mathrm{i}} = 1$ with a probability sufficiently close to 1) or we reach the maximum number of rounds N_R. The output of our algorithm is a time-series of behavioral level values. We emphasize that the learning comes from the reinforcements received each round which controls the propensity of the defender to choose particular budget distributions in next rounds and that the defender does not know the optimal investments apriori.

Algorithm 2 Reinforcement Learning to Reduce Behavioral Biases

Input: Set of behavioral levels α and number of rounds N_R

Output: Vector of behavioral level over rounds $\mathcal{O}$

Round Number = t = 0

$q^0(\alpha_{\mathrm{i}}) = A$ and $q^0(\alpha_{\mathrm{j}}) = B \forall \mathrm{j} \neq \mathrm{i}$

while $t < N_R$ *or not Convergence to* $\alpha_{\mathrm{i}} = 1$ **do**

  for $\alpha_{\mathrm{i}} \in \alpha$ **do**

    if α_{i} *was observed in round* t **then**

      $x_k^t \in argmin_{x_k \in X_k} C_k^t(x_k, \alpha_{\mathrm{i}})$

      $R^t = \hat{C}_{max} - \hat{C}_k^t(x_k^t)$

      $q^{t+1}(\alpha_{\mathrm{i}}) = q^t(\alpha_{\mathrm{i}}) + R^t$

    end

    else

      $q^{t+1}(\alpha_{\mathrm{i}}) = q^t(\alpha_{\mathrm{i}})$

    end

    $p^{t+1}(\alpha_{\mathrm{i}}) = \frac{q^{t+1}(\alpha_{\mathrm{i}})}{\sum_{\alpha_{\mathrm{i}} \in \alpha} q^{t+1}(\alpha_{\mathrm{i}})}$

  end

  Sample random α_{i} with probability $p^{t+1}(\alpha_{\mathrm{i}})$ to get α^{t+1}

  Append ($\mathcal{O}$, α^{t+1})

end

Return $\mathcal{O}$

Convergence of Algorithm 2 to rational behaviour: We now provide the discussion about the convergence of Algorithm 2. Note that the convergence of Algorithm 2 depends on the relation between the total loss (true cost) under rational behavior $\alpha = 1$ and the total loss (true cost) under behavioral bias $\alpha < 1$. We state this result in Lemma 12 and provide its proof below.

Lemma 12. *Let N_1 and N_{α_i} represent the number of rounds in which the defender chose to invest rationally and with behavioral level α_i, respectively. Let $\hat{C}_{opt}$ and $\hat{C}_i$ be the total real loss incurred by the defender when investing rationally and with behavioral level α_i, respectively. Then, we have*

i. If $q^0(\alpha_i) = q^0(1)$, then Algorithm 2 converges to rational behavior in the round N_R if $\frac{\hat{C}_{max}-\hat{C}_{opt}}{\hat{C}_{max}-\hat{C}_i} >> \frac{N_{\alpha_i}}{N_1}$.

ii. If $q^0(\alpha_i) = A_i$ and $q^0(1) = B$, then Algorithm 2 converges to rational behavior in the round N_R if $(N_1 - N_{\alpha_i})\hat{C}_{max} + N_{\alpha_i}(\hat{C}_i) - N_1(\hat{C}_{opt}) >> A_i - B$.

Proof. We calculate the propensities for each behavioral level. From Algorithm 2, we have

$$q^{N_R}(1) = q^0(1) + N_1(\hat{C}_{max} - \hat{C}_{opt})$$
$$q^{N_R}(\alpha_i) = q^0(\alpha_i) + N_{\alpha_i}(\hat{C}_{max} - \hat{C}_i)$$

(i) To reach convergence, $\forall \alpha_i \neq 1$ and $q^0(\alpha_i) = q^0(1)$, we have

$$q^{N_R}(1) >> q^{N_R}(\alpha_i) \iff N_1(\hat{C}_{max} - \hat{C}_{opt}) >> N_{\alpha_i}(\hat{C}_{max} - \hat{C}_i)$$
$$\iff \frac{\hat{C}_{max} - \hat{C}_{opt}}{\hat{C}_{max} - \hat{C}_i} >> \frac{N_{\alpha_i}}{N_1}$$

(ii) With a similar argument to (i), $\forall \alpha_i \neq 1$ and $q^0(\alpha_i) \neq q^0(1)$ where $q^0(\alpha_i) = A_i$ and $q^0(1) = B$, we have

$$q^{N_R}(1) >> q^{N_R}(\alpha_i)$$
$$\iff (N_1 - N_i)\hat{C}_{max} + N_i(\hat{C}_i) - N_1(\hat{C}_{opt}) >> A_i - B$$

Note that in all of the possible cases, $\hat{C}_i - \hat{C}_{opt} >> 0$ ensures convergence under any choice of A and $B \neq 0$ which is realistic where the real loss associated with suboptimal investments decisions is much higher compared to the real loss associated with optimal (i.e., rational) investments decisions. □

7.4.3 Hybrid-Learning Algorithm

In Algorithm 2 the defender learns through observing her payoffs in the last recent rounds. In Algorithm 1, the defender learns the attacker's chosen paths. Here, we combine these two forms of learning to create a hybrid learning algorithm. This algorithm is a modified version of Algorithm 2 where the cost $C_k^t(x_k, \alpha_{\mathrm{i}})$ is the cost proposed in Algorithm 1, which changes each round as the defender updates the weights of each path according to the history of attack paths. We will evaluate this hybrid-learning algorithm in Section 7.5 and will compare it with both of Algorithm 1 and Algorithm 2, described earlier in this section. As will be shown later in Section 7.5, this Hybrid-learning is useful to guide behavioral defenders for the different attack types that we consider in our work.

7.5 Evaluation

Our evaluation aims to answer the following questions:

- What is the gain of using our approaches for guiding behavioral decision-makers towards rational decision-making?
- How can we decrease level of behavioral bias over rounds?
- How does each system parameter affect the overall security level of the system with behavioral decision-making?

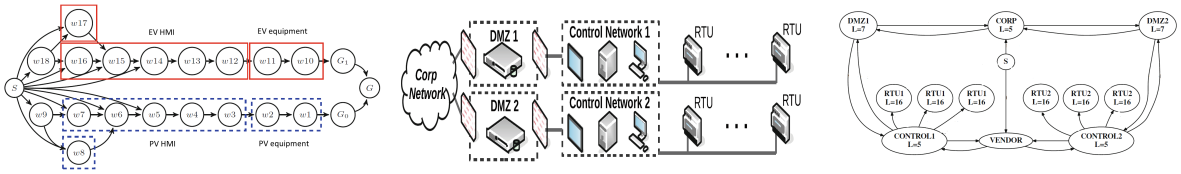
7.5.1 Experimental Setup

Dataset Description: We use five synthesized attack graphs that represent real-world interdependent systems with different sizes to evaluate our setups, i.e., different attacks, defense, and learning (See Table 7.2). Specifically, we consider 5 popular interdependent systems from the literature which are: DER.1 [17], SCADA (with internal attacks) [12], SCADA (with only external attacks), IEEE 300-bus smart grid [37], E-commerce [13], and VOIP [13]. In all of these systems, nodes represent attack steps (e.g., taking privilege of control unit software in SCADA, accessing customer confidential data such as credit card

Table 7.2. The one-round gain of our approach compared to behavioral investment decisions for the five studied interdependent systems.

System	# Nodes	# Edges	# Min-cut Edges	# Critical Assets	Avg Gain	Max Gain
SCADA-external	13	20	2	6	1.43	2.63
SCADA-internal [12]	13	26	8	6	4.43	9.42
DER.1 [17]	22	32	2	2	1.29	2.38
E-Commerce [13]	18	26	1	4	3.70	18.28
VOIP [13]	20	28	2	4	4.46	18.66
IEEE 300-bus [37]	300	822	98	69	5.85	11.25

information in E-commerce). Now, we give a detailed explanation of two of these systems; the SCADA and the IEEE 300 BUS systems (see Section 8.6.1 and [13], [17], [37] for detailed description of the rest of the systems). We generate the attack graphs using the CyberSage tool [17] which maps the failure scenarios of the system automatically into an attack graph given the workflow of that system, the security goals, and the attacker model.



(a) Attack Graph of DER System

(b) A high level network overview of the SCADA system

(c) Attack Graph of SCADA System

Figure 7.7. Attack graphs of DER.1 and SCADA case studies. The attack graphs of the remaining systems are given in Section 8.6.1.

SCADA system description: The SCADA system (shown in Figure 7.7b) is composed of two control subsystems, where each incorporates a number of cyber components, such as control subnetworks and remote terminal units (RTUs), and physical components, such as, valves controlled by the RTUs. This system is architected following the NIST guidelines for industrial control systems. For example, each subsystem is separated from external networks through a demilitarized zone (DMZ). The purpose of a DMZ is to add an additional layer of security between the local area networks of each control subsystem and the external/corporate networks, from where external attackers may attempt to compromise the system. The system implements firewalls both between the DMZ and the external networks,

as well as between the DMZ and its control subnetwork. Therefore, an adversary must bypass two different levels of security to gain access to the control subnetworks.

Mapping this system to our proposed security game model, each control subnetwork is owned by a different defender. These two subsystems are interdependent via the shared corporate network, as well as due to having a common vendor for their control equipment. The resulting interdependencies map to the attack graph shown in Figure 7.7c. The "Corp" and the "Vendor" nodes connect the two subnetworks belonging to the two different defenders and can be used as jump points to spread an attack from one control subsystem to the other. This system has six critical assets (i.e., 3 RTUs, Control Unit, CORP, and DMZ). The compromise of a control network "CONTROL i" will lead to loss of control of all 3 connected RTUs.

IEEE 300 BUS System Description: Finally, we consider the widely used benchmark IEEE 300 bus power grid network [37]. We define the network itself as the interdependency graph where each node represents a bus (i.e., the network has 300 nodes), and the physical interconnection between the buses represent the edges. Each bus has generators and/or load centers associated with it. As shown in Figure 7.8, the 300 bus network data divides the buses or nodes into 3 different regions containing 159, 78 and 63 nodes respectively. We assume that each region is managed by an independent entity.

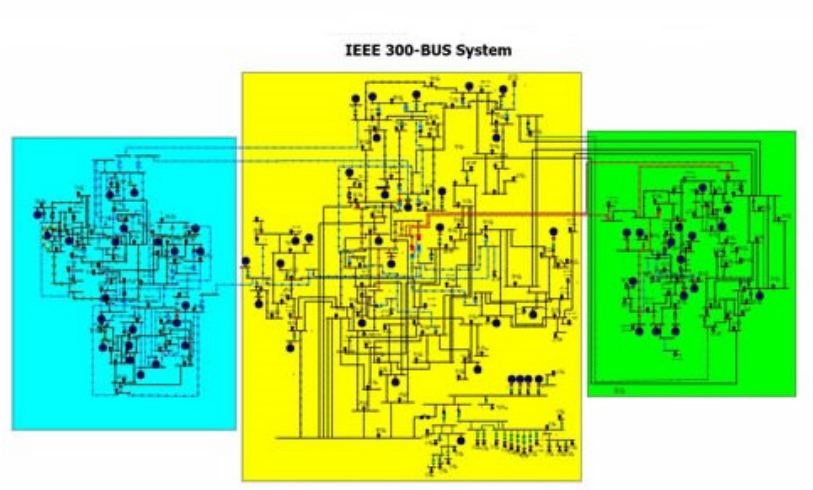


Figure 7.8. A high level overview of the IEEE 300-BUS (adapted from [37]). Each area has a different color.

Now, we present the various system parameters.

Baseline Probability of successful attack: Each edge in the attack graphs represents a real vulnerability. To create the baseline probability of attack on each edge (i.e., without any security investment), we first create a table of CVE-IDs (based on real vulnerabilities reported in the CVE database for 2000-2019). We then followed [24] to convert the attack's metrics (i.e., attack vector (AV), attack complexity (AC)) to a baseline probability of successful attack (e.g., Table 8.2 in illustrates such process for SCADA and DER.1). Interestingly, we show that the gain of rational vs. behavioral investments exists for any combination of baseline probabilities (as will be shown in Section 7.5.5).

Security Budget: We assume that the total budget available at the defenders' organization is B, and that an amount BT of this budget is set aside for security investments. We refer to $BT < 0.3B$, $0.3B < BT < 0.6B$, and $BT > 0.6B$, as low, medium, and high security budgets. For instance, $BT = \$10$ and $\$20$ reflect low and moderate budgets, respectively and $BT \geq \$30$ reflects high budgets in SCADA system given that $B = \$50$. We emphasize that the gain of our proposed techniques exists for any choice of budget (as will be shown in Section 7.5.5).

Convergence to Optimal Solution: In our experiments, to find the optimal investments, we use the notion of *best response dynamics*, where the investments of each defender D_k are iteratively updated based on the investments of the other defenders. In each iteration, the optimal investments for defender D_k can be calculated by solving the convex optimization problem in (2.5).[2] Note that the best response dynamics converge to a Nash equilibrium [12] and we study the security outcomes at that equilibrium.

7.5.2 Gain from Using Our Approach in One Round

Here, we show the gain that behavioral security decision-maker would have using our approaches.

Reduction in Defender's Total Loss: To show the gain of our proposed algorithm, we quantitatively compare the total system loss of the aforementioned five systems in two

[2]↑ Note that in the results of learning attack paths and Hybrid learning techniques, we use different cost function (shown in Algorithm 1).

scenarios which are assuming behavioral decision-maker without the help of our technique and with the help of our technique investments, respectively. We then calculate the gain as the ratio of the total system loss by behavioral decision-maker to the total system loss by our approach to quantify the benefit of using our proposed algorithm.

1) Average Gain: We define the Average Gain as the ratio of the weighted sum of total system loss by behavioral decision-maker to the total system loss by our approach assuming that 50% of the decision-makers are fully rational (with $\alpha = 1$) and 50% are behavioral defenders ($\alpha \in [0.4, 1)$); this is consistent with the range of behavioral parameters from prior experimental studies [15] and our subject study. Average Gain for all systems is shown in Table 7.2.

2) Maximum Gain: We define the Maximum Gain as the ratio of the total system loss by the highest behavioral defender ($\alpha = 0.4$) to the total system loss by rational ($\alpha = 1$) decision-maker (computed by our approach). Table 7.2 shows maximum gains which are 2.38, 9.43, 2.63, 11.25, 18.28, and 18.66 for the DER.1, SCADA-internal, SCADA-external, IEEE 300-bus, E-commerce, and VOIP respectively.

7.5.3 Learning over Rounds Results

Now, we consider the different setups where the defender learn over rounds using our proposed algorithms in Section 7.4. For some results, we only show results on the SCADA attack graph as we observe similar patterns on the remaining studied attack graphs.

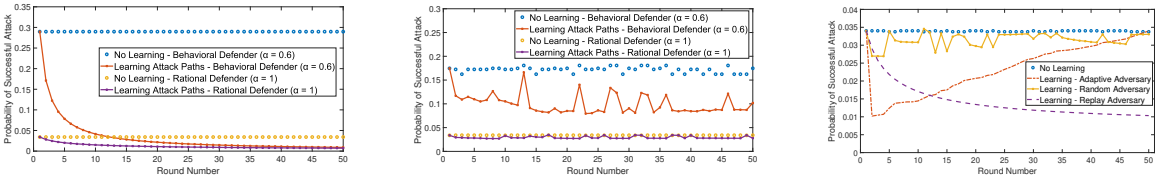
1) Learning of attack paths: We show the effect of learning attack paths over the rounds for all of the possible attack scenarios described in Section 7.4. We consider the five systems described earlier and simulate our learning algorithm over 50 rounds with considering medium budget. For each round, the attacker chooses one path for compromising each critical asset (for SCADA, we have six critical assets (i.e., 3 RTUs, Control Unit, CORP, and DMZ) and thus each round the attacker chooses six paths, one for each critical asset) and then the overall probability of successful attack is calculated. We show that the learning of attack paths is useful for both behavioral and rational defenders. Specifically, Figure 7.9a shows such effect of learning if the attacker chooses same attack paths for each critical asset.

Also, Figure 7.9b shows that our proposed algorithm helps enhancing system security even if the attacker chooses attack paths randomly over rounds since it captures an approximate distribution of the attacker choice of the paths over the rounds. Interestingly, behavioral defender that learns attack paths can eventually reach comparable security level as rational defender (with same security level if the attacker chooses same attack path for each critical asset over rounds; here, after 40 rounds as shown in Figure 7.9a). Moreover, we compare the learning effect for all attack types, defined in Section 7.4, in Figure 7.9c which shows that adaptive attacker is the most challenging attack type.

2) Reinforcement learning of behavioral level: Now, we show the performance of our reinforcement learning algorithm to guide behavioral decision-makers to rational behavior. Here, we consider the attacker who chooses the most vulnerable path to each target asset as we explained earlier. For each system of the five systems, we run our learning algorithm over 500 rounds with considering medium budget. For each round, the attacker chooses the most vulnerable path for compromising each critical asset. First, Figure 7.10a shows the convergence of our algorithm over the rounds to rational behavior (i.e., $\alpha = 1$) for all of the five systems where the probability of having rational behavior after learning over 100 rounds is more than 0.9 and approaches 1 by the end of 500 rounds (for four systems from the five systems). Note that here we show the convergence when the initial behavior was $\alpha = 0.2$ (i.e., $\alpha^0 = 0.2$). Such convergence would happen for any behavioral defender (with any $\alpha < 1$) given enough learning. This also shows that behavioral defender with our proposed Reinforcement learning algorithm can eventually reach optimal investment decisions (that leads to comparable security level as rational defender).

Figure 7.10a shows the rate of convergence of our Reinforcement-learning algorithm for the five case studies. It worth noting that learning is slower for VOIP compared to the other four systems. The reason is the higher criss-cross edges across the VOIP system (see Figure 8.8 in Section 8.6.1). This also sheds the light that each system has its own characteristics and may need further parameter tuning for enhancing convergence.

Initial values of propensities: Recall from Algorithm 2 that A and B represent the initial propensities for investing with the initial behavioral level and the propensities of other possible behavioral levels, respectively. To test convergence under different setups, we

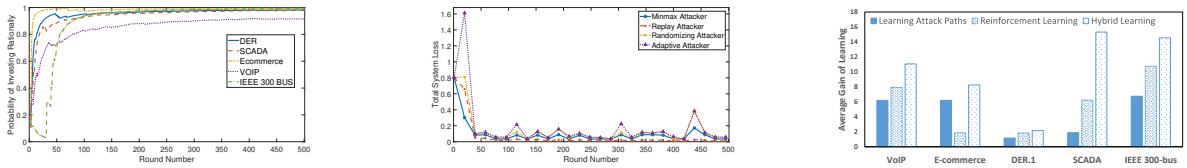


(a) Attacker chooses same attack paths

(b) Attacker chooses attack paths randomly

(c) Different attack types comparison

Figure 7.9. The effect of learning attack paths over the rounds. The learning is useful for both behavioral and rational defenders. Moreover, behavioral defender with learning attack paths can eventually reach same security level as rational defender (specifically if the attacker chooses same attack path for each critical asset over rounds). The adaptive attacker is the most challenging attack type.



(a) Convergence of Reinforcement learning to rational behavior for the five studied interdependent systems.

(b) Defense Enhancement under Hybrid Learning for different attack types. The spikes (that represents investing suboptimally) decreases in later rounds.

(c) Average Gain in Total System Loss for the different Learning techniques. The Hybrid Learning is superior for all five systems.

Figure 7.10. (a) shows the convergence of Reinforcement learning for all systems. (b) shows the effect of Hybrid learning for each attack type. In (c), we show the average gain of learning for all systems.

iterate A over the values $\{0.1, 0.2, 0.6, 1, 1.6, 2\}$ while keeping $B = 0.1$ to simulate different propensities for investing with initial behavior level α_0. In all of the experiments, the algorithm converges to rational behaviour with an average of 400 iterations (i.e., $P^t(1) > 0.95$ at $t \geq 400$).

3) Hybrid-learning Results: Here, we show the performance of our proposed Hybrid-learning Algorithm in Section 7.4. Figure 7.10b shows the enhancement of defense (represented by total system loss) over rounds under the Hybrid-learning for all proposed attack types. Note that we let the initial attack to be the same for all of the four attack types. We note that our proposed Hybrid-learning algorithm is effective in reducing total system

loss for all attack types with emphasizing that it is more effective with the replay attacker (i.e., the attacker that chooses same attack path for each critical asset every round) and the minmax attacker (i.e., the attacker that chooses the attack path with the highest probability for each critical asset every round). The enhancement is also noticeable for the two other attack types (i.e., randomizing and adaptive) but with less magnitude since capturing the attack patterns by the defender is more challenging in these two attack types. Note also that the spikes in the figure corresponds to the rounds in which the defender invest sub-optimally. These spikes decrease with rounds since the probability of investing behaviorally decreases as defender learns and enhance her budget distribution over rounds.

Benefit of Hybrid Learning: We show the benefit of the learning techniques by calculating the Average Gain of Learning (which is the ratio of total system loss after learning to the total system loss with no learning averaged over the four attack types we study in this chapter). Figure 7.10c shows the Average Gain of learning for the three earning techniques: Learning attack paths only (Algorithm 1), Reinforcement Learning only (Algorithm 2), and Hybrid Learning. We observe the superiority of Hybrid Learning compared to using only one of the two learning techniques for all of the five systems. The intuition is that this Hybrid learning combines both learning behavioral level with learning attack paths.

7.5.4 Baseline Systems

We compare our approaches with two baseline systems: the seminal work of [16] for security investment with attack graphs on attack graph generation and investment decision analysis[3] and [38] for placing security resources using defense in depth technique which traverses all edges that can be used to compromise each critical asset and distribute resources equally on them. In [16], the defense mechanism is to select the minimal set C of edges that, if removed from the attacker's arsenal, will prevent her from reaching the target asset (there can be multiple sets in case of non-uniqueness). This is equivalent to our min edge-cut. We compare [16] and [38] with our approach under both single and multi-round setups. We compare the two methods in Table 7.3 by calculating the probability of successful attack

[3]↑More recent approaches (e.g., [92]) follow the same strategy proposed in [16].

(PSA) and show the superiority of our technique in multi-round for all different attack types. Note that the defense investments given by our system for non-behavioral defenders is identical to that determined by [16] in single-round setup.

7.5.5 Evaluation of Multiple-defender Setups

Here, we evaluate our proposed algorithm in multiple-defender setups. There are six parameters that could affect the total loss of the defender. The six parameters are: defenders' security budget availability (Low, Moderate, and High), the defense mechanism (Individual, and Joint), the budget distribution among defenders (Symmetric, and Asymmetric), the degree of interdependency (number of edges between defenders' subnetworks), the sensitivity of edges to investments (the hyperparameter $s_{\mathrm{i,j}}$), and the edges' baseline probabilities of successful attacks (the hyperparameter $p^0_{\mathrm{i,j}}$). When studying the impact of a specific parameter, we fix the remaining parameters to their default values. Next, we study the impact of each system parameter with the behavioral decision-making and identify the effects of these system parameters on the degree of suboptimality of security outcomes due to behavioral decision-making in the two-defenders SCADA system.

1) Effect of defense mechanism: We observe the merits of cooperation (i.e., joint defense) in decreasing the total loss to the defenders as shown in Figure 7.11. The effect is more pronounced for a higher degree of behavioral bias of the defenders. For example, at moderate budget ($BT = 20$), the relative decrease in total system loss due to joint defense at $\alpha_1 = \alpha_2 = 0.4$ is 25% while $\alpha_1 = \alpha_2 = 0.8$, the decrease is lower (10%). Thus, as the defenders exhibit higher degree of cognitive bias, it is more advantageous to adopt joint defense mechanisms.

2) Interdependency among different defenders. Here, we observe effect of interdependency between defenders on the security of the SCADA system. In the SCADA system, the degree of interdependency increases if assets from one subnetwork can access assets in the other, without going through the Corporate or Vendor nodes. For example, if the attacker gets access to Control unit 1, this enables her to compromise RTU2 as well, in addition to RTU1. Figure 7.12 illustrates this effect—as the number of interdependent edges

Table 7.3. Comparison of our approach and baseline systems for different attacks scenarios. We consider here rational defender for our approach. The column "System Setup" shows the specific scenario; the second, third, and forth columns show the respective probability of successful attack (PSA) under [16], [38], and our system for each scenario.

System Setup	[16]	[38]	Our Approach
DER.1			
	PSA		
Single-round	**0.075**	0.208	**0.075**
Multi-round, Random Att.	0.095	0.205	**0.080**
Multi-round, Replay Att.	0.075	0.208	**0.037**
Multi-round, Adaptive Att.	0.091	0.209	**0.080**
SCADA			
Single-round	**0.035**	0.110	**0.035**
Multi-round, Random Att.	0.034	0.582	**0.029**
Multi-round, Replay Att.	0.033	0.110	**0.010**
Multi-round, Adaptive Att.	**0.035**	0.582	**0.035**
VOIP			
Single-round	**0.337**	0.556	**0.337**
Multi-round, Random Att.	0.348	0.559	**0.313**
Multi-round, Replay Att.	0.337	0.556	**0.084**
Multi-round, Adaptive Att.	0.354	0.559	**0.313**
E-commerce			
Single-round	**0.124**	0.276	**0.124**
Multi-round, Random Att.	0.139	0.572	**0.097**
Multi-round, Replay Att.	0.124	0.276	**0.007**
Multi-round, Adaptive Att.	0.139	0.569	**0.097**
IEEE 300-BUS			
Single-round	**0.431**	0.653	**0.431**
Multi-round, Random Att.	0.439	0.680	**0.168**
Multi-round, Replay Att.	0.431	0.653	**0.086**
Multi-round, Adaptive Att.	0.448	0.680	**0.186**

between the two defenders increases, the total system loss increases in both non-behavioral and behavioral security games. The highest level of interdependency is when there are two edges between DMZ1 and DMZ2, between Control1 and Control2, and the controller to the 3 RTUs of the other defender. An example of this phenomenon is that if both defenders are non-behavioral and the level of interdependency is the highest, the total system loss is higher by 462% over the case of the lowest level of interdependency (2 interdependent links). We also see that as the interdependency between the different defenders increases, the suboptimal security decisions have greater adverse impact on the total system loss.

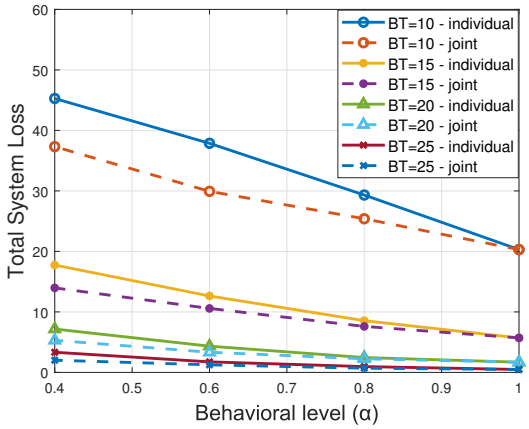


Figure 7.11. Comparison between individual and joint defense mechanisms. Joint defense is superior under asymmetric budget distribution.

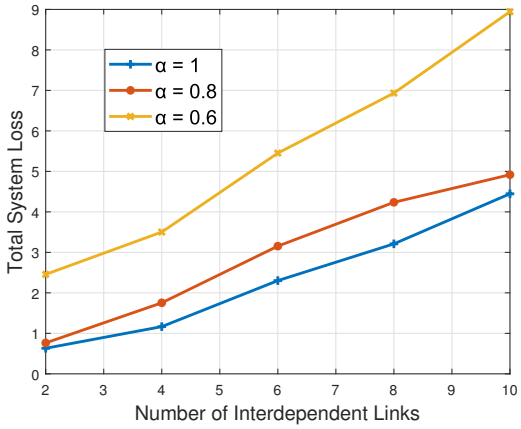
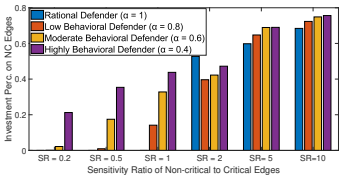
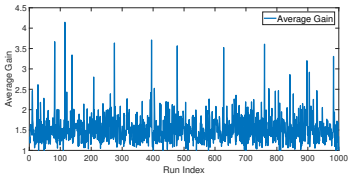


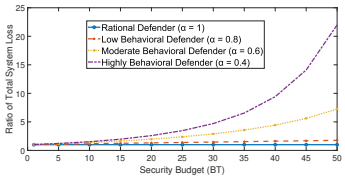
Figure 7.12. The effect of increasing the degree of interdependency on the total system loss. Such effect is more pronounced when the defender is more behavioral.



(a) Percentage of investments on non-critical edges for different edge sensitivities ratios (SR).



(b) Average gain for different random attack success probabilities over all of the edges.



(c) Effect of behavioral investments for different security budgets.

Figure 7.13. (a) The effect of edges' sensitivities on investments for different behavioral levels. (b) The average gain of rational decision-making for randomly chosen baseline probabilities of successful attacks. (c) The effect of sub-optimal investments for different choices of security budget.

3) Sensitivity of edges to investments: We next consider the effects of different sensitivities of edges to security investments. Recall that higher sensitivity edges are those for which the probability of successful attack decreases faster with each unit of security investment. We show the result in Figure 7.13a by using as the independent variable the ratio of sensitivity of non-critical to critical edges. First, assume critical edges correspond to mature systems that are already highly secure and difficult to secure further. For our model,

this translates to high (resp. low) $s_{i,j}$ for non-critical (resp. critical) edges. We observe that as the sensitivity ratio increases, all defenders put more investments on the non-critical edges, but the increase is slower in behavioral defenders. However, lower sensitivity ratio will result in investing almost all budget on these critical edges, even for behavioral defenders.

4) Baseline probabilities of successful attacks: We show that the gain of rational vs. behavioral investments exists for any combination of baseline probabilities by performing 1000 runs and in each run, for each edge, we draw the baseline probability of successful attack on that edge from a uniform distribution $p^0_{i,j} \sim \mathcal{U}(0, 1]$. We consider a symmetric budget distribution and medium security budgets. Figure 7.13b shows that the gain for rational over behavioral decision-making (with mean 1.53X) exists for any randomly chosen baseline probability of successful attacks.

5) Amount of security budget: We next show that the total system loss of rational defenders is less than that of behavioral defenders for any choice of security budget (as shown in Figure 7.13c).

6) Security budget distribution among defenders: Finally, we analyze the effect of asymmetric budget distribution between the defenders facing the attacker. Figure 7.14 illustrates the total loss as a function of the fraction of defender 1's budget. For the individual-defense loss, we observe that the suboptimality of behavioral decision-making is more pronounced with higher budget asymmetries. For example, if defender 1 has 20% of the total budget, the relative increase in total loss from $\alpha = 1$ to $\alpha = 0.4$ is 25%. In contrast, the same change of α when the budget is symmetric results in only a 6% relative increase in the total loss. This observation can be explained by two facts. First, with suboptimal behavioral allocation, the poorer defender wastes even her constrained budget on non-critical edges. Second, the richer player also allocates her resources suboptimally. This leads to this magnified relative increase in losses under budget asymmetry.

We now present system parameters evaluation of DER.1, which has similar insights as SCADA. In particular, Figures 7.15-7.18 show the effect of four different parameters.

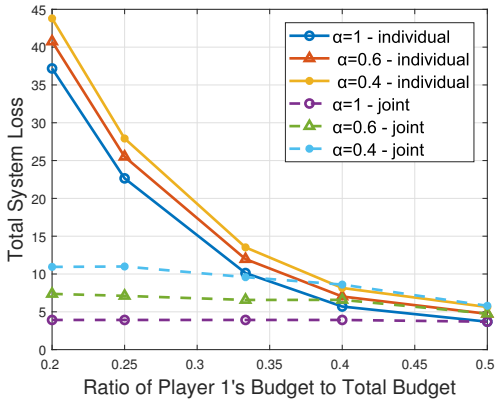


Figure 7.14. The total system loss as a function of the fraction of defender 1's budget. We observe that joint defense outperforms individual defense at higher budget asymmetry.

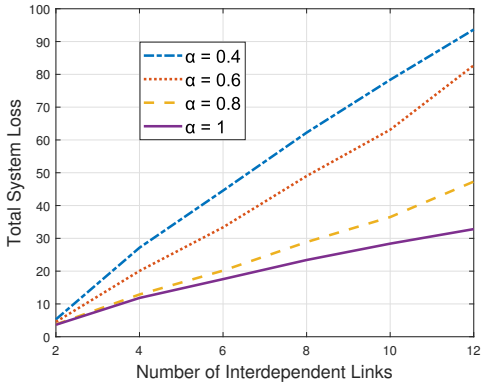


Figure 7.15. (a) Interdependency Effect

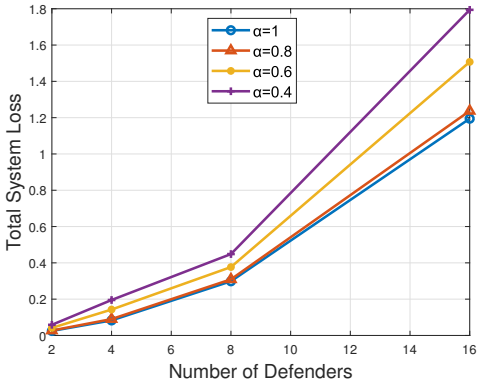


Figure 7.16. (b) Number of Defenders

7.6 Limitations and Discussion

Guiding security decision-makers: We believe that our work opens up a new dimension of *intervention* in securing interdependent systems. Our framework allows a quantification of the improvements in security that can be obtained by training security professionals to reduce their behavioral biases. In this context, we can quantitatively show the decision-maker the improvement in system security when moving from her current (sub-optimal) investments to that given by a (rational) algorithm (e.g., our model with $\alpha = 1$). Furthermore, our framework can guide security audits by system operators of large-scale interdependent system, by allowing the operator to investigate subsystems within

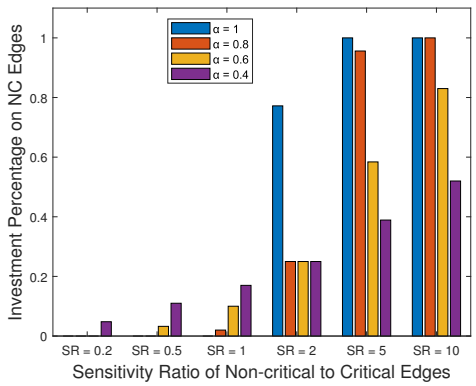


Figure 7.17. (c) Sensitivity of Edges

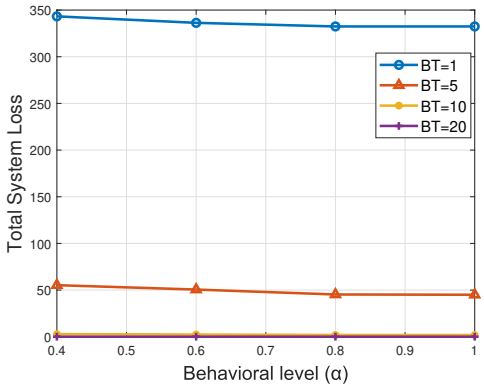


Figure 7.18. (d) Security Budget

Figure 7.19. Results of Multi-defenders for DER.1 system.

the system where sub-optimal security investments might have been made by subordinates operating those subsystems. While such an operator may not be able to check every single aspect of every subsystem, she may be able to "zoom in" to portions of the overall system where an audit may be warranted due to evidence of sub-optimality from our framework.

Behavioral level of the attacker: We assume that defenders perceive the attacker as non-behavioral; in reality the attacker can be behavioral as well. Our assumption of a non-behavioral attacker gives the worst case loss for the system; as a behavioral attacker may not choose the path of true highest vulnerability due to probability misperceptions. This can open the interesting question "how a rational defender, who uses the security investments recommended by our approach, can deceive a behavioral attacker to choose harder attack paths?" This can help the defender to misguide the attacker and make the target system more secure.

Multi-hop dependence: In several cybersecurity scenarios, the ease of an attacker in achieving an attack goal depends not just on the immediate prior attack step but on steps farther back. In such scenarios, the simpler formulation of using probabilities on each edge and assuming independence of the events of traversing the different edges can lead to inaccurate estimates. However, we follow several prior works (e.g., [13], [88]) that leveraged the property that in most cases, a node has the highest dependence on the previous node, in order to build computationally tractable analysis tools. Moreover, to handle this issue

in our model, the notion of *k-hop dependence* [93] can be used, whereby the probability of reaching a particular node depends nodes up to k hops away.

7.7 Related Work

Game-theoretic modeling of security: Game theory has been used to describe the interactions between attackers and defenders and their effects on system security. A commonly used model in this context is that of two-player games, where a single attacker attempts to compromise a system controlled by a single defender [89], [94]. Game theoretic models have been further used in [11] to study the interaction between one defender and (multiple) attackers attempting Distributed Denial of Service attacks. Game theoretic models have also been proposed for studying critical infrastructure security (See the survey [3]). The major difference of our work with all aforementioned literature is that existing work has focused on classical game-theoretic models of rational decision-making, while we analyze behavioral models of decision-making.

Human behavior in security and privacy: Notable departure from classical economic models within the security and privacy literature is [81], which identifies the effects of behavioral decision-making on individual's personal privacy choices. The importance of considering similar models in the study of system security has been recognized in the literature [95]. Prior works [49], [82] considered models from behavioral economics in the context of security applications. However, these works are based only on psychological studies [49] and human subject experiments [82] for end-user. Our work differs from these in that we explore a rigorous mathematical model of defenders' (decision-makers) behavior, model the interaction between multiple defenders (in contrast to the study of only one defender for all of these studies), and consider interdependent assets (in contrast to these studies which reason about binary decisions on isolated assets). To the best of our knowledge, the exceptions that provide a theoretical treatment of behavioral decision-making in certain specific classes of interdependent security games are [31], [33], [36], [77]. These works, however, are theoretical in scope and do not consider the more realistic attack scenarios and types that we consider, do

not validate bias of decision-makers via subject experiments, and don't consider multi-round setups or learning algorithms that we consider here.

Multi-round in Security: Reinforcement-based learning models have been used in literature where players' strategies receive reinforcement related to the payoffs they earn and adjust their moves over time seeking higher payoffs. Specifically, [91] proposed reinforcement learning for an environment with only two possible actions. Such Reinforcement-based learning models have been used in different security applications such as the robustness of smart grid [96]. Our work differs from these works that we guide the behavioral decision-maker towards rational decision-making where the reinforcements are received from the true loss that the defender accrues when investing with behavioral bias. Likelihood method of discovering attack paths using Bayesian attack graphs has been proposed in [88]. However, to the best of our knowledge, no previous work has the idea of minimizing the adapted defender's cost and generate optimal allocations each round while weighting attack paths based on previous rounds that we consider in our Hybrid-learning algorithm.

7.8 Summary of Findings

In this chapter, we presented several algorithms to enhance human behavioral decision-making on the security of interdependent systems with multiple defenders where we model stepping-stone attacks by the notion of *attack graphs*. While behavioral decision-makers tend to allocate their budget across the network, our approaches help decision-makers concentrate their budget on critical edges to make the system more secure. We performed a controlled subject experiment to validate our behavioral model. In multi-round setups, we proposed different learning algorithms to guide behavioral decision-makers towards optimal decisions. We evaluated our techniques on five real case studies of interdependent systems where we studied the effects of several system parameters. The insights gained from our analysis would be useful for configuring real-world systems with optimal parameter choices and guiding behavioral decision-makers toward rational decision-making that can ultimately lead to improvements in interdependent systems' security.

8. Using Mechanism Design for Enhancing Security Resource Allocation in Interdependent Systems

In the previous chapters, we modeled the *behavioral* biases of human decision-making in securing interdependent systems and showed that such behavioral decision-making leads to a suboptimal pattern of resource allocation compared to non-behavioral (rational) decision-making and we proposed learning techniques to guide each stakeholder (defender) to make better decisions in interdependent security games. In this chapter, we incorporate into our framework two types of tax-based mechanisms for such interdependent security games where the central regulator incentivizes defenders to invest well in securing their assets so as to achieve the socially optimal outcome. We first show that due to the nature of our interdependent security game, no reliable tax-based mechanism can incentivize the socially optimal investment profile while maintaining a weakly balanced budget. We then show the effect of behavioral probability weighting bias on the amount of taxes paid by defenders, and prove that higher biases make defenders pay more taxes under the two mechanisms. We then explore voluntary participation in tax-based mechanisms. To evaluate our mechanisms, we use four representative real-world interdependent systems where we compare the game-theoretic optimal investments to the socially optimal investments under the two mechanisms. We show that the mechanisms yield higher decrease in the social cost for behavioral decision-makers compared to rational decision-makers.

8.1 Introduction

Recent work has begun to model and predict the effect of behavioral decision-making on security investments [36], [71], [77], [97], [98]. However, none of this research sheds light on the mitigation of such cognitive biases and these works have only studied specific interdependent games. In contrast, we consider general defense allocation techniques that can be applied to any system whose failure scenarios are modeled by an attack graph. We consider tax-based mechanisms to guide behavioral decision-makers towards enhancing their security investments and incentivize them to achieve socially optimal allocations that reduce

Table 8.1. Comparison between the prior related work and our framework in terms of the available features. Our framework provides an analytical framework that incorporates two mechanism designs for incentivizing defenders in multi-defender interdependent systems (modeled by attack graphs) and mitigates behavioral cognitive biases by human defenders.

System	Multiple Defenders	Interdependent Subnetworks	Analytical Framework	Behavioral (Cognitive) Biases		Mechanism Design
				Effects	Mitigation	
S&P02 [16], CCS12 [11], CCS21 [99]	✗	✓	✓	✗	✗	✗
S&P09 [81], EC18 [82], ACSAC12 [49]	✗	✗	✗	✓	✗	✗
ICC17 [36], CDC19 [33], CDC20 [70]	✗	✗	✓	✓	✗	✗
INFOCOM16 [41], SIGMETRICS18 [100]	✓	✗	✓	✗	✗	✓
AsiaCCS21 [71], TCNS18 [31], SPW21 [101]	✓	✓	✓	✓	✗	✗
Our Work	✓	✓	✓	✓	✓	✓

the overall security risk. Fundamentally, our framework, identifies the effects of behavioral bias on the design of mechanisms for improving security decisions in interdependent systems.

Problem setup and mechanism design:

In this chapter, we model a security setup of interdependent systems with multiple defenders. Each defender is responsible for defending a subnetwork of the whole network. In such interdependent systems, stepping-stone attacks are often used by external attackers to exploit vulnerabilities within the system in order to compromise critical targets. These stepping-stone attacks are captured via *attack graphs* [24].

We first show the difference between the Pure-Strategy Nash Equilibrium (PNE) investments (by both rational and behavioral defenders) and the socially optimal investments via multiple motivating examples. We then design two tax-based mechanisms that enhance security investment decision-making for our interdependent security games. Such mechanisms use monetary payments/rewards to incentivize socially optimal (SO) security behavior, i.e., those minimizing the sum of the costs of all defenders due to a security attack. The two tax-based mechanisms are the 'Externality' mechanism [39] and the Vickrey-Clarke-Groves ('VCG') mechanism [40]. These mechanisms enhance the implemented security policy by incentivizing defenders to allocate their limited security resources to minimize the system's social cost.

We then show a fundamental result that there exists no reliable tax-based mechanism which can incentivize the socially optimal investment profile while maintaining a weakly balanced budget (i.e., the central regulator does not pay out-of-pocket money) for all

instances of interdependent security games. We show the difference between our result and prior results in the security economics literature [40], [41] in Section 8.7. Our result shows that designing mechanisms in interdependent security games is more challenging compared to monolithic systems. We also show the effect of behavioral biases on the two mechanisms' outcomes in our interdependent security games framework. We then evaluate our findings using four synthesized attack graphs that represent realistic interdependent systems and attack paths through them. These systems are DER.1 [17] (modeled by NESCOR), SCADA industrial control system modeled using NIST guidelines for ICS [12], E-commerce [13], and VOIP [13]. We do a benchmark comparison with four prior solutions for optimal security controls with attack graphs [16], [38], [71], [99]. In conducting our analysis, we address several domain-specific challenges in the context of security for interdependent systems. These include modifying mechanism formulations for our interdependent security games (Section 8.5), and incorporating behavioral biases in our formulations (Section 8.2).

Key insights:

Abstracting from the details, we provide three hitherto unknown insights into the security of interdependent systems.

i. A social planner (e.g., government agency) can achieve much lower security loss than each defender acting on her own. The difference increases when security defenders have more cognitive biases (Figure 8.9). The global planning is beneficial even if the planner is behavioral (Example 7.1). However, if the degree of interdependency is slight, then there is no need to go to the complexity of setting up central regulation — each defender acting independently (selfishly) achieves close to the optimal security (Figure 8.10(a)).

ii. Our work supports recent proposals for companies to buy cyber insurance as part of their risk management strategy. In such process, the company would pay a tax (determined by the regulator depending on the system architecture (Figure 8.12)) and then transfer the financial risks related to network and computer incidents to that regulator.

iii. Behavioral decision-making leads to suboptimal resource allocation and thus tax-based mechanisms can be more helpful in a system with behavioral defenders compared to non-behavioral (rational) decision-makers (Figure 8.11). In such mechanisms, we prove that behavioral biases make defenders pay *more* taxes compared to rational defenders.

In summary, this chapter makes the following contributions:

i. We propose a *security investment guiding* technique for defenders of interdependent systems whose assets have mutual interdependencies. We show the effect of an important behavioral bias of human decision-making and selfishness of PNE decision-making on system security.

ii. We consider two mechanism designs for interdependent security games modeled by attack graphs to guide decision-makers toward the socially optimal solution. In contrast to excludable public good games, we show that a weak budget balance condition is not guaranteed for all instances of interdependent security games.

iii. We explore the voluntary participation in tax-based mechanisms and show that behavioral defenders participate under higher tax payments, compared to rational defenders.

iv. We illustrate the benefits of our mechanisms through four real-world interdependent systems and analyze the different system parameters and the effect of behavioral decision-making on mechanisms' outcomes and the overall security of the systems.

The remainder of this chapter is organized as follows. We introduce the preliminaries in Section 8.2, and the tax-based mechanism design notations in Section 8.3. We provide motivating examples in Section 8.4. We then present the mechanisms and main results in Section 8.5. In Section 8.6, we evaluate our framework on real-world interdependent systems. The related literature is given in Section 8.7. The discussion and limitations are given in Section 8.8. We conclude the chapter in Section 8.9.

8.2 Background and Problem Setup

8.2.1 Perceived Cost of a Behavioral Defender

Recall that in our *Behavioral Security Game*, each defender misperceives attack success probability on each edge according to the probability weighting function in (2.3). She then chooses her investments $x_k := \{x^k_{\mathrm{i,j}}\}_{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_k}$ to minimize her *perceived* loss

$$C_k(x_k, \mathbf{x}_{-k}) = \sum_{v_m\in V_k} L_m\Big(\max_{P\in P_m} \prod_{(v_\mathrm{i},v_\mathrm{j})\in P} w\left(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})\right)\Big)\,, \tag{8.1}$$

subject to her total security investment budget B_k, i.e., $\sum_{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_k} x^k_{\mathrm{i,j}} \leq B_k$[1], and non-negativity of the investments, i.e., $x^k_{\mathrm{i,j}} \geq 0$.

8.2.2 Socially Optimal Investments

It is also common in the literature to measure the sub-optimality of Nash equilibria (attained by interdependent security games between multiple selfish defenders) by comparing them to socially optimal (SO) investments. Formally, the socially optimal investment levels $\mathbf{x}^*$ are those that maximize the social welfare (i.e., these investments minimize the sum of all defenders' costs), which is given by

$$\mathbf{x}^* = \underset{\substack{\mathbf{x}\succeq\mathbf{0};\\ \mathbf{1}^T\mathbf{x}\leq\sum_{k=1}^{|D|}B_k}}{\operatorname{argmin}} \sum_{k=1}^{|D|} C_k(\mathbf{x}), \tag{8.2}$$

where $|D|$ is the number of defenders.

A comparison of the Nash equilibria and the socially optimal solution often reveals sub-optimal investment in security by defenders at PNE where each defender only cares about her own critical assets. In the literature, there are several works that have proposed mechanisms for decreasing this inefficiency gap, by incentivizing improved security investments [41], [102]. However, these works studied specific games where each defender has a single asset in which she allocates her resources [41] or considered that all defenders have a common asset [102]. Moreover, all of these works considered only classical models of rational decision-making introduced earlier. On the contrary, we consider an attack graph based system where each defender has the ownership of a subset of nodes. Further, the interdependency between defenders is captured via overlapping paths for reaching different defenders' assets, and we model the behavioral probability weighting bias as well. These two distinctions make our setup more challenging compared to prior work and more representative of the reality of interdependent system security with humans acting as security decision-makers.

[1]↑Our findings will also follow if each defender invests any amount subject to a maximum budget. The stakeholder (defender) can use any amount from such a maximum budget limit for enhancing the security of her subnetwork.

8.3 Mechanism Design Setup

The focus of the present chapter is designing and evaluating regulatory mechanisms, specifically monetary taxation, to incentivize socially optimal security behavior for defenders in interdependent security games. Our goal is to find a mechanism, run by a central regulator (e.g., a government agency), such that the induced interdependent security game has as its equilibrium the solution to the centralized problem (8.2) (also referred to as "implementing" the socially optimal solution). Such mechanisms incentivize optimal behavior by assessing a tax t_k to each participating defender D_k; this tax may be positive, negative, or zero, indicating payments, rewards, or no payment, respectively. Similar to prior work [41], [72], we assume that defenders' costs are quasi-linear; i.e., linear in the tax term t_k. Therefore, the total (security) cost for a defender D_k when she is assigned a tax t_k is

$$C_k(\mathbf{x}, t_k) := C_k(\mathbf{x}) + t_k, \tag{8.3}$$

where the tax amount t_k can in general be a function of the total security investment $\mathbf{x}$ or the overall state of system's security (as will be explained later in Section 8.5) where each mechanism corresponds to one form of t_k.

Remark 11. Following the previous works [41], [72], [103], we assume that the money used for the taxes paid by each defender comes from a separate pool from the pool from which the security enhancement budget of each defender is drawn. However, we believe that considering them to be from the same pool is an interesting direction for the future extensions.

Proposition 8.3.1. *There always exists a Pure-Strategy Nash Equilibrium in an unregulated (i.e.* $t_{\mathrm{i}} = 0$, $\forall \mathrm{i}$*) Behavioral Security Game as modeled in this section.*

The proof of the above result follows by noting that the cost function of each defender is convex in the security investment level $\mathbf{x}$ (equivalently the payoff is concave function in $\mathbf{x}$), thus this game is an instance of concave games which always have a PNE [54].

Mechanism Properties: In addition to implementing the socially optimal solution, incentive mechanisms are often designed so as to satisfy one main property. When using

taxation, the mechanism designer prefers to maintain *weak budget balance* (WBB) [39], [72]; i.e., $\sum_{i=1}^{N} t_i \geq 0$. In other words, the regulator does not pay out to the defenders. In contrast, $\sum_{i=1}^{N} t_i < 0$ implies a budget deficit, i.e., the mechanism would require spending external resources by the designer. At first, we consider two mechanism designs where participation by defenders is mandatory (Sections 8.5.1 and 8.5.2) and then we consider the mechanism where participation is voluntary (Section 8.5.3). The mandatory participation maps to the realistic case that a government agency can make participation in cyber-insurance a prerequisite for companies to receive security funding or business opportunities [104]; see for example the recent California proposal for mandatory cyber insurance [105].

8.4 Motivational Examples

Having provided the game notations and the general tax-based mechanism, we now provide a couple of examples to show the difference between the social optimal solution (given by (8.2)) and the PNE solution (where each defender best responds to the aggregate optimal investments of other defenders) to reach the PNE of Behavioral Security Games.

Example 7.1. Consider the attack graph of Figure 8.1. There are two defenders, D_1 and D_2, where defender D_1 aims to protect node v_4, and defender D_2 wishes to protect node v_5. Suppose that D_1 has a budget $B_1 = 16$ and D_2 has $B_2 = 12$, and 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 $p^0_{i,j} = 1$). Moreover, both defenders have behavioral bias with $\alpha_1 = \alpha_2 = 0.5$. Figures 8.1a and 8.1b illustrate two distinct PNE for this game.

We obtained these multiple Nash equilibria by varying the starting investment decision of defender D_1 and then following best response dynamics until the investments converged to an equilibrium. It is interesting to note that these two Nash equilibria lead to different costs for the defenders.

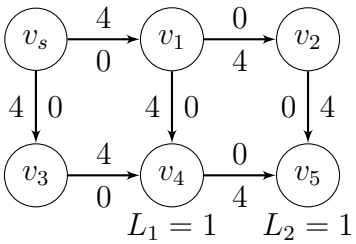
Difference between PNE and social optimal: First, for the Nash equilibrium of Figure 8.1a, defender D_1's perceived expected cost, given by (8.1), is equal to $\exp(-4)$, while her true expected cost, given by (2.2), is equal to $\exp(-8)$. Defender D_2 has a perceived expected cost of $\exp(-6)$, and a true expected cost of $\exp(-12)$. In contrast, for the Nash

equilibrium in Figure 8.1b, defender D_1 has a perceived expected cost of $\exp(-4.5)$ and a true expected cost of $\exp(-10)$. Defender D_2 has a perceived expected cost of $\exp(-5.78)$ and a true expected cost of $\exp(-11.28)$. As a result, the equilibrium in Figure 8.1a is preferred by defender D_2, while the equilibrium in Figure 8.1b has a lower expected cost (both perceived and real) for defender D_1.

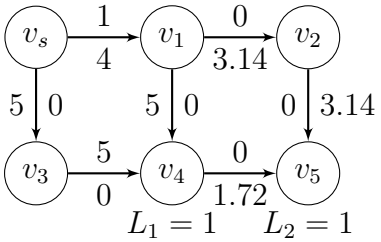
Second, we calculate the optimal investments by a social planner for such network. We assume that this social planner would have the same total budget (i.e., the sum of the two budgets of defenders D_1 and D_2) and calculate the optimal investment of that social planner (given by (8.2)). Figure 8.1c shows that the rational social planner would distribute her budget equally (only) on the edges (v_s, v_1) and (v_s, v_3) while Figure 8.1d shows that the behavioral social planner (with $\alpha = 0.5$) would distribute investments on all edges. We emphasize that the true expected cost of defender D_1 is $\exp(-14.0)$ and the true expected cost of defender D_2 is $\exp(-14.0)$ under rational central planning. On the other hand, the true expected cost of D_1 is $\exp(-11.88)$ and the true expected cost of defender D_2 is $\exp(-12.31)$ under behavioral central planning. In other words, rational central planning is better for both defenders and for the system as a whole.

Key takeaways: For both scenarios (rational social planner and behavioral social planner), the true costs are better (lower) for both defenders than in both of the attained PNEs. Moreover, the system's social cost is lower under such socially optimal solutions. This example sheds light on the inefficiency of the PNEs compared to the social optimal solution. In this context, the notion of *Price of Anarchy (PoA)* is often used to quantify the inefficiency of Nash equilibrium compared to the socially optimal outcome [55]. The Price of Anarchy is defined as the ratio of the highest total system cost at a PNE to the total system cost at the social optimum. In Example 1, the PoA under rational and behavioral social planning is 205.41 and 30.11, respectively, indicating a 205X and 30X reduction in expected security loss with central planning. The higher the PoA is, the greater is the motivation for centralized design of a mechanism that incentivizes the defenders to enhance their investments and achieve social optimal.

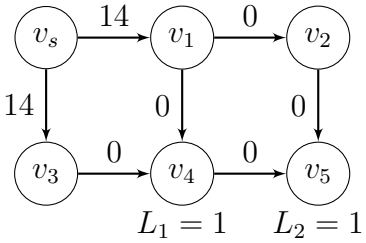
Example 2. Consider the attack graph in Figure 8.2, where the probability of successful attack on each edge $(v_{\mathrm{i}}, v_{\mathrm{j}})$ is given by (2.6) with $p^0_{\mathrm{i,j}} = 1$. This graph contains $|D| = K$



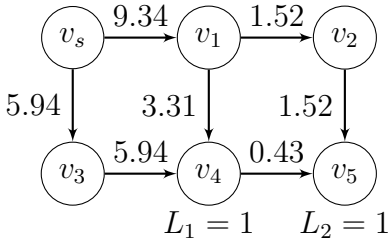
(a) First PNE



(b) Second PNE



(c) Rational central regulator



(d) Behavioral central regulator

Figure 8.1. An instance of a Behavioral Security Game with multiple PNE and its corresponding social optimal solution. The costs for each defender are lower with the central regulator than with PNE. Defenders D_1 and D_2 are behavioral decision-makers with $\alpha_1 = \alpha_2 = 0.5$. In (a) and (b), the numbers above/left and below/right of the edges represent investments by D_1 and D_2, respectively. In (c) and (d) these numbers represent investments by rational and behavioral (with $\alpha = 0.5$) central regulator, respectively.

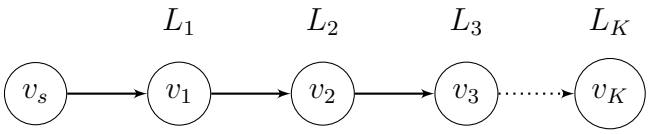


Figure 8.2. An attack graph where the social optimal investment is better than the PNE's investments for all behavioral defenders.

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 defenders (i.e., each defender has a security budget of $\frac{B}{K}$). Let all nodes $v_1, v_2, \cdots, v_K$ have same loss which is L. Then, the socially optimal solution would put all the budget B on the first edge (v_s, v_1), so that all nodes have probability of successful attack given by $\exp(-B)$.

We now characterize the cost under the PNE for behavioral defenders. This PNE is given by the investment profile where each defender D_k puts their entire budget $\frac{B}{K}$ on the edge

coming into their node v_k. 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, given D_1's investment on (v_s, v_1), defender D_2 should 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 (8.1). Thus, D_2's optimization problem, given D_1's investment, is

$$\underset{x_{s,1}^2 + x_{1,2}^2 = \frac{B}{K}}{\text{minimize}} \quad \mathrm{e}^{-\left(\frac{B}{K} + x_{s,1}^2\right)^{\alpha_2} - \left(x_{1,2}^2\right)^{\alpha_2}}. \tag{8.4}$$

The unique optimal solution of (8.4) (for all $\alpha_2 \in (0,1)$) would be to put all $\frac{B}{K}$ into the edge (v_1, v_2), i.e., $x_{1,2}^2 = \frac{B}{K}$ and zero on the edge (v_s, v_1), i.e., $x_{s,1}^2 = 0$.

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. Therefore, the true cost of defender D_1 under this PNE is given by $K \exp\left(-\frac{B}{K}\right)$, which is much larger than this of the social optimal solution. Thus, the PoA in this game instance grows exponentially in the sum of budgets B.

In total, the two examples show the importance of attaining social optimal solution for both per-defender total real loss and the social cost (sum of defenders' real total losses).

8.5 Mechanism Types and Properties

We now provide two incentive mechanisms in our interdependent security games, and identify features of the interdependent systems that affect the properties attainable through these mechanisms. Specifically, we explain and study the performance of the two mechanisms within our class of interdependent security games.

8.5.1 The Externality Mechanism

We now introduce the Externality mechanism inspired by the work of Hurwicz [106]. A main design goal of this mechanism is to guarantee a complete redistribution of taxes; i.e., strong budget balance. This mechanism has been adapted in [39], where it is shown to achieve

social optimality, guarantee participation, and maintain a balanced budget, in allocation of power in cellular networks. However, the recent work [41] has shown that this is not the case in security games where each defender has a single asset in which she allocates her resources. However, that work only considered classical decision-making models (where all defenders are fully rational decision-makers), and did not consider interdependency (attack graph models).

Let us denote the total tax paid by defender D_k at the equilibrium as t_k^*, which depends on the investment vector $\mathbf{x}$, i.e., $t_k^* = \mathbf{l_k^*}\mathbf{x}$. We denote $\mathbf{l_k^*} := \{l_{\mathrm{ij}}^{kn^*}\}_{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_n, D_n\in D}$ where $l_{\mathrm{ij}}^{kn^*} = -L_k \frac{\partial C_k}{\partial x_{\mathrm{i,j}}^n}(\mathbf{x}^*)$ is the positive externality of defender D_k due to defender D_n's investment on the edge $(v_\mathrm{i}, v_\mathrm{j})$.

To have the designed mechanism achieve the social optimal, the socially optimal investments $\mathbf{x}^*$ will be individually optimal as well; in other words, we have

$$\mathbf{x}^* \in \underset{\substack{\mathbf{x}\succeq\mathbf{0};\\ \mathbf{1}^T\mathbf{x}\leq\sum_{k=1}^{|D|}B_k}}{\operatorname{argmin}} \quad C_k(\mathbf{x}) + \mathbf{l_k^*}\mathbf{x}. \tag{8.5}$$

As a result, the Karush-Kuhn-Tucker (KKT) conditions on (8.5) yield that the tax term of defender D_k under the Externality mechanism in our interdependent security games is

$$t_k^*(\mathbf{x}^*) = \sum_{n=1}^{|D|} \sum_{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_n} t_{\mathrm{ij}}^{kn^*}. \tag{8.6}$$

In other words, the total tax paid by defender D_k is a summation of the taxes over all edges, where the tax on each edge depends on the sum of the externalities of all defenders on that edge. Specifically, the investment by defender D_n on the edge $(v_\mathrm{i}, v_\mathrm{j})$ is denoted by $x_{\mathrm{i,j}}^{n^*}$.

Thus, the tax term that D_k pays due to the externality of defender D_n's investment on the edge $(v_\mathrm{i}, v_\mathrm{j})$ is given by

$$t_{\mathrm{ij}}^{kn^*} = -L_k x_{\mathrm{ij}}^{n^*} \frac{\partial C_k}{\partial x_{\mathrm{i,j}}^n}(\mathbf{x}^*). \tag{8.7}$$

Interpretation of the Externality Mechanism: The interpretation of the above tax terms is that by implementing this externality mechanism, each defender D_k will be financing

part of defender $D_n \neq D_k$'s reimbursement. According to (8.6) and (8.7), this amount is proportional to the positive externality of D_n's investment on D_k's cost.

Budget deficit: It can be shown that despite attaining the socially optimal solution, these taxes may fail to satisfy the weak budget balance constraint in our behavioral interdependent security games. We characterize this finding via the following result.

Proposition 8.5.1. *There exists an interdependent security game instance where the Externality mechanism cannot implement the social optimal while guaranteeing weak budget balance.*

Proof. The proof of Proposition 8.5.1 follows by the following counter example in which we give an instance of interdependent security game that has a budget deficit.

Example 3. Consider the attack graph in Figure 8.3. This graph contains 2 rational defenders ($\alpha_1 = \alpha_2 = 1$), and each defender D_k is responsible for defending target node v_k. Let the defender D_1's node have loss equal to L_1, and the defender D_2's node have loss L_2. From (8.5), the cost of defender D_1 is given by $C_1(\mathbf{x}) = L_1 \mathrm{e}^{-x^1_{s,1}-x^2_{s,1}} + \begin{bmatrix} l^{11^*}_{s,1} & l^{12^*}_{s,1} & l^{11^*}_{1,2} & l^{12^*}_{1,2} \end{bmatrix} \begin{bmatrix} x^1_{s,1} \\ x^2_{s,1} \\ x^1_{1,2} \\ x^2_{1,2} \end{bmatrix}$. Thus, the Lagrangian of the defender D_1 is given by

$$\mathcal{L}(\mathbf{x}, \mu) = L_1 \mathrm{e}^{-x^1_{s,1}-x^2_{s,1}} + \begin{bmatrix} l^{11^*}_{s,1} & l^{12^*}_{s,1} & l^{11^*}_{1,2} & l^{12^*}_{1,2} \end{bmatrix} \begin{bmatrix} x^1_{s,1} \\ x^2_{s,1} \\ x^1_{1,2} \\ x^2_{1,2} \end{bmatrix} + \mu[x^1_{s,1} + x^1_{1,2} - B_1]. \tag{8.8}$$

Applying KKT conditions [107] to (8.8) yields

$$-L_1 \mathrm{e}^{-x^1_{s,1}-x^2_{s,1}} + l^{11^*}_{s,1} + \mu = 0 \tag{8.9}$$

$$-L_1 \mathrm{e}^{-x^1_{s,1}-x^2_{s,1}} + l^{12^*}_{s,1} = 0 \tag{8.10}$$

$$l^{11^*}_{1,2} + \mu = 0 \tag{8.11}$$

$$l^{12^*}_{1,2} = 0. \tag{8.12}$$

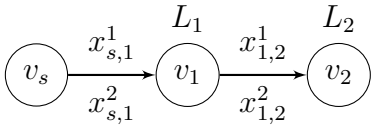


Figure 8.3. An attack graph where the Externality mechanism has individual rationality (achieves social optimal solution) but does not have weakly budget balance.

Thus, by solving (15)-(18) we have

$$\mathbf{l_1^*} = \begin{bmatrix} L_1 \mathrm{e}^{-x^1_{s,1}-x^2_{s,1}} - \mu & L_1 \mathrm{e}^{-x^1_{s,1}-x^2_{s,1}} & -\mu & 0 \end{bmatrix}$$
$$t_1^* = \mathbf{l_1^*} \begin{bmatrix} x^1_{s,1} & x^2_{s,1} & x^1_{1,2} & x^2_{1,2} \end{bmatrix}^T.$$

Similarly, calculating the Lagrangian of defender D_2 and doing a similar analysis to that of defender D_1 and letting $\beta_2 = \mathrm{e}^{-x^1_{s,1}-x^2_{s,1}-x^1_{1,2}-x^2_{1,2}}$, the tax terms of defender D_2 are

$$\mathbf{l_2^*} = L_2 \begin{bmatrix} \beta_2 & \beta_2 - \frac{\mu}{L_2} & \beta_2 & \beta_2 - \frac{\mu}{L_2} \end{bmatrix},$$
$$t_2^* = \mathbf{l_2^*} \begin{bmatrix} x^1_{s,1} & x^2_{s,1} & x^1_{1,2} & x^2_{1,2} \end{bmatrix}^T.$$

Now, we calculate summation of taxes for the two defenders. Note that under social optimal $\mathbf{x}^*$, we have $x^1_{s,1} = B_1, x^1_{1,2} = 0$, $x^2_{s,1} = B_2$, and $x^2_{1,2} = 0$. Thus, the taxes terms are

$$t_1^* = 2L_1 B_1 \mathrm{e}^{-B_1-B_2} - \mu B_1,$$

$$t_2^* = 2L_2 B_2 \mathrm{e}^{-B_1-B_2} - \mu B_2.$$

For simplicity, suppose that $L_1 = L_2 = L$ and $B_1 = B_2 = B$, we thus have $t_1^* = 2LB\mathrm{e}^{-2B} - \mu B$ and $t_2^* = 2LB\mathrm{e}^{-2B} - \mu B$. Therefore, summing the taxes of the two defenders yield $\sum_{\mathrm{i}=1}^{2} t_{\mathrm{i}}^* = 4LB\mathrm{e}^{-2B} - B(\mu + \mu)$. Note that if $4L\mathrm{e}^{-2B} < \mu + \mu$ (which can happen under large budget B and small loss L, e.g., $L = 4$ and $B = 50$ yields $4L\mathrm{e}^{-2B} = 2.97 \times 10^{-43}$), we would have $\sum_{\mathrm{i}=1}^{2} t_{\mathrm{i}}^* < 0$. □

Interpretation: Proposition 8.5.1 shows a budget deficit case for the Externality mechanism in which the central regulator has to spend out-of-pocket money to incentivize the defenders to achieve the socially optimal solution in the context of our interdependent security games (modeled by attack graphs). Thus, we show for the first time that the prior result of Externality mechanism [39], [106], [108], social optimality *and* balanced budget, is not guaranteed in interdependent systems.

Now, we turn our attention to the effect of defender's behavioral bias on amount of taxes paid by the defender.

Theorem 8.5.1. *Consider a set of defenders D and an underlying attack graph G. Suppose that the joint investment profile by all defenders except D_k, denoted by $\mathbf{x}_{-k}$, is fixed. Suppose that $p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) \in (0, \frac{1}{\mathrm{e}}]$. Then the tax paid by defender D_k under Externality mechanism, denoted by $t_k^*(\mathbf{x}^*)$ in (8.6), is a decreasing function in α_k. In other words, the behavioral defender pays more taxes compared to a rational defender.*

Proof. We prove this result by showing that the amount of taxes paid by defender D_k, given by $t_k^*(\mathbf{x}^*)$ is a decreasing function in the defender D_k's behavioral level α_k. Recall from (8.6) the tax term of D_k under Externality mechanism in interdependent security games is:

$$t_k^*(\mathbf{x}^*) = \sum_{n=1}^{|D|} \sum_{(v_{\mathrm{i}},v_{\mathrm{j}})\in\mathcal{E}_n} t_{\mathrm{ij}}^{kn^*} \overset{(8.7)}{=} -L_k \sum_{n=1}^{|D|} \sum_{(v_{\mathrm{i}},v_{\mathrm{j}})\in\mathcal{E}_n} x_{\mathrm{ij}}^{n^*} \frac{\partial C_k}{\partial x_{\mathrm{i,j}}^n}(\mathbf{x}^*). \tag{8.13}$$

Note that the marginal derivative of defender D_k's cost w.r.t. the investment of defender D_n on the edge $(v_{\mathrm{i}}, v_{\mathrm{j}})$ follows from differentiating (8.1) and is given by

$$\frac{\partial C_k}{\partial x_{\mathrm{i,j}}^n}(\mathbf{x}^*) = \sum_{v_m\in V_k} L_m \exp\left(-\sum_{(v_{\mathrm{i}},v_{\mathrm{j}})\in\overline{P}} [-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))]^{\alpha_k}\right) \times \alpha_k[-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))]^{\alpha_k-1} \times \frac{p_{\mathrm{i,j}}(x_{\mathrm{i,j}})}{p_{\mathrm{i,j}}(x_{\mathrm{i,j}})},$$

where $\overline{P} = \underset{P\in P_m}{\operatorname{argmax}} \prod_{(v_{\mathrm{i}},v_{\mathrm{j}})\in P} w\left(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})\right)$. Now, differentiating $\frac{\partial C_k}{\partial x_{\mathrm{i,j}}^n}(\mathbf{x}^*)$ w.r.t. α_k yields

$$\frac{d}{d\alpha_k}\frac{\partial C_k}{\partial x_{\mathrm{i,j}}^n}(\mathbf{x}^*) =$$

$$\sum_{v_m \in V_k} L_m \exp\left(-\sum_{(v_\mathrm{i},v_\mathrm{j})\in\overline{P}} [-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))]^{\alpha_k}\right) \times [-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))]^{\alpha_k - 1} \times \frac{p_{\mathrm{i,j}}(x_{\mathrm{i,j}})}{p_{\mathrm{i,j}}(x_{\mathrm{i,j}})}$$
$$\times \left(-\sum_{(v_\mathrm{i},v_\mathrm{j})\in\overline{P}} \log(-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))) \times [-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))]^{\alpha_k} - 1 + \left(\frac{\alpha_k(\alpha_k-1)}{\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))} \times \frac{p_{\mathrm{i,j}}(x_{\mathrm{i,j}})}{p_{\mathrm{i,j}}(x_{\mathrm{i,j}})}\right)\right).$$

Since $0 < p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) \leq \frac{1}{\mathrm{e}}$, we have $1 \leq -\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})) < \infty$ and $0 \leq \log(-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))) < \infty$. Thus, the firt term is negative. Moreover, since $p_{\mathrm{i,j}}(x_{\mathrm{i,j}})$ is decreasing in the defense investment $x_{\mathrm{i,j}}$, we have $p_{\mathrm{i,j}}(x_{\mathrm{i,j}}) < 0$, and since $\alpha_k \in (0,1]$ and $-\infty < \log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}})) \leq -1$ (from above), the third term is non-positive. Therefore, the whole term

$$\left(-\sum_{(v_\mathrm{i},v_\mathrm{j})\in\overline{P}} \log(-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))) \times [-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))]^{\alpha_k}\right) - 1 + \left(\frac{\alpha_k(\alpha_k-1)}{\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))} \times \frac{p_{\mathrm{i,j}}(x_{\mathrm{i,j}})}{p_{\mathrm{i,j}}(x_{\mathrm{i,j}})}\right)$$

is negative. Finally, from the above analysis and noting that $\exp(x) > 0 \forall x \in (0,\infty)$, the whole term $\sum_{v_m \in V_k} L_m \exp\left(-\sum_{(v_\mathrm{i},v_\mathrm{j})\in\overline{P}} [-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))]^{\alpha_k}\right) \times [-\log(p_{\mathrm{i,j}}(x_{\mathrm{i,j}}))]^{\alpha_k - 1} \times \frac{p_{\mathrm{i,j}}(x_{\mathrm{i,j}})}{p_{\mathrm{i,j}}(x_{\mathrm{i,j}})}$ is negative. Therefore, we have $\frac{d}{d\alpha_k}\frac{\partial C_k}{\partial x^n_{\mathrm{i,j}}}(\mathbf{x}^*) > 0$.

Now, differentiating (8.13) w.r.t. α_k with noting that the joint investment profile $\mathbf{x}_{-k}$ is fixed yields

$$\frac{d}{d\alpha_k} t^*_k(\mathbf{x}^*) = -L_k \sum_{n=1}^{|D|} \sum_{(v_\mathrm{i},v_\mathrm{j})\in\mathcal{E}_n} x^{n^*}_{\mathrm{ij}} \frac{d}{d\alpha_k}\frac{\partial C_k}{\partial x^n_{\mathrm{i,j}}}(\mathbf{x}^*),$$

which is negative since $\frac{d}{d\alpha_k}\frac{\partial C_k}{\partial x^n_{\mathrm{i,j}}}(\mathbf{x}^*) > 0$ and since $\exists D_n$ s.t. $x^{n^*}_{\mathrm{i,j}} > 0$ for at least one edge $(v_\mathrm{i}, v_\mathrm{j})$. □

Behavioral level and the amount of taxes: Theorem 8.5.1 shows that under appropriate conditions, the behavioral defender would pay more taxes compared to a rational defender under the Externality mechanism. The reason for such an increase in taxes is that the perception of the behavioral defender of the externality from other defenders' investments (via the drop in her perceived cost from such investments) induce the defender to pay more taxes for such a (perceived) increased safety level. We emphasize that the central regulator does not enforce rational decision-making on defenders but serves as a coordinator that

facilitates the mechanism-based game between the defenders and incentivizes the optimal behavior of each defender by assessing a tax t_k (via creating the tax scheme upfront).

8.5.2 The VCG Mechanism

The second mechanism that we consider here is the VCG mechanism [40], [109], also commonly known as the Pivotal Mechanism. This is a family of mechanisms in which the central planner incentivizes users (defenders) to reveal their true preferences in dominant strategies through the appropriate design of taxes for users with quasi-linear utilities (or costs). This leads to achieving the socially optimal solution. In this mechanism, each defender D_k receives a monetary transfer equal to the amount he contributes to the rest of the society. This ingenious, but simple, idea leads to aligning the incentives of all players with the social cost.

VCG Mechanism Explanation: Let $\mathbf{x}^*_{-\mathbf{k}}$ denote the equilibrium (by all defenders except D_k) under exit of user D_k (i.e., assuming D_k is not spending anything on defense), which is given by

$$\mathbf{x}^*_{-\mathbf{k}} = \underset{\substack{\mathbf{x}\succeq\mathbf{0};\\ \mathbf{1}^T\mathbf{x}\leq\sum_{\mathrm{j}\neq k} B_\mathrm{j}}}{\operatorname{argmin}} \sum_{\mathrm{j}\neq k} C_\mathrm{j}(\mathbf{x}). \tag{8.14}$$

Let $\overline{\mathbf{x}}$ represents a PNE investment vector by all defenders (including defender D_k). Thus, the taxes paid by D_k in the VCG mechanism under $\overline{\mathbf{x}}$ for our interdependent security games are given by

$$t^*_k = \sum_{\mathrm{j}\neq k} C_\mathrm{j}(\overline{\mathbf{x}}) - \sum_{\mathrm{j}\neq k} C_\mathrm{j}(\mathbf{x}^*_{-\mathbf{k}}). \tag{8.15}$$

Interpretation of the VCG mechanism: Intuitively, each defender receives a monetary transfer which is equivalent to her "contribution" to the rest of the society. For instance, if the defender D_k's investments makes the system worse, i.e., the social cost (without counting defender D_k) under the social optimal (including defender D_k's investments) is higher than the social cost without including her in the system, then the tax amount t^*_k would be positive. In other words, the mechanism penalizes the defender D_k for worsening the system. On the other hand, if defender D_k's investments makes the system better (i.e., with less social cost), t_k would be negative (i.e., D_k would receive such amount as a reward).

We now characterize the weak budget balance constraint and different amount of taxes paid by defenders under the VCG mechanism in our interdependent security games, respectively.

Proposition 8.5.2. *There exists an interdependent security game instance in which the VCG tax-based incentive mechanism cannot implement the socially optimal solution while guaranteeing weak budget balance.*

Proof. We prove this impossibility by the following counter example with one family of instance game as shown below.

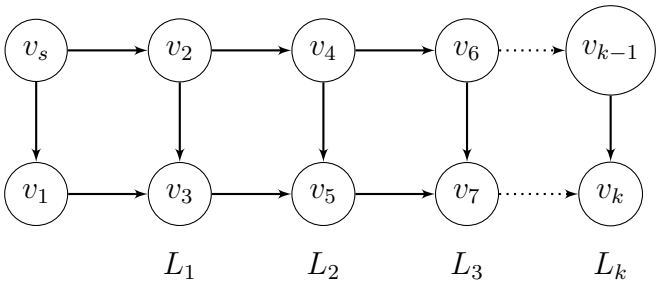


Figure 8.4. An example for a graph structure (with k defenders) in which the VCG mechanism achieves the socially optimal allocation but has a budget deficit.

Example 4. Consider the instance of interdependent security game of k rational defenders on the attack graph shown in Figure 8.4. We now show the details of taxes calculation.

First the PNE solution is given by

$$\overline{\mathbf{x}} = \left[\frac{\sum_{\mathrm{i}=1}^{k} B_{\mathrm{i}}}{2} \quad \frac{\sum_{\mathrm{i}=1}^{k} B_{\mathrm{i}}}{2} \quad 0 \quad \cdots \quad 0\right]$$

In other words, the total budget, which is the sum of the budgets of all defenders, would be distributed equally between the two min-cut edges (v_s, v_1), and (v_s, v_2). For each defender D_{i}, the total social cost (not counting D_{i}) is given by

$$\sum_{\mathrm{j}=1,\mathrm{j}\neq\mathrm{i}}^{k} C_{\mathrm{j}}(\overline{\mathbf{x}}) = \left(\sum_{\mathrm{j}\neq\mathrm{i}} L_{\mathrm{j}}\right) \times \left(\mathrm{e}^{-\frac{\sum_{\mathrm{j}=1}^{k} B_{\mathrm{j}}}{2}}\right).$$

Now, if defender D_{i} was not a member of the society, the equilibrium without defender D_{i}, denoted by $\mathbf{x}^*_{-\mathbf{i}}$ is given by $\mathbf{x}^*_{-\mathbf{i}} = \left[\frac{\sum_{\mathrm{j}=1,\mathrm{j}\neq\mathrm{i}}^{k} B_{\mathrm{j}}}{2} \quad \frac{\sum_{\mathrm{j}=1,\mathrm{j}\neq\mathrm{i}}^{k} B_{\mathrm{j}}}{2} \quad 0 \quad \dots \quad 0\right]$. Therefore, the amount of tax paid by defender D_{i} is given by

$$\begin{aligned} t^*_{\mathrm{i}} &= \sum_{\mathrm{j}\neq\mathrm{i}} C_{\mathrm{j}}(\overline{\mathbf{x}}) - \sum_{\mathrm{j}\neq\mathrm{i}} C_{\mathrm{j}}(\mathbf{x}^*_{-\mathbf{i}}) \\ &= \left(\sum_{\mathrm{j}\neq\mathrm{i}} L_{\mathrm{j}}\right) \times \left(\mathrm{e}^{-\frac{\sum_{\mathrm{j}=1,\mathrm{j}\neq\mathrm{i}}^{k} B_{\mathrm{j}}}{2}}\right) \times \left(\mathrm{e}^{-\frac{B_{\mathrm{i}}}{2}} - 1\right), \end{aligned}$$

which is negative for each defender D_{i} with a positive security budget (with $B_{\mathrm{i}} > 0$). Therefore, summing the taxes of all players yields that $t^*_{\mathrm{i}} < 0$. □

Intuition: This result shows a budget deficit case for the VCG mechanism in which the central regulator has to spend out-of-pocket money to incentivize the defenders to achieve the social optimal solution. It was shown that the VCG mechanism achieves social optimality, and achieves weak budget balance in many private and public good games (see [40], [110], [111] for more details and related background). However, we show for the first time that this is not satisfied in interdependent security games. Fundamentally this is because, in interdependent security games a defender can free ride (i.e., under-invest in security and depend on investments from other defenders). Thus, such defender needs to be incentivized to achieve the socially optimal solution.

Effect of behavioral level on amount of taxes: We now show that higher behavioral bias (i.e., smaller α) leads to the payment of more taxes (by defenders) under the VCG mechanism. The reason for such increase in the taxes paid is that if any defender $D_k \in \mathcal{D}$ becomes more behavioral, her investments become more suboptimal and consequently increase (worsen) the system's social cost compared to the case in which D_k is not a member of the society. Thus, the VCG mechanism imposes more taxes on D_k in such scenario. We validate this finding in our evaluation (Section 8.6).

8.5.3 Voluntary Participation Mechanism Design

We next explore voluntary participation in interdependent security games modeled by attack graphs. To participate in the mechanism, a defender $D_k \in \mathcal{D}$ should have a preference for being part of the mechanism over opting out. In other words, the overall cost of defender D_k under the mechanism, which is the defender's cost under the attained joint investment profile by the mechanism plus the taxes paid by the defender to the central regulator (planner), must be lower than or equal to defender D_k's cost under PNE (for all defenders). Formally, a defender $D_k \in \mathcal{D}$ participates in the mechanism if

$$C_k(\mathbf{x}^*) + t_k \leq C_k(\bar{\mathbf{x}}),$$

where $C_k(\mathbf{x}^*)$ is defender D_k's cost under the socially optimal outcome (induced by the mechanism) and $C_k(\bar{\mathbf{x}})$ is the corresponding PNE (state of anarchy) with no defender $D_k \in \mathcal{D}$ being a part of the mechanism.

We first define a class of directed acyclic attack graphs (DAG) defined as a "Layered DAG" [112] which is a special case of a DAG where nodes are partitioned into l layers and the DAG has certain properties.[2]

Definition 8.5.1. *Let $v_{\mathrm{i}}^{\mathrm{j}}$ be the* j*-th node in layer* i *and $H_{\mathrm{i}} = \{v_{\mathrm{i}}^{\mathrm{j}} | \forall \mathrm{j}\}$ be the set of all nodes in layer* i*. In a layered DAG, $\mathcal{E}$ only contains edges that connect nodes in H_{i} to nodes in $H_{\mathrm{i}+1}$, $\forall 1 \leq \mathrm{i} \leq l-1$.*

Amount of Taxes and Voluntary Participation: We now present result on voluntary participation in our tax-based framework for the introduced class of layered attack graphs.

Proposition 8.5.3. *Suppose that G denotes a layered DAG that has K behavioral defenders (with $\alpha_k \in (0,1)$), where each layer k has a single node v_k and under ownership of a defender $D_k \in D$. Suppose that the probability of successful attack on each edge $(v_{\mathrm{i}}, v_{\mathrm{j}})$ is given by (2.6) with $p_{\mathrm{i,j}}^0 = 1$. Suppose that each defender has security budget $\frac{B}{K}$ and that L_{i} is the financial loss of asset v_{i}. Then, we have*

[2] ↑The layered DAG structure represents stepping-stone nature of attacks on the critical assets within the system that we consider here where attacker uses one asset in one layer to progressively attack other assets in deeper layers.

i. If $t_{\mathrm{i}} \leq L_{\mathrm{i}} \left[\exp\left(-\frac{\mathrm{i}B}{K}\right) - \exp(-B)\right]$*, then defender* D_{i} *would participate in the mechanism*

ii. The maximum amount of tax t_{i}^{max} *that a defender can be charged and participate in the mechanism is decreasing in the defender index* $\mathrm{i}, \forall \mathrm{i} = 1, \cdots, K$.[3]

Proof. From the Proposition statement, the socially optimal solution would put all the budget B on the first edge (v_s, v_1), so that all nodes have a probability of successful attack given by $\exp(-B)$. Now, we prove the first part (i) as follows.

The PNE for behavioral defenders is given by the investment profile where each defender D_k puts their entire budget $\frac{B}{K}$ on the edge coming into their node v_k (similar to analysis in Example 2). Therefore, the true cost of defender D_1 under this PNE is $L_1 \exp\left(-\frac{B}{K}\right)$.

Now, to have defender D_1 participate in the mechanism we must have

$$\begin{aligned} C_1(\mathbf{x}^*) + t_1 \leq C_1(\bar{\mathbf{x}}) & \\ \iff L_1 \exp(-B) + t_1 \leq L_1 \exp\left(-\frac{B}{K}\right) & \\ \iff t_1 \leq L_1 \left[\exp\left(-\frac{B}{K}\right) - \exp(-B)\right]. & \end{aligned}$$

For defenders $D_2, D_3, \cdots, D_{K-1}$, defender D_{i} would participate in the mechanism if

$$\begin{aligned} C_{\mathrm{i}}(\mathbf{x}^*) + t_{\mathrm{i}} \leq C_{\mathrm{i}}(\bar{\mathbf{x}}) \iff L_{\mathrm{i}} \exp(-B) + t_{\mathrm{i}} \leq L_{\mathrm{i}} \exp\left(-\frac{\mathrm{i}B}{K}\right) & \\ \iff t_{\mathrm{i}} \leq L_{\mathrm{i}} \left[\exp\left(-\frac{\mathrm{i}B}{K}\right) - \exp(-B)\right]. & \end{aligned}$$

This concludes the proof of the first part.

Now, we prove the second part (ii) From part (i), a defender $D_{\mathrm{i}} \in D$ can participate while paying at most the max amount of tax $t_{\mathrm{i}}^{max} = L_{\mathrm{i}} \left[\exp\left(-\frac{\mathrm{i}B}{K}\right) - \exp(-B)\right]$. Differentiating t_{i}^{max} w.r.t the defender index i yields

$$\frac{\partial t_{\mathrm{i}}^{max}}{\partial \mathrm{i}} = L_{\mathrm{i}} \times \exp\left(-\frac{\mathrm{i}B}{K}\right) \times \frac{-B}{K},$$

[3]↑Defender D_{i}'s asset is closer to attacker's source node than defender $D_{\mathrm{i}+1}$'s asset and thus defender D_{i} securing her asset benefits all D_{j}, with $\mathrm{j} > \mathrm{i}$.

which is negative since the exponential function range is $(0, \infty)$, L_{i} is the non-negative financial loss when defender D_{i}'s asset is compromised, and $\frac{B}{K}$ is the non-negative security budget of each defender $D_{\mathrm{i}} \in D$. This concludes the proof of the second part. □

Intuition: The above result shows two main insights about taxation and participation in the mechanism. First, in the layered DAG, each defender would prefer participation in the mechanism if the amount of taxes she pays is less than or equal to the difference between the socially optimal solution and the state of anarchy (PNE). Otherwise, the defender would prefer to not participate in the mechanism since she can have a lower cost without participation. Second, the social planner can impose more taxes on the defenders that are nearer from the attacker's source node v_s in the attack graph compared to those who are far from the source node. The reason is that the latter can free-ride on the security investments of the former and will prefer PNE over the mechanism if they are charged high amount of taxes. For instance, in the DAG considered in Proposition 8.5.3, the maximum amount of tax to be imposed on the last defender D_K to participate in the mechanism is zero.

Remark 12. We also observe similar results of amount of taxes and participation in all of our four case studies (in Section 8.6) which have different attack graph structures.

Having introduced the two mechanisms, established the impossibility result, shown the effect of behavioral level on tax amounts paid by defenders, and explored voluntary participation, we now turn our attention to the evaluation of the mechanisms using real-world interdependent systems.

8.6 Evaluation

Our evaluation aims to answer the following questions:

- What is the gain of using mechanism design for incentivizing behavioral defenders toward the socially optimal solution?
- How does the level of behavioral bias affect the mechanism design outcomes?
- What is the maximum tax payment under which the defender prefers to participate in a tax-based mechanism over the state of anarchy (PNE)?

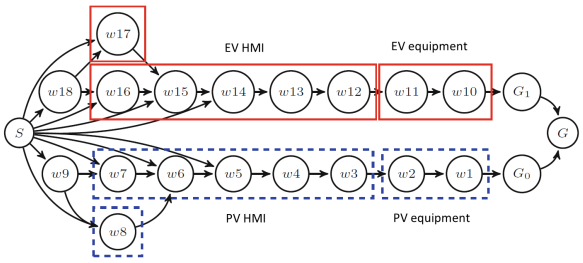


Figure 8.5. Attack Graph of DER System

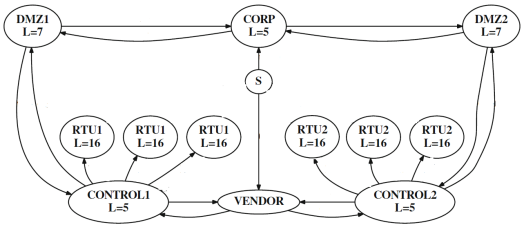


Figure 8.6. Attack Graph of SCADA System

8.6.1 Dataset Description

We use four synthesized attack graphs that represent real-world interdependent systems to evaluate our setups. Specifically, we consider four popular interdependent systems from the literature which are: DER.1 [17], SCADA [12], E-commerce [13], and VoIP [13]. In all of these systems, nodes represent the progression of attack steps (e.g., unauthorized control of a physical generator in DER.1, taking privilege of control unit software in SCADA). Note that for each of our applications, it could be either air-gapped (attack would be from an insider attacker) or externally accessible (attack would be from an external adversary).

Now, we give a brief explanation of these systems and their associated failure scenarios. We generate the attack graphs of these systems using the CyberSage tool [17] 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 US National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group has introduced a framework for evaluating the risks of cyber attacks on the electric grid. A distributed energy resource (DER) is described as a cyber-physical system consisting of entities such as generators, storage devices, and electric vehicles, that are part of the smart energy distribution system. The DER.1 failure scenario has been identified as the riskiest failure scenario affecting distributed energy resources according to the NESCOR ranking [17]. As shown in Figure 8.5, there are two critical equipment assets: a PhotoVoltaic (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.1 failure scenario is triggered when the attacker gets access to the HMI. Once the attacker gets access to the system, she changes the DER settings and gets physical access to the DER equipment so that they continue to provide power even during a power system fault. Through this manipulation, the attacker can cause serious physical damage to the system.

SCADA System Description: The SCADA system is composed of two control subsystems, where each incorporates a number of cyber components, such as control subnetworks and remote terminal units (RTUs), and physical components, such as, valves controlled by the RTUs. We followed the NIST guidelines for industrial control systems for such architecture [113], where each subsystem is separated from external networks through a demilitarized zone (DMZ). The system implements firewalls both between the DMZ and the external networks, as well as between the DMZ and its control subnetwork. Therefore, an attacker must bypass two different levels of security to gain access to these control subnetworks. These two subsystems are interdependent via the shared corporate network, as well as due to having a common vendor for their control equipment. The resulting attack graph of the described system is shown in Figure 8.6. The "Corp" and the "Vendor" nodes connect the two subnetworks belonging to the two different defenders and can be used as jump points to spread an attack from one control subsystem to the other. This system has six critical assets (3 RTUs, Control Unit, CORP, and DMZ). The compromise of a control network "CONTROL i" will lead to loss of control of all 3 connected RTUs.

E-commerce System Description: The E-commerce system overview is shown in Figure 8.7. The web server sits in a DMZ separated by a firewall from the other two servers, which are connected to a network not accessible from the Internet. All connections from the Internet and through servers are controlled by the firewall. Rules state that the web and application servers can communicate, and the web server can be reached from the Internet. Here, the attacker is assumed to be external and thus her starting point is the Internet and uses stepping-stone attacks with the goal of having access to the MySQL database, (specifically access customer confidential data such as credit card information) represented by node 19 in the attack graph. For this system, we follow the attack graph generated by

[13] (Figure 8.7 (on right), shaded nodes are detectors, not attack steps), based on popular vulnerabilities databases [114].

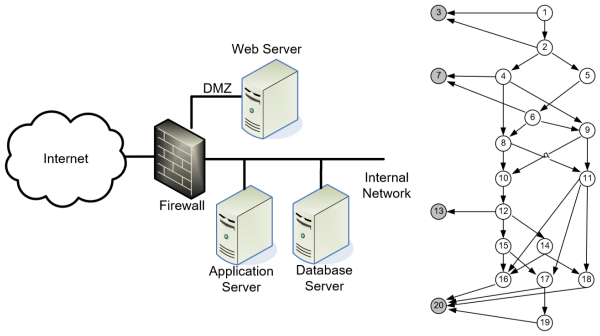


Figure 8.7. A high level network overview of E-commerce (on left) adapted from [13]. The resultant attack graph (on right).

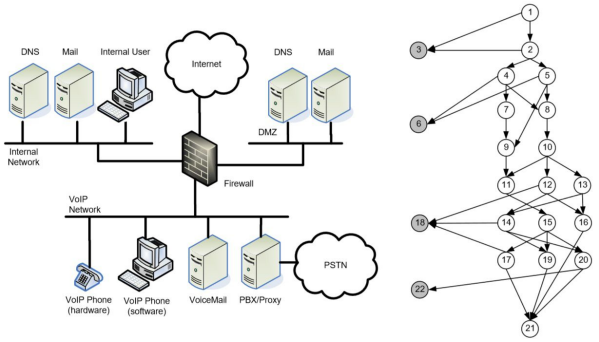


Figure 8.8. A high level network overview of VoIP (on left) adapted from [13] and its resultant attack graph (on right).

VoIP System Description: As shown in Figure 8.8, the VoIP system is composed of three zones; a DMZ for the servers accessible from the cloud, an internal network for local resources (e.g., computers, mail server and DNS server), and an internal network that is consisted of only VoIP components. This architecture follows the NIST security guidelines for deploying a secure VoIP system [107]. In this context, the VoIP network consists of a Proxy, voicemail server, and software-based and hardware-based phones. The firewall has rules to control the traffic between the three zones. Note that the DNS and mail servers in the DMZ are the only accessible nodes to the Internet. The PBX server can route calls to the Internet or to a public-switched telephone network (PSTN). The ultimate attack goal is to eavesdrop on VoIP communication. Figure 8.8 shows the resultant attack graph.

Having explained the failure scenarios of our four interdependent systems. Next, we present our experimental setup which includes simulation parameters and the procedure.

8.6.2 Experimental Setup

The simulations are based on our proposed game-theoretic models in Section 8.2 and mechanism-based models in Section 8.5 with the following parameters. Each system has two defenders. For DER, E-commerce, and VoIP, we have the financial losses $L_i = L =$

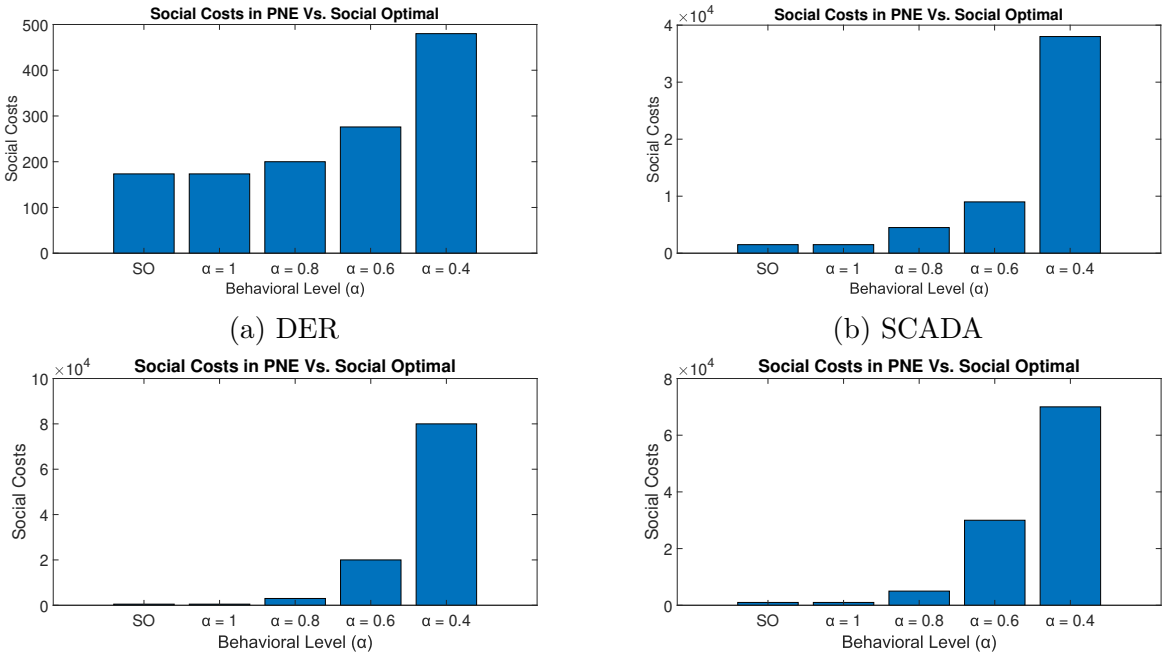
$\$2M, \forall$i. The losses of the critical assets within SCADA (in Million dollars) are shown in Figure 8.6. We used the probability of successful attack function in (2.6) in our simulations. To estimate the baseline probability of successful attack on each edge (i.e., without any security investment), we first create a table of CVE-IDs (from real vulnerabilities reported in the CVE database for 2000-2020). We then followed [24] to convert the main attack's metrics (i.e., attack vector, attack complexity) to a baseline probability of successful attack. Table 8.2 illustrates this process for DER.1 and SCADA systems. We sweep the behavioral bias α such that $\alpha \in [0.4, 1]$; this is consistent with the range of behavioral parameters from prior experimental studies [15], [78]. We consider a symmetric security budget across the defenders (unless otherwise stated). For Nash Equilibrium, we run the best response dynamics until the game reaches the Nash Equilibrium while the social optimal is found using (8.2). Our work refers to the setup with any of the two proposed mechanisms since both mechanisms lead to the social optimal, albeit with different tax collections.

Table 8.2. Baseline probability of successful attack for vulnerabilities in SCADA and DER.1 systems.

Vulnerability (CVE-ID)	**Edge(s)**	**Attack Vector**	**Score**
SCADA application			
Control Unit (CVE-2018-5313)	(Vendor,Control1),(Vendor,Control2)	Local	0.78
Remote authentication (CVE-2010-4732)	(S, Vendor)	Network	0.9
Remote cmd injection (CVE-2011-1566)	(Control,RTU1),(Control,RTU2)	Network	1.0
Authentication bypassing (CVE-2019-6519)	(Corp,DMZ1),(Corp,DMZ2)	Network	0.75
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

8.6.3 Evaluation Results

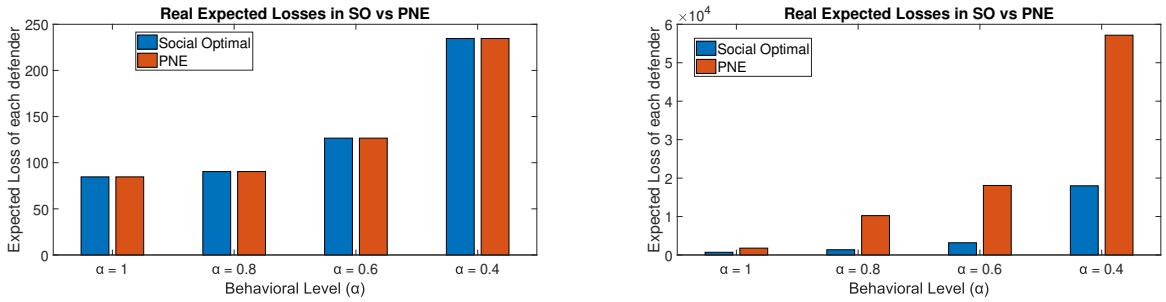
Next, we show our findings from different experiments for the four interdependent systems. Mainly, we compare the security investments (by both classes of decision-makers), the social costs under different investments, the per-defender expected loss, the amount of taxes (payments) under the two mechanisms (from Section 8.5), the effect of behavioral decision-making, and the trends in voluntary participation. The complete evaluation results can e found in [115].



(a) DER (b) SCADA

(c) E-commerce (d) VoIP

Figure 8.9. A comparison of social costs under the socially optimal allocation (induced by mechanism) versus the PNE. We observe that the social cost under the socially optimal allocation is much lower than the social cost under PNE with behavioral defenders.



(a) DER (b) SCADA

Figure 8.10. A comparison of expected loss of each defender under the social optimal (SO) versus the PNE under different behavioral levels. We observe that the expected loss under SO is lower than (same in DER) that under PNE irrespective of behavioral level.

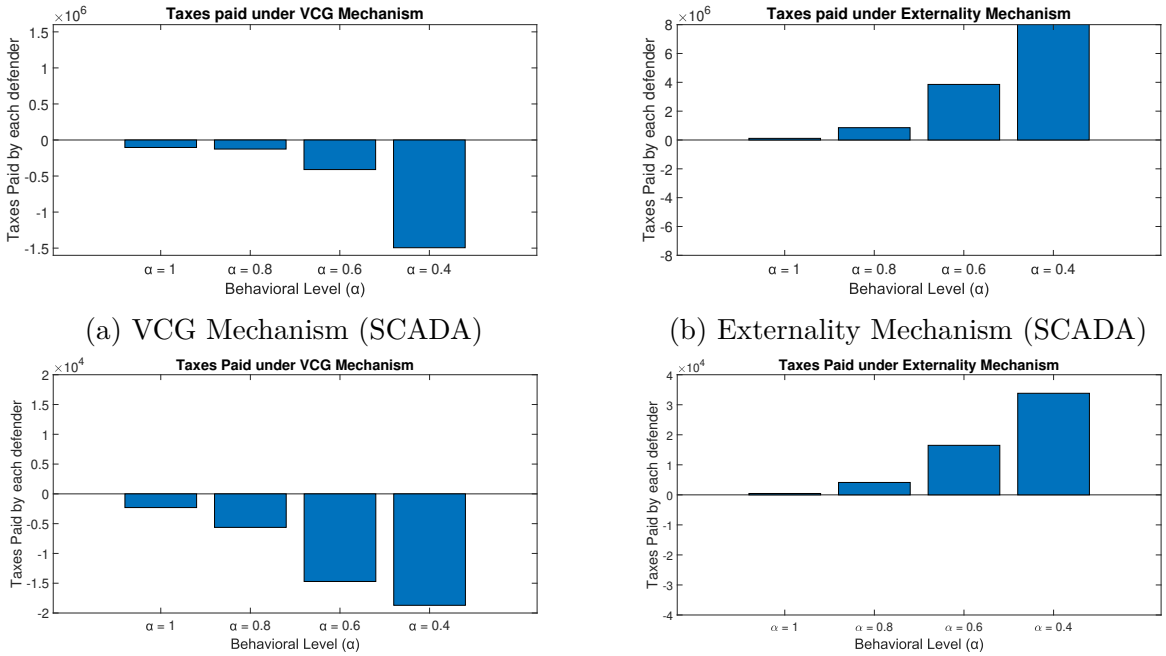
Security Investments: We observe that the socially optimal allocation leads to distributing investments only on min-cut edges[4]. On the other hand, behavioral defenders distribute their investments across the network. This finding motivates the importance of incentivizing behavioral defenders to achieve social optimal investments since this would lead to reducing the per-defender real cost and the social cost as shown next.

Social Costs: Figure 8.9a-8.9d demonstrate the reduction in social cost (which is the sum of the real costs of all defenders) following the implementation of the mechanism for the four systems. We observe that the mechanism design is more helpful for moderate and highly behavioral defenders since the behavioral investments under PNE is much worse than the social optimal solution. Numerically, as a result of risk reduction following the implementation of the mechanism, we see that the gain for society (represented by the ratio of the social cost under PNE to social cost under the mechanism) is 3X for DER, 180X for SCADA, 450X for E-commerce, and 390X for VoIP when the defenders are highly behavioral (i.e., $\alpha_1 = \alpha_2 = 0.4$). This result shows that the social cost under the socially optimal allocation is much lower than that under PNE, and the gap is higher for highly behavioral defenders and for systems with higher degree of interdependency.

Defender's Real Expected Loss: Figure 8.10a and 8.10b illustrate the real expected losses of all defenders under both the PNE and the socially optimal outcome (incentivized by the mechanism). Here the social planner is made to be behavioral along with the defenders, at the same level (same value of α). From the result, we see that implementing the proposed mechanisms would incentivize risk reduction for each defender for SCADA system while keeping the risk the same for the DER system. This happens due to the loose interdependency in the DER system. With such loose interdependency, the social optimality is achieved simply by the defenders individually spending their security resources efficiently.

Tax Payment Amounts: Here, we compare tax payments under different scenarios for both mechanisms that we study here. First, for the DER.1 system, it has the nature that each subnetwork is mainly affected by the corresponding defender. Therefore, under VCG mechanism, both defenders can reach the social optimal without paying taxes (i.e.,

[4]↑The min-cut edges are the edges in the minimal set that can be removed to disconnect the graph. Here the same concept is applied to our attack graph.



(a) VCG Mechanism (SCADA)

(b) Externality Mechanism (SCADA)

(c) VCG Mechanism (E-commerce)

(d) Externality Mech. (E-commerce)

Figure 8.11. The amount of taxes paid by each defender under the studied mechanisms. For the VCG Mechanism, the player receives payment (i.e., pay negative taxes). On the other hand, under the Externality mechanism each defender pays positive taxes.

budget balance for the central regulator). Hence, we omit this figure. However, for the SCADA system since the two subnetworks are mainly interdependent (i.e., if the attacker access both subnetworks via the Corp and the Vendor nodes, as explained earlier), the budget balance condition is not satisfied for the VCG mechanism. Figure 8.11a shows such insight where each of the two defenders is paid by the central regulator in the VCG mechanism since each defender makes the SCADA system more secure by her investments. We note also that although behavioral defenders invest suboptimally, they also benefit other defenders in the network (reduce the social cost) and thus need also to be paid by the VCG mechanism regulator. On the other hand, Figure 8.11b shows that the budget balance condition is satisfied with the Externality mechanism since each defender pays for the positive externalities on her cost due to other defender's investments. Figure 8.11c-8.11d show similar findings for E-commerce system due to interdependency among servers via firewalls and internet. We omit similar tax figures for VoIP.

Amount of Taxes and Voluntary Participation: Human bias is an important factor when trying to understand how stakeholders would react to the security tax. Thus, we consider next the voluntary participation of the defenders under any quasi-linear tax-based mechanism. This requires calculation of the maximum tax payment under which each defender would participate in the mechanism. Figure 8.12 shows such maximum tax amount for our four interdependent systems under different behavioral levels. The highly behavioral defender is willing to participate in the mechanism even under higher tax payments since her suboptimal investments are far from the socially optimal level. For her, paying higher taxes and allocating resources according to the social optimum would yield lower total real loss compared to opting out and achieving PNE.

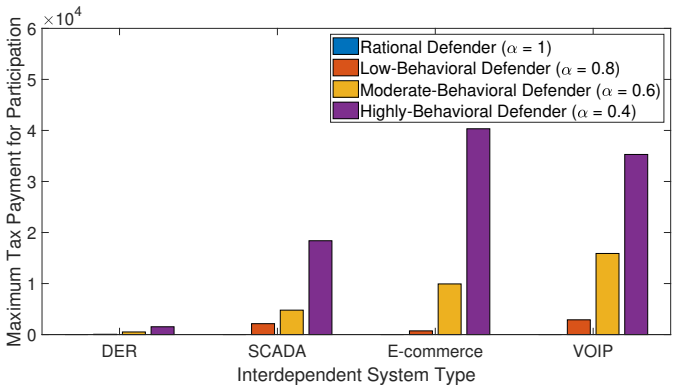
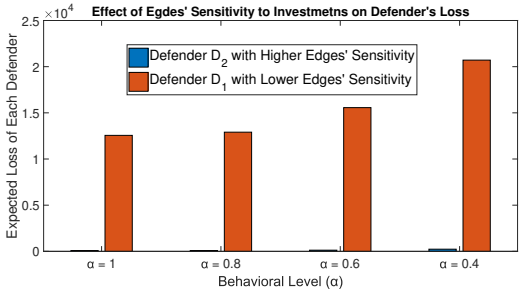


Figure 8.12. The maximum amount of tax payment under which each defender participates in the mechanism for the four studied interdependent systems. The highly behavioral defender is willing to participate under higher tax payment.

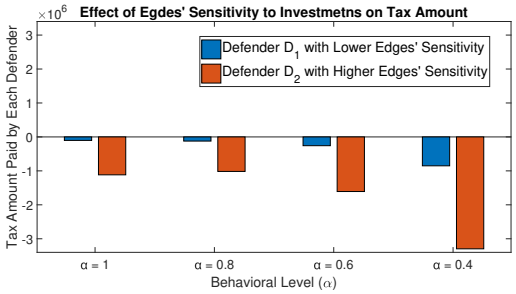
Sensitivity of Edges to Investments: Finally, we show the effect of edges' sensitivity to investments on each defender's real expected loss for different behavioral levels. Recall from (2.6) that edges with higher sensitivity are those for which the probability of successful attack decreases faster with each unit of security investment. In this experiment, for both DER and SCADA systems, we assume that the defender D_1 has lower edges' sensitivities to her investments compared to the defender D_2. Formally, we let $s^1_{i,j} = 0.5$ (for D_1) and $s^2_{i,j} = 1$ (for D_2). That can be mapped into realistic scenario where D_1's methods for investing on edges are less effective in reducing the probability of successful attack compared to D_2.

For DER system, we show the effect of edges' sensitivity to investments on each defender's real expected loss for different behavioral levels in Figure 8.13a. We observe that the defender with the higher edges' sensitivity (here, D_1) would have much lower expected loss compared to the defender with the lower edges' sensitivity (here, D_2) irrespective of the behavioral level of the defender. However, both defenders pay zero amount of taxes under all behavioral levels due to loose interdependency across the two defenders' subnetworks in DER.

For SCADA system, we show the effect of sensitivity of edges to investments on the amount of taxes paid by each defender under the VCG mechanism. Figure 8.13b shows that D_2 would receive more amount of payments compared to D_1 for all behavioral levels. The intuition here is that D_2 is more beneficial to the society as her investments reduce the social cost more compared to the investments of D_1 (since the sensitivity of edges to D_2's investments is twice the sensitivity of edges to D_1's investments). Therefore, under the VCG mechanism, D_2 would receive much more amount due to her contribution to the society. Moreover, we note that the effect of edges' sensitivity is more pronounced under higher behavioral bias (i.e., less α) and therefore the difference in the amount of taxes among the two defenders increases as defenders become more behavioral (since D_1 even wastes her budget on edges that has less sensitivity to those non-critical edges). The high-level takeaway is that a defender whose edge is more sensitive to investments (i.e., the probability of successful attack goes down faster) gets more tax payments under the mechanisms.



(a) Effect of asymmetry in edges' sensitivity to investments across the two defenders on the loss of each defender on DER system.



(b) Effect of asymmetry in edges' sensitivity to investments across the two defenders on tax amount under VCG on SCADA system.

Figure 8.13. The effect of asymmetry in edges' sensitivity to investments across the two defenders on the loss of each defender and the amount of taxes paid by the defender under the VCG mechanism.

8.6.4 Baseline Systems

We compare our framework with four baseline systems under rational defenders: the seminal work of [16] for security investment with attack graphs on attack graph generation and investment decision analysis[5], [38] for placing security resources using defense in depth technique which traverses all edges that can be used to compromise each critical asset and distribute resources equally on them, the recent work [71] that explored behavioral decision-making in a non-cooperative setup (PNE characterization), and the recent work [99] that showed that attackers follow shorter paths to exploit target assets in the generated attack graphs. Table 8.3 shows such comparison by calculating the social cost under each work's defense allocation, indicating the superiority of our proposed framework for almost all our interdependent systems (note similar results between our proposed approach and most baselines for DER.1 in Table 8.3 due to the weak interdependency in this system). Since three of the four baselines (except [71]) do not design for behavioral defenders, we do not consider such defenders in this experiment. The result bears out the fact that the defense investments given by [71] and [16] are identical under rational decision-making.

Table 8.3. Comparison of our framework and baseline systems in terms of the social cost under each system's defense allocation (lower is better). For our framework, we consider a rational social planner. Our framework gives the best defense allocation among the techniques (resp. the lowest social cost).

System Type	S&P02 [16]	Milcomm06 [38]	AsiaCCS21 [71]	CCS21 [99]	Our Work
DER.1	**173.390**	600.451	**173.390**	**173.390**	**173.390**
SCADA	513.230	4.023×10^4	513.230	5.902×10^3	**222.210**
E-commerce	47.014	8.115×10^4	47.014	2.493×10^4	**45.001**
VoIP	184.120	1.525×10^5	184.120	1.4859×10^4	**110.21**

8.7 Related Work

Mechanism design in security: The motivation for considering mechanism design models in the security literature comes from two main characteristics of security games with multiple defenders. First, the security investments of each defender can help other defenders, similar to public good provision with positive externalities. Second, defenders can

[5]↑More recent approaches (e.g., [92], [116], [117]) follow same strategy of [16].

therefore free ride and depend on security investments by other defenders. This leads to an inefficiently low overall security level of the system [39], [40]. This motivates the study of mechanisms for improving network security, and ideally, incentivizing user cooperation and driving the system to a socially optimal state of enhanced overall security, e.g., [41], [72]. However, to the best of our knowledge, no previous work in mechanism design has investigated behavioral decision-making effects and considered attack graphs that can model any large-scale interdependent system.

Our presented impossibility result differs from those in the existing literature, which builds on the seminal work of Green and Laffont [118]. We differ in terms of the selected equilibrium solution concept, the set of properties the mechanism is required to satisfy, the space of cost functions, or the nature of the system type. For instance, the Myerson and Satterthwaite result [40] considers a Bayesian Nash solution while we have a Pure Nash implementation. On the other hand, Maskin's work on implementation theory [119] considers Nash equilibrium for the complete information setup. However it requires that all NE be socially optimal which cannot be guaranteed in interdependent security games (see Section 8.4). Finally, the line of work [41], [72] has considered quasi-linear costs (where the tax is added to the original cost function) and Nash equilibrium solutions of the mechanisms, which has two main differences from our present work. First, they consider utilities with classical decision-making models, without the cognitive biases that we consider here. Second, they do not consider interdependent systems with attack graphs.

8.8 Discussion

(1) Existence of bias in security decision-makers: Numerous academic studies of even the most highly-trained specialists have shown that experts are also susceptible to systematic failures of human cognition (e.g., [84], [85]). Specifically, the work [85] has conducted a survey of experiments that considered behavior of students against experts in a wide variety of professions. This survey reports only one out of thirteen considered studies found that professionals make decisions more closely in line with standard economic theory. Moreover, recent research has shown that cybersecurity professionals' probability perceptions are as

susceptible to systematic biases as those of the general population [86], [120]. Finally, even if security experts exhibit weaker biases, this can still result in sub-optimal security investments and their effects may be magnified due to the magnitude of losses associated with compromised real-world assets that these experts control.

(2) Guiding security decision-makers: We believe that our framework provides an important estimate of the probability of successful attack (resp. expected financial loss). We compose that estimate from something that is easier to grasp — the loss due to each asset in the system being compromised. We believe that our work opens up a new dimension of *intervention* in securing interdependent systems by calculating the taxes charged to each subordinate to participate in the mechanism and enhance overall system security (social cost). As shown in Section 8.6, this would depend on the nature of the network and the interdependency among different defenders.

(3) Mechanism design to solve behavioral bias in different security problems: Our proposed adaptation of the Externality and VCG mechanisms to interdependent security games (Section 8.5) can be further used for different security problems. Examples include defending isolated assets with heterogeneous valuations, e.g., for enhancing security decisions to defend different airports [121] or preventing DAG-based ransomware attacks [122]. Recent work has shown the effect of cognitive biases on security resource allocations in such settings using decision- and game-theoretic analysis [33], [36]. However, these studies do not consider any mitigation for such biases. Thus, using mechanism design to improve such biases would be an avenue for future work.

8.9 Summary of Findings

In this chapter, we analyzed two tax-based mechanism types for our interdependent security setups where the central regulator incentivizes defenders to achieve socially optimal allocations. The first mechanism, denoted by the Externality mechanism, charges each defender an amount that depends on the positive externalities on her cost under the other defenders' investments. The second mechanism, the Vickery-Clarke-Groves (VCG) mechanism, makes each defender pay a tax which is equivalent to his contribution to the

rest of the society (in terms of a social cost). We then showed that a mechanism designer cannot guarantee social optimality level of investment for the defenders under the mechanism without paying money to incentivize defenders in all instances of our interdependent security games. We also showed the effect of behavioral bias on the two mechanisms' outcomes where higher bias leads to paying more taxes under the two mechanisms. We then explored the relation between the tax amount and the voluntary participation of defenders in the mechanism and showed that behavioral defenders choose to participate in the mechanism even under higher tax payments, compared to rational defenders. We evaluated our framework via four real-world interdependent systems and showed the effect of mechanisms on social cost and the effect of behavioral decision-making on the mechanisms' outcomes. We compared the security cost achieved by security allocations of our framework compared to those of four baseline solutions from the attack graph literature. We found that even with rational defenders our framework either equals or outperforms the baselines. We believe that our study can help central regulators and interdependent systems' defenders attain improved understanding of their security risks and consequently make more effective investment decisions to mitigate such risks, including additional risk from decisions under cognitive biases.

9. SUMMARY AND Future Work

The security of interdependent systems, such as CPS, is challenging nowadays due to increasingly sophisticated attacks from external adversaries. Our work is exploring the effect of human bias on security decision-making in different interdependency settings (interdependent vs isolated) and game-theoretic scenarios (simultaneous vs sequential). This chapter summarizes my findings through my PhD research and presents possible future research extensions.

9.1 Behavioral Decision-Making in Securing Interdependent Systems

In this line of work, I have proposed a novel mathematical behavioral security game model for the study of the human decision-making in multi-defender Cyber Physical Systems (CPS). I have showed that behavioral biases lead to suboptimal decision-making compared to rational decision-making under correct perception of risk. In particular, the behavioral defenders shift investments from critical edges to non-critical edges. I have also given bounds on the inefficiency of game-theoretic equilibria with multiple behavioral defenders. Moreover, I have illustrated the effect of behavioral biases in five interdependent CPS case studies based on real-world attack scenarios where characterized different system parameters that affect the security decisions made by the system operators. The predictions generated by my model have subsequently been validated by controlled human subject experiments.

9.2 Behavioral Decision-Making in Securing Heterogeneous Isolated Assets

In this research, I have created a framework to analyze the outcomes of a human defender protecting multiple isolated assets with heterogeneous valuations. I have characterized the impacts of risk misperceptions on the security investments made by the defender, and showed that behavioral probability weighting can cause the defender to shift more of her investments to higher-valued assets compared to a defender who correctly perceives the attack probabilities. This suboptimal investment pattern thereby leads to an increase in the (true) expected loss for the behavioral defender. Then, I have extended the decision-theoretic

setup (that has only one defender) to the game-theoretic setup with multiple defenders protecting these assets. In particular, I have explored different characteristics of the game under the behavioral probability weighting bias such as the arising properties of total investments on the assets under different PNE, and the decreasing nature of the total investments on the highest valued asset as the defenders become more rational.

9.3 Behavioral Decision-Making in Attacker-Defender Games

In this line of work, I have characterized behavioral decision-making effects for multi targets with heterogeneous valuations using game-theoretic analysis. In particular, I have proposed a sequential game setting between the defender and the attacker in which the attacker targets the site that maximizes the expected loss for the defender (after observing the defender's investments). In another piece of work, I have proposed a simultaneous move game between the defender and the attacker where the defender can allocate preventive resources to best protect the assets while the attacker can allocate attack resources on these assets simultaneously. In this context, I studied the properties of the Nash equilibrium under both rational and behavioral decision-making.

9.4 Guiding Behavioral Decision-makers

In this line of work, I have proposed a *security investment guiding* technique for the defenders of interdependent systems where defenders' assets have mutual interdependencies. I have showed the effect of *behavioral* biases of human decision-making on system security and we quantify the level of gain due to our decision-making technique where defenders are behavioral. We validated the existence of bias via a controlled subject study and illustrated the benefits of our decision-making through multiple real-world interdependent systems. I have also analyzed the different system parameters that affect the security of interdependent systems under our behavioral model. I have then proposed three learning techniques to improve defense decisions in multi-round scenarios against different attack models that affect the security of interdependent systems while incorporating such effects with behavioral decision-making.

9.5 Using Mechanism Design for Enhancing Security Resource Allocation

In this line of work, I have studied how to enhance security investments by using mechanism design. I tried to show how can a social planner create incentives for the decision-makers to enhance their decisions to improve the overall security of their networks. I have incorporated two types of tax-based mechanisms (Externality mechanism and VCG mechanism) for our interdependent security games where the central regulator incentivizes defenders to invest well in securing their assets so as to achieve the socially optimal outcome. I have showed the effect of behavioral probability weighting bias on the amount of taxes paid by defenders, and proved that higher biases make defenders pay more taxes under the two mechanisms. I also explored voluntary participation in tax-based mechanisms and evaluated the mechanisms using four representative real-world interdependent systems where I compared the game-theoretic optimal investments to the socially optimal investments under the two mechanisms. I have shown that the mechanisms yield higher decrease in the social cost for behavioral decision-makers compared to rational decision-makers.

9.6 Conclusion

In total, my PhD research has established rigorous mathematical frameworks to analyze both large-scale interdependent systems and large-scale heterogeneous isolated assets managed by human decision-makers, which has led to new and important insights into security vulnerabilities that can arise in such settings. I strongly believe that the key drivers of my research (CPS security and behavioral human decision-making) are going to be increasingly important over the next decade due to the evolution of CPS systems and related security threats.

Although most of previous research that have considered behavioral economics in security and privacy has the common theme of considering individual choices regarding privacy and how people treat their own personal data [81], [123] or entirely based on psychological studies [49], [50], I consider the defense choices made by people in organizational contexts with interdependent system under control. My work considers scenarios that can be applied to critical infrastructure systems (e.g., cyber-physical systems).

9.7 Future Work

Having summarized the main findings of my thesis, I now present some prospective research directions to build upon my PhD research.

9.7.1 Enhancing security investments by learning

The first question to answer is: "How can the human decision-makers learn from their past decisions to improve the security of their networks?" The motivation for this question is the fact that the attackers and defenders have repeated interactions in practice (e.g., a hacker would perform trials for breaching the target system and the organization's security chef would refine the security protocols based on the history of attack incidents). In this context, I will propose learning algorithms (e.g., regret-learning and statistical learning) to help the defender take better actions. I have proposed preliminary models for a simplified version of such setup with different rounds in this thesis (see Chapter 7). However, proposing more rigorous models and explore more complex setups would be of interest.

9.7.2 Guiding security analysts and inferring attackers' strategies

The second question to answer is: "How can human security specialists make better decisions to make their systems less vulnerable to cyber attacks despite their incomplete information about the attacker?" The main motivation of this question is the pressing need to identify the most critical parts in the interdependent systems. Therefore, I will seek to create a visualization tool based on my analysis that can be readily utilized by security analysts to help them overcome behavioral biases and guide them towards optimal security investments. The second motivation for that question is the pressing need to rigorously model and infer the attacker strategies and incentives in such setups. Such modeling can help human security analysts to make better decisions and explore if the attacker can be deceived or has some behavioral aspects in her attack decisions. In this context, I will explore deception mechanisms and analyze how to exploit the behavioral risk attitude of the attacker to let her take actions that lead to a lower likelihood of successful attack.

REFERENCES

[1] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security – a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[2] V. Shandilya and S. Shiva, "On a generic security game model," *International Journal of Communications, Network and System Sciences*, vol. 10, no. 07, p. 142, 2017.

[3] A. Laszka, M. Felegyhazi, and L. Buttyan, "A survey of interdependent information security games," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, p. 23, 2015.

[4] T. Alpcan and T. Başar, *Network security: A decision and game-theoretic approach*. Cambridge University Press, 2010.

[5] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2038–2049, 2016.

[6] K. Hausken, "Strategic defense and attack of complex networks," *International Journal of Performability Engineering*, vol. 5, no. 1, pp. 13–30, 2009.

[7] P. Guan, M. He, J. Zhuang, and S. C. Hora, "Modeling a multitarget attacker–defender game with budget constraints," *Decision Analysis*, vol. 14, no. 2, pp. 87–107, 2017.

[8] R. J. La, "Interdependent security with strategic agents and cascades of infection," *IEEE/ACM Trans. on Networking (TON)*, vol. 24, no. 3, pp. 1378–1391, 2016.

[9] A. R. Hota, A. A. Clements, S. Bagchi, and S. Sundaram, "A game-theoretic framework for securing interdependent assets in networks," in *Game Theory for Security and Risk Management*, Springer, 2018, pp. 157–184.

[10] B. An, M. Tambe, and A. Sinha, "Stackelberg security games (ssg) basics and application overview," in *Improving Homeland Security Decisions*, Cambridge Univ. Press, 2016.

[11] G. Yan, R. Lee, A. Kent, and D. Wolpert, "Towards a bayesian network game framework for evaluating ddos attacks and defense," in *Proceedings of the 2012 ACM conference on Computer and communications security (CCS)*, 2012, pp. 553–566.

[12] A. R. Hota, A. A. Clements, S. Sundaram, and S. Bagchi, "Optimal and game-theoretic deployment of security investments in interdependent assets," in *International Conference on Decision and Game Theory for Security*, Springer, 2016, pp. 101–113.

[13] G. Modelo-Howard, S. Bagchi, and G. Lebanon, "Determining placement of intrusion detectors for a distributed application through bayesian network modeling," in *International Workshop on Recent Advances in Intrusion Detection*, Springer, 2008, pp. 271–290.

[14] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Econometrica: Journal of the econometric society*, pp. 263–291, 1979.

[15] R. Gonzalez and G. Wu, "On the shape of the probability weighting function," *Cognitive psychology*, vol. 38, no. 1, pp. 129–166, 1999.

[16] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proceedings 2002 IEEE Symposium on Security and Privacy*, IEEE, 2002, pp. 273–284.

[17] S. Jauhar, B. Chen, W. G. Temple, *et al.*, "Model-based cybersecurity assessment with NESCOR smart grid failure scenarios," in *IEEE 21st Pacific Rim International Symposium on Dependable Computing*, 2015, pp. 319–324.

[18] S. Mullainathan and R. H. Thaler, "Behavioral economics," National Bureau of Economic Research, Tech. Rep., 2000.

[19] I. Week, *IT Leadership: 3 Tips for Making Better Investments in Security*, https://www.informationweek.com/strategic-cio/3-tips-for-making-better-investments-in-security/a/d-id/13298802, [Online; accessed 21-October-2018], 2017.

[20] F. T. Council, *CISO Should Stand For Chief Influence Security Officer*, https://www.forbes.com/sites/forbestechcouncil/2018/09/24/ciso-should-stand-for-chief-influence-security-officer/, [Online; accessed 21-October-2018], 2018.

[21] CNBC, *Here's what cybersecurity professionals at companies actually do, and why they're so vital*, https://www.cnbc.com/2018/07/20/what-is-ciso-chief-information-security-officer.html, [Online; accessed 21-October-2018], 2018.

[22] D. Dor and Y. Elovici, "A model of the information security investment decision-making process," *Computers & security*, vol. 63, pp. 1–13, 2016.

[23] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Systems*, vol. 86, pp. 13–23, 2016.

[24] J. Homer, S. Zhang, X. Ou, *et al.*, "Aggregating vulnerability metrics in enterprise networks using attack graphs," *Journal of Computer Security*, vol. 21, no. 4, pp. 561–597, 2013.

[25] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[26] H. Cavusoglu, S. Raghunathan, and W. T. Yue, "Decision-theoretic and game-theoretic approaches to IT security investment," *Journal of Management Information Systems*, vol. 25, no. 2, pp. 281–304, 2008.

[27] C. D. Huang, Q. Hu, and R. S. Behara, "An economic analysis of the optimal information security investment in the case of a risk-averse firm," *International Journal of Production Economics*, vol. 114, no. 2, pp. 793–804, 2008.

[28] Y. Baryshnikov, "IT security investment and Gordon-Loeb's 1/e rule.," in *Workshop on Economics and Information Security (WEIS)*, 2012.

[29] S. Farrow, "The economics of homeland security expenditures: Foundational expected cost-effectiveness approaches," *Contemporary Economic Policy*, vol. 25, no. 1, pp. 14–26, 2007.

[30] R. Powell, "Allocating defensive resources with private information about vulnerability," *American Political Science Review*, vol. 101, no. 4, pp. 799–809, 2007.

[31] A. R. Hota and S. Sundaram, "Interdependent security games on networks under behavioral probability weighting," *IEEE Trans. on Control of Network Systems*, vol. 5, no. 1, pp. 262–273, 2018, ISSN: 2325-5870. DOI: 10.1109/TCNS.2016.2600484.

[32] M. Abdallah, P. Naghizadeh, A. R. Hota, T. Cason, S. Bagchi, and S. Sundaram, "The impacts of behavioral probability weighting on security investments in interdependent systems," in *2019 American Control Conference (ACC)*, 2019, pp. 5260–5265. DOI: 10.23919/ACC.2019.8814307.

[33] M. Abdallah, P. Naghizadeh, T. Cason, S. Bagchi, and S. Sundaram, "Protecting assets with heterogeneous valuations under behavioral probability weighting," in *2019 IEEE 58th Conference on Decision and Control (CDC)*, 2019, pp. 5374–5379.

[34] B. Roberson, "The colonel blotto game," *Economic Theory*, vol. 29, no. 1, pp. 1–24, 2006.

[35] G. Schwartz, P. Loiseau, and S. S. Sastry, "The heterogeneous colonel blotto game," in *2014 7th International Conference on NETwork Games, COntrol and OPtimization (NetGCoop)*, 2014, pp. 232–238.

[36] A. Sanjab, W. Saad, and T. Başar, "Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game," in *IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[37] M. Khanabadi, H. Ghasemi, and M. Doostizadeh, "Optimal transmission switching considering voltage security and n-1 contingency analysis," *IEEE Transactions on Power Systems*, vol. 28, no. 1, pp. 542–550, 2012.

[38] R. Lippmann, K. Ingols, C. Scott, *et al.*, "Validating and restoring defense in depth using attack graphs," in *IEEE Military Communications Conference*, IEEE, 2006, pp. 1–10.

[39] S. Sharma and D. Teneketzis, "A game-theoretic approach to decentralized optimal power allocation for cellular networks," *Telecommunication systems*, vol. 47, no. 1, pp. 65–80, 2011.

[40] D. C. Parkes, *Iterative combinatorial auctions: Achieving economic and computational efficiency*. University of Pennsylvania, PA, 2001.

[41] P. Naghizadeh and M. Liu, "Exit equilibrium: Towards understanding voluntary participation in security games," in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, IEEE, 2016, pp. 1–9.

[42] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[43] H. Zhang, F. Lou, Y. Fu, and Z. Tian, "A conditional probability computation method for vulnerability exploitation based on CVSS," in *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, 2017, pp. 238–241. DOI: 10.1109/DSC.2017.33.

[44] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Trans. on Smart Grid*, vol. 3, no. 4, pp. 1790–1799, 2012.

[45] M. Jain, D. Korzhyk, O. Vaněk, V. Conitzer, M. Pěchouček, and M. Tambe, "A double oracle algorithm for zero-sum security games on graphs," in *The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 1*, International Foundation for Autonomous Agents and Multiagent Systems, 2011, pp. 327–334.

[46] G. Brown, M. Carlyle, A. Abdul-Ghaffar, and J. Kline, "A defender-attacker optimization of port radar surveillance," *Naval Research Logistics (NRL)*, vol. 58, no. 3, pp. 223–235, 2011.

[47] D. Prelec, "The probability weighting function," *Econometrica*, pp. 497–527, 1998.

[48] M. Baddeley, "Information security: Lessons from behavioural economics," in *Workshop on the Economics of Information Security*, 2011.

[49] R. Anderson, "Security economics: A personal perspective," in *Proceedings of the 28th Annual Computer Security Applications Conference*, ACM, 2012, pp. 139–144.

[50] B. Schneier, "The psychology of security," in *International Conference on Cryptology in Africa*, Springer, 2008, pp. 50–79.

[51] R. A. Martin, "Managing vulnerabilities in networked systems," *Computer*, vol. 34, no. 11, pp. 32–38, 2001.

[52] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge University Press, 2004.

[53] D. B. West *et al.*, *Introduction to graph theory*. Prentice hall Upper Saddle River, 2001, vol. 2.

[54] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica*, pp. 520–534, 1965.

[55] T. Roughgarden, "The price of anarchy is independent of the network topology," *Journal of Computer and System Sciences*, vol. 67, no. 2, pp. 341–364, 2003.

[56] M. Grant and S. Boyd, *CVX: Matlab software for disciplined convex programming, version 2.1*, http://cvxr.com/cvx, Mar. 2014.

[57] T. Coleman, M. A. Branch, and A. Grace, "Optimization toolbox," *For Use with MATLAB. User's Guide for MATLAB 5, Version 2, Relaese II*, 1999.

[58] J. Sell and Y. Son, "Comparing public goods with common pool resources: Three experiments," *Social Psychology Quarterly*, pp. 118–137, 1997.

[59] M. B. Brewer and R. M. Kramer, "Choice behavior in social dilemmas: Effects of social identity, group size, and decision framing.," *Journal of personality and social psychology*, vol. 50, no. 3, p. 543, 1986.

[60] C. McCusker and P. J. Carnevale, "Framing in resource dilemmas: Loss aversion and the moderating effects of sanctions," *Organizational Behavior and Human Decision Processes*, vol. 61, no. 2, pp. 190–201, 1995.

[61] J. Apesteguia and F. P. Maier-Rigaud, "The role of rivalry: Public goods versus common-pool resources," *Journal of Conflict Resolution*, vol. 50, no. 5, pp. 646–663, 2006.

[62] M. W. McCarter, K. W. Rockmann, and G. B. Northcraft, "Is it even worth it? the effect of loss prospects in the outcome distribution of a public goods dilemma," *Organizational Behavior and Human Decision Processes*, vol. 111, no. 1, pp. 1–12, 2010.

[63] I. Iturbe-Ormaetxe, G. Ponti, J. Tomás, and L. Ubeda, "Framing effects in public goods: Prospect theory and experimental evidence," *Games and Economic Behavior*, vol. 72, no. 2, pp. 439–447, 2011.

[64] J. Shalev, "Loss aversion equilibrium," *International Journal of Game Theory*, vol. 29, no. 2, pp. 269–287, 2000.

[65] P. Leclerc, "Prospect theory preferences in noncooperative game theory," 2014.

[66] E. Baharad and S. Nitzan, "Contest efforts in light of behavioural considerations," *The Economic Journal*, vol. 118, no. 533, pp. 2047–2059, 2008.

[67] R. Cornes and R. Hartley, "Fully aggregative games," *Economics Letters*, vol. 116, no. 3, pp. 631–633, 2012.

[68] C. K. Butler, "Prospect theory and coercive bargaining," *Journal of Conflict Resolution*, vol. 51, no. 2, pp. 227–250, 2007.

[69] A. R. Hota, S. Garg, and S. Sundaram, "Fragility of the commons under prospect-theoretic risk attitudes," *Games and Economic Behavior*, vol. 98, pp. 135–164, 2016.

[70] M. Abdallah, T. Cason, S. Bagchi, and S. Sundaram, "The effect of behavioral probability weighting in a sequential defender-attacker game," in *2020 59th IEEE Conference on Decision and Control (CDC)*, 2020, pp. 3255–3260. DOI: 10.1109/CDC42340.2020.9304311.

[71] M. Abdallah, D. Woods, P. Naghizadeh, *et al.*, "Morshed: Guiding behavioral decision-makers towards better security investment in interdependent systems," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021, pp. 378–392.

[72] P. Naghizadeh and M. Liu, "Opting out of incentive mechanisms: A study of security as a non-excludable public good," *IEEE Trans. on Information Forensics and Security*, vol. 11, no. 12, pp. 2790–2803, 2016.

[73] R. M. Sheremeta, "Behavior in group contests: A review of experimental research," *Journal of Economic Surveys*, vol. 32, no. 3, pp. 683–704, 2018.

[74] J. P. Choi, S. M. Chowdhury, and J. Kim, "Group contests with internal conflict and power asymmetry," *The Scandinavian Journal of Economics*, vol. 118, no. 4, pp. 816–840, 2016.

[75] Y. D. Abbasi, M. Short, A. Sinha, N. Sintov, C. Zhang, and M. Tambe, "Human adversaries in opportunistic crime security games: Evaluating competing bounded rationality models," in *Proceedings of the third annual conference on advances in cognitive systems ACS*, 2015, p. 2.

[76] Y. Alarie and G. Dionne, "Lottery decisions and probability weighting function," *Journal of Risk and Uncertainty*, vol. 22, no. 1, pp. 21–33, 2001.

[77] 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 Transactions on Control of Network Systems*, vol. 7, no. 4, pp. 1585–1596, 2020. DOI: 10.1109/TCNS.2020.2988007.

[78] D. Woods, M. Abdallah, S. Bagchi, S. Sundaram, and T. Cason, "Network defense and behavioral biases: An experimental study," *Experimental Economics*, pp. 1–33, 2021.

[79] M. Abdellaoui, "Parameter-free elicitation of utility and probability weighting functions," *Management science*, vol. 46, no. 11, pp. 1497–1512, 2000.

[80] I. L. Glicksberg, "A further generalization of the kakutani fixed point theorem, with application to nash equilibrium points," *Proceedings of the American Mathematical Society*, vol. 3, no. 1, pp. 170–174, 1952.

[81] A. Acquisti, "Nudging privacy: The behavioral economics of personal information," *IEEE security & privacy*, vol. 7, no. 6, 2009.

[82] E. M. Redmiles, M. L. Mazurek, and J. P. Dickerson, "Dancing pigs or externalities?: Measuring the rationality of security decisions," in *Proceedings of the 2018 ACM Conference on Economics and Computation*, ACM, 2018, pp. 215–232.

[83] S. Benartzi and R. H. Thaler, "Naive diversification strategies in defined contribution saving plans," *American economic review*, vol. 91, no. 1, pp. 79–98, 2001.

[84] L. Haynes, B. Goldacre, D. Torgerson, *et al.*, "Test, learn, adapt: Developing public policy with randomised controlled trials," *Cabinet Office-Behavioural Insights Team*, 2012.

[85] G. R. Fréchette and A. Schotter, *Handbook of experimental economic methodology*. Oxford University Press, USA, 2015.

[86] K. Mersinas, B. Hartig, K. M. Martin, and A. Seltzer, "Experimental elicitation of risk behaviour amongst information security professionals.," in *14th Workshop on the Economics of Information Security (WEIS)*, 2015.

[87] K. Mersinas, B. Hartig, K. M. Martin, and A. Seltzer, "Are information security professionals expected value maximizers?: An experiment and survey based test," *Journal of Cybersecurity*, vol. 2, no. 1, pp. 57–70, Dec. 2016.

[88] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy, "Using Bayesian networks for cyber security analysis," in *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, IEEE, 2010, pp. 211–220.

[89] T. Alpcan and T. Basar, "An intrusion detection game with limited observations," in *12th Int. Symp. on Dynamic Games and Applications*, vol. 26, 2006.

[90] B. Wang and N. Z. Gong, "Attacking graph-based classification via manipulating the graph structure," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019, pp. 2023–2040.

[91] N. Feltovich, "Reinforcement-based vs. belief-based learning models in experimental asymmetric-information games," *Econometrica*, vol. 68, no. 3, pp. 605–641, 2000.

[92] M. Zhang, L. Wang, S. Jajodia, A. Singhal, and M. Albanese, "Network diversity: A security metric for evaluating the resilience of networks against zero-day attacks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 1071–1086, 2016.

[93] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*, IEEE, 2007, pp. 107–115.

[94] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, IEEE, 2010, pp. 1–10.

[95] L. F. Cranor, "A framework for reasoning about the human in the loop.," *Proc. 1st Conference on Usability, Psychology, and Security, Usenix Assoc.*, 2008.

[96] Z. Ni and S. Paul, "A multistage game in smart grid security: A reinforcement learning solution," *IEEE transactions on neural networks and learning systems*, vol. 30, no. 9, pp. 2684–2695, 2019.

[97] P. Morgner, C. Mai, N. Koschate-Fischer, F. Freiling, and Z. Benenson, "Security update labels: Establishing economic incentives for security patching of iot consumer products," in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2020, pp. 429–446.

[98] M. Abdallah, T. Cason, S. Bagchi, and S. Sundaram, "The effect of behavioral probability weighting in a simultaneous multi-target attacker-defender game," in *2021 European Control Conference (ECC)*, IEEE, 2021, pp. 933–938.

[99] A. Nadeem, S. Verwer, S. Moskal, and S. J. Yang, "Enabling visual analytics via alert-driven attack graphs," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '21, Virtual Event, Republic of Korea: Association for Computing Machinery, 2021, pp. 2420–2422, ISBN: 9781450384544. DOI: 10.1145/3460120.3485361. [Online]. Available: https://doi.org/10.1145/3460120.3485361.

[100] R. Freeman, S. M. Zahedi, V. Conitzer, and B. C. Lee, "Dynamic proportional sharing: A game-theoretic approach," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 2, no. 1, pp. 1–36, 2018.

[101] M. Abdallah, S. Mitra, S. Sundaram, and S. Bagchi, "Hioa-cps: Combining hybrid input-output automaton and game theory for security modeling of cyber-physical systems," in *2021 IEEE Security and Privacy Workshops (SPW)*, 2021, pp. 253–259. DOI: 10.1109/SPW53761.2021.00044.

[102] H. Varian, "System reliability and free riding," in *Economics of information security*, Springer, 2004, pp. 1–15.

[103] M. M. Khalili, X. Zhang, and M. Liu, "Contract design for purchasing private data using a biased differentially private algorithm," in *Proceedings of the 14th Workshop on the Economics of Networks, Systems and Computation*, 2019, pp. 1–6.

[104] S. Dambra, L. Bilge, and D. Balzarotti, "Sok: Cyber insurance–technical challenges and a system security roadmap," in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2020, pp. 1367–1383.

[105] M. Rasch, *California Proposal for Mandatory Cyber Insurance*, https://securityboulevard.com/2020/03/california-proposal-for-mandatory-cyber-insurance//, [Online; accessed 21-October-2021], 2020.

[106] L. Hurwicz, "Outcome functions yielding walrasian and lindahl allocations at nash equilibrium points," *The Review of Economic Studies*, vol. 46, no. 2, pp. 217–225, 1979.

[107] D. R. Kuhn, T. J. Walsh, and S. Fries, "Security considerations for voice over ip systems," *NIST special publication*, vol. 800, 2005.

[108] L. Mathevet, "Supermodular mechanism design," *Theoretical Economics*, vol. 5, no. 3, pp. 403–443, 2010.

[109] W. Conen and T. Sandholm, "Partial-revelation vcg mechanism for combinatorial auctions," in *AAAI/IAAI*, 2002, pp. 367–372.

[110] T. Groves and M. Loeb, "Incentives and public inputs," *Journal of Public economics*, vol. 4, no. 3, pp. 211–226, 1975.

[111] A. Wolitzky, "Mechanism design with maxmin agents: Theory and an application to bilateral trade," *Theoretical Economics*, vol. 11, no. 3, pp. 971–1004, 2016.

[112] S. Milani, W. Shen, K. S. Chan, *et al.*, "Harnessing the power of deception in attack graph-based security games," in *International Conference on Decision and Game Theory for Security*, Springer, 2020, pp. 147–167.

[113] K. Stouffer, "Guide to industrial control systems (ics) security," *NIST special publication*, vol. 800, no. 82, pp. 16–16, 2011.

[114] *gtraq Vulnerability Database*, https://www.securityfocus.com/, [Online; accessed 18-March-2020], 2008.

[115] M. Abdallah, D. Woods, P. Naghizadeh, *et al.*, "Tasharok: Using mechanism design for enhancing security resource allocation in interdependent systems," in *2022 2022 IEEE Symposium on Security and Privacy (SP) (SP)*, Los Alamitos, CA, USA: IEEE Computer Society, 2022, pp. 1535–1535. DOI: 10.1109/SP46214.2022.00106. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/SP46214.2022.00106.

[116] X. Sun, J. Dai, P. Liu, A. Singhal, and J. Yen, "Using bayesian networks for probabilistic identification of zero-day attack paths," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2506–2521, 2018.

[117] H. S. Lallie, K. Debattista, and J. Bal, "A review of attack graph and attack tree visual syntax in cyber security," *Computer Science Review*, vol. 35, p. 100 219, 2020.

[118] J. Green and J.-J. Laffont, *Incentives in public decision-making*. Elsevier North-Holland, 1979.

[119] E. Maskin, "The theory of implementation in nash equilibrium: A survey," *Cambridge, Mass.: Dept. of Economics, Massachusetts Institute of Technology*, 1983.

[120] K. Mersinas, B. Hartig, K. M. Martin, and A. Seltzer, "Are information security professionals expected value maximizers?: An experiment and survey-based test," *Journal of Cybersecurity*, vol. 2, no. 1, pp. 57–70, Dec. 2016, ISSN: 2057-2085. DOI: 10.1093/cybsec/tyw009. eprint: https://academic.oup.com/cybersecurity/article-pdf/2/1/57/10833200/tyw009.pdf. [Online]. Available: https://doi.org/10.1093/cybsec/tyw009.

[121] G. Kuper, F. Massacci, W. Shim, and J. Williams, "Who should pay for interdependent risk? policy implications for security interdependence among airports," *Risk Analysis*, vol. 40, no. 5, pp. 1001–1019, 2020.

[122] A. Zimba, Z. Wang, and H. Chen, "Reasoning crypto ransomware infection vectors with bayesian networks," in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, IEEE, 2017, pp. 149–151.

[123] A. Acquisti and J. Grossklags, "What can behavioral economics teach us about privacy," *Digital privacy: theory, technologies and practices*, vol. 18, pp. 363–377, 2007.

VITA

Mustafa Abdallah received the B.Sc. degree in Electrical and Electronics Engineering and the M.Sc. degree in Engineering Mathematics from the Faculty of Engineering, Cairo University, Egypt, in 2012 and 2016, respectively. He is currently a Ph.D. candidate in the Elmore Family School of Electrical and Computer Engineering with Purdue University, USA. His research interests include game theory, behavioral decision making, and deep learning, with applications including Cyber Security and Data Science applications. His current focus is to predict the effects of human decision-making bias in securing interdependent systems and to design practical learning algorithms to mitigate such effects. Mr. Abdallah has several industrial research experiences, including internships with Adobe Research, Principal, and part-time machine learning research experience with RDI (in Egypt).

Mr. Abdallah's research contribution is recognized by receiving the Purdue Bilsland Dissertation Fellowship and having several publications in top journals and conferences, including IEEE Transactions on Control of Network Systems, IEEE Symposium of Security and Privacy, ACM Asia Conference on Computer and Communications Security, and IEEE Internet of Things Journal. He also was the recipient of the Best Fresher and the Group Champ Awards of DCSL research lab in Fall 2017 and Fall 2020, respectively, and a M.Sc. Fellowship from the Faculty of Engineering, Cairo University, in 2013. He also received several travel grants for presenting his work in several IEEE conferences and workshops.

PUBLICATIONS

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," The 43rd IEEE Symposium on Security and Privacy (S&P 2022), 2022 (Acceptance rate: 57/407 = 14.0% (in 3rd reviewing cycle)).

M. Abdallah, T. Cason, S. Bagchi, and S. Sundaram, "The Effect of Behavioral Probability Weighting in a The Effect of Behavioral Probability Weighting in a Simultaneous Multi-Target Attacker-Defender Game," IEEE European Control Conference (ECC), 2021.

D. Woods, **M. Abdallah**, S. Bagchi, S. Sundaram, and T. Cason "Network Defense and Behavioral Biases: An Experimental Study," Experimental Economics Journal, Feb 2021.

M. Abdallah, S. Mitra, S. Sundaram, and S. Bagchi, "Combining Hybrid Input-Output Automaton and Game Theory for Security Modeling of Cyber-Physical Systems," IEEE Workshop on the Internet of Safe Things (Safe Things), 2021.

M. Abdallah, D. Woods, P. Naghizadeh, I. Khalil, T. Cason, S. Sundaram, S. Bagchi, "Morshed: Guiding Behavioral Decision-Makers towards Better Security Investment in Interdependent Systems", 16th ACM Asia Conference on Computer and Communications Security (ASIACCS), pp. 1–15, 2021 (Acc. rate: 28/157 = 17.8%).

M. Abdallah, P. Naghizadeh, A. Hota, T. Cason, S. Bagchi, and S. Sundaram, "Behavioral and Game-Theoretic Security Investments in Interdependent Systems Modeled by Attack Graphs," IEEE Transactions on Control of Network Systems (TCNS) (Impact Factor: 4.802), April 2020.

M. Abdallah, T. Cason, S. Bagchi, and S. Sundaram, "The Effect of Behavioral Probability Weighting in a Sequential Defender-Attacker Game," IEEE Conference on Decision and Control (CDC), 2020.

M. Abdallah, P. Naghizadeh, T. Cason, S. Bagchi, and S. Sundaram, "Protecting Assets with Heterogeneous Valuations under Behavioral Probability Weighting," IEEE Conference on Decision and Control (CDC), 2019.

M. Abdallah, P. Naghizadeh, A. Hota, T. Cason, S. Bagchi, and S. Sundaram, "The Impacts of Behavioral Probability Weighting on Security Investments in Interdependent Systems," American Control Conference (ACC), 2019.

Working Papers:

M. Abdallah, D. Woods, T. Cason, S. Bagchi, and S. Sundaram, "A Game-Theoretic Analysis to Protect Heterogeneous Common Pool Resources under Behavioral Probability Weighting," **Under preparation for submission as a Journal Paper at Games and Economic Behavior (GEB**), 2022.