2019 IEEE 58th Conference on Decision and Control (CDC)
Palais des Congrès et des Expositions Nice Acropolis
Nice, France, December 11-13, 2019

Protecting Assets with Heterogeneous Valuations under Behavioral Probability Weighting

Mustafa Abdallah, Parinaz Naghizadeh, Timothy Cason, Saurabh Bagchi, and Shreyas Sundaram.

***Abstract*— 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-$\grave{a}$-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.**

I. Introduction

Today's cyber-physical systems (CPS) are increasingly facing attacks by sophisticated adversaries. The operators of such CPS are typically responsible for managing and protecting multiple assets against such attacks, and are tasked with allocating their often limited security budget across these assets to best mitigate their vulnerabilities. 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 the defenders and attackers [8]–[10].

One of the seminal papers pertaining to strategic (or economic) decision-making in security is [11], 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], [12]–[14] and the references therein).

In these works, the defenders are modeled as fully rational decision-makers (perhaps with some measure of risk-aversion [13]) who choose their actions to maximize their expected utilities. However, a large body of work in behavioral economics and psychology has shown that humans consistently deviate from such classical models of decision-making. A seminal model capturing such deviations is *prospect theory* (introduced by Kahneman and Tversky in [15]), which shows that humans perceive gains, losses, and probabilities in a skewed (nonlinear) manner, typically overweighting low probabilities and underweighting high probabilities. While a large literature on prospect theory exists in economics and psychology, relatively little research has investigated such behavioral decision-making by defenders and/or attackers, and its effects on CPS security and robustness (exceptions include [16]–[18]).

In this paper, 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. Existing work on the study of behavioral decision-making in CPS has focused on the impact of probability weighting on defenders' investments in networks (with the emphasis being on understanding the role of the network structure) [16], [18]. In contrast to these works, we consider the effects of behavioral decision-making in a setting with multiple targets with heterogeneous values to the defender.

We first establish the convexity of the objective function of the defender in this setting, even under nonlinear probability weighting (subject to appropriate conditions on the probability of successful attack on the nodes). We then characterize the optimal investments in the assets. Interestingly, 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. We provide numerical examples to illustrate our theoretical findings.

This research was supported by grant CNS-1718637 from the National Science Foundation. Mustafa Abdallah, Parinaz Naghizadeh, Saurabh Bagchi, and Shreyas Sundaram are with the School of Electrical and Computer Engineering at Purdue University. Email: {abdalla0,parinaz,sbagchi,sundara2}@purdue.edu. Timothy Cason is with the Krannert School of Management at Purdue University. Email: cason@purdue.edu.

978-1-7281-1398-2/19/$31.00 ©2019 IEEE

II. The Multi-Target Security Problem

A. 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

$$X \triangleq \{\mathbf{x} \in \mathbb{R}^n_{\geq 0} : \sum_{v_i \in V} x_i \leq B\}. \tag{1}$$

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 $\mathbf{x} \in X$.

B. 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 $v_i \in V$, let $p_i : \mathbb{R}_{\geq 0} \to [0, 1]$ 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

$$\overline{C}_D(\mathbf{x}) = \sum_{v_i \in V} L_i p_i(x_i) \tag{2}$$

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], [11]–[13]. 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 review certain classes of probability weighting functions that capture this phenomenon, and subsequently introduce such functions into the above multi-target security formulation.

III. The Behavioral Multi-Target Security Problem

A. Nonlinear Probability Weighting

The behavioral economics and psychology literature has shown that humans consistently misperceive probabilities by overweighting low probabilities and underweighting high probabilities [15], [19]. 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 [19], and is given by

$$w(p) = \exp\Big[-(-\log(p))^\alpha\Big], \quad p \in [0, 1], \tag{3}$$

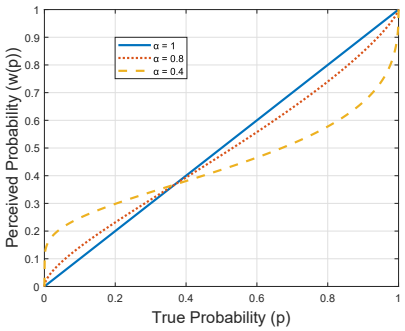

Fig. 1: Prelec probability weighting function which transforms true probabilities p into perceived probabilities $w(p)$. The parameter α controls the extent of overweighting and underweighting.

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. 1.

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.

B. The Multi-Target Behavioral Security Problem

Definition 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 (3). Specifically, the perceived attack probability on an asset $v_i \in V$ is given by:

$$w(p_i(x_i)) = \exp\Big[-(-\log(p_i(x_i)))^\alpha\Big], \tag{4}$$

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:

$$\underset{\mathbf{x} \in X}{\text{minimize}} \quad C_D(\mathbf{x}) = \sum_{i=1}^{n} L_i w(p_i(x_i)), \tag{5}$$

where the strategy space X is defined in (1).

The nonlinear (and nonconvex) nature of the probability weighting function (as shown in Fig. 1) leads to a complicated form for the utility function in (5). 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.

IV. 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 III. 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 1: 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 $x_i < \infty$.
- $p_i(x_i)$ is strictly decreasing and log-convex[1] in x_i.
- $\frac{p_i'(x_i)}{p_i(x_i)}$ is bounded in $x_i \in \mathbb{R}_{\geq 0}$.

□

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 1; two examples are

$$p_i(x_i) = \exp(-x_i - a_i),\ p_i(x_i) = \frac{1}{x_i + a_i},$$

where $a_i \in \mathbb{R}_{>0}$ ($a_i \in \mathbb{R}_{\geq 1}$ 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 1: Under Assumption 1, for every asset $v_i \in V$, the perceived probability of attack $w(p_i(x_i))$ is strictly convex in the defense investment x_i. Thus, the Multi-Target Behavioral Security Problem (5) is strictly convex.

The proof directly follows by calculating the second derivative of $w(p_i(x_i))$ and using Assumption 1.

V. Properties of the Optimal Investment Decisions

Proposition 1 showed that the optimization problem (5) is convex as long as each node's probability of successful attack satisfies Assumption 1. 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 paper.

Assumption 2: 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 1. □

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).

A. 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 (5).

[1]This is a common assumption in the literature. In particular, [14] 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 [11] to hold.

Lemma 1: Under Assumption 2, the marginal $L_i \frac{\partial w(p_i(x))}{\partial x}$ is negative, continuous, and increasing to 0 in x for all $i \in \{1, 2, \ldots, n\}$. Furthermore, for each pair of nodes v_i, v_j with $i < j$, the marginals satisfy

$$L_i \frac{\partial w(p_i(x))}{\partial x} < L_j \frac{\partial w(p_j(x))}{\partial x} \tag{6}$$

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

Proof: The perceived expected loss at node v_i is given by $L_i w(p_i(x_i))$. Differentiating (4) with respect to the defender's investment in that node, we obtain

$$L_i \tfrac{\partial w(p_i(x))}{\partial x} = \alpha L_i (-\log(p_i(x)))^{\alpha-1} w(p_i(x)) \frac{p_i'(x)}{p_i(x)}. \tag{7}$$

This function is negative (since $p_i'(x)$ is negative and $-\log(p_i(x))$ is positive). Furthermore it is continuous, and increasing in x ($w(p_i(x))$ is strictly convex as shown in Proposition 1, and thus we have $\frac{\partial}{\partial x}(\frac{\partial w(p_i(x))}{\partial x}) > 0$). To show that the marginal goes to zero as $x \to \infty$, we note that

$$\lim_{x\to\infty} \left| L_i \frac{\partial w(p_i(x))}{\partial x} \right| = \lim_{x\to\infty} \left| \alpha L_i (-\log(p_i(x)))^{\alpha-1} w(p_i(x)) \right| \left| \frac{p_i'(x)}{p_i(x)} \right| = 0,$$

since $p_i(x) \to 0$ as $x \to \infty$ (which means $w(p_i(x)) \to 0$ and $-\log(p_i(x)) \to \infty$), and $\frac{p_i'(x)}{p_i(x)}$ is bounded by Assumption 1. This proves the first part of the result. For the second part, note that if $L_j < L_i$ and $p_i(x) = p_j(x) = p(x)$ under Assumption 2, we obtain

$$L_i (-\log(p(x)))^{\alpha-1} w(p(x)) \frac{p'(x)}{p(x)} < L_j (-\log(p(x)))^{\alpha-1} w(p(x)) \frac{p'(x)}{p(x)},$$

for all $x \in \mathbb{R}_{\geq 0}$. Multiplying both sides by α to obtain the marginals, we have the ordering given by (6). ■

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 2: Consider a defender $\mathcal{D}$ and a set of n assets satisfying Assumption 2. Then, the optimal defense allocation of (5), denoted $\mathbf{x}^* = \begin{bmatrix} x_1^* & x_2^* & \ldots & x_n^* \end{bmatrix}^\intercal$, 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 $L_i \frac{\partial(w(p_i(x_i)))}{\partial x_i}|_{x_i = x_i^*} = L_j \frac{\partial(w(p_j(x_j)))}{\partial x_j}|_{x_j = x_j^*}$.

If the probability of successful attack on the asset v_i satisfies Assumption 1, the perceived probability of successful attack on v_i would be given by (4).

Under Assumption 2, the above marginals under the defender's optimal investments would satisfy

$$L_i(-\log(p(x_i^*)))^{\alpha-1}w(p(x_i^*))\frac{p'(x_i^*)}{p(x_i^*)} = L_j(-\log\big(p(x_j^*)\big))^{\alpha-1}w(p(x_j^*))\frac{p'(x_j^*)}{p(x_j^*)} \quad (8)$$

for all nodes v_i, v_j with nonzero optimal investments x_i^* and x_j^*, respectively. Using (8) and assuming without loss of generality that $i < j$, we obtain

$$\begin{aligned}(-\log(p(x_i^*)))^{\alpha-1}w(p(x_i^*))\frac{p'(x_i^*)}{p(x_i^*)} &= \frac{L_j}{L_i}(-\log\big(p(x_j^*)\big))^{\alpha-1}w(p(x_j^*))\frac{p'(x_j^*)}{p(x_j^*)} \\ &\geq (-\log\big(p(x_j^*)\big))^{\alpha-1}w(p(x_j^*))\frac{p'(x_j^*)}{p(x_j^*)}\end{aligned}$$

since $L_i \geq L_j$ and all of the above expressions are negative. As the marginals are increasing in x (by Lemma 1), the above expression implies $x_i^* \geq x_j^*$. This concludes the proof. ■

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

B. Water-Filling Nature of Investments

To gain further insights into the optimal investments, we can leverage Lemma 1 to introduce the following quantities.

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

$$L_i \frac{\partial w(p_i(x))}{\partial x}\bigg|_{x=x_{ij}^*} = L_j \frac{\partial w(p_j(x))}{\partial x}\bigg|_{x=0}. \quad (9)$$

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

Note that by Lemma 1, the quantity x_{ij}^* exists and is unique for each $i < j$ (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: Under Assumption 2, node v_j will have a nonzero optimal investment x_j^* if and only if the defense budget satisfies $B > \sum_{i=1}^{j-1} x_{ij}^*$.

Proof: First suppose that v_j has a nonzero optimal investment x_j^*, and suppose by way of contradiction that $B \leq \sum_{i=1}^{j-1} x_{ij}^*$. Then, $\exists i \in \{1, \ldots, j-1\}$ such that $x_i^* < x_{ij}^*$ (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 2, and using Lemma 1, we have

$$\begin{aligned}L_i \frac{\partial(w(p_i(x_i)))}{\partial x_i}|_{x_i=x_i^*} &< L_j \frac{\partial(w(p_j(x_j)))}{\partial x_j}|_{x_j=0} \\ &< L_j \frac{\partial(w(p_j(x_j)))}{\partial x_j}|_{x_j=x_j^*}\end{aligned}$$

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

To prove the other direction, suppose that $B > \sum_{i=1}^{j-1} x_{ij}^*$. Suppose by way of contradiction that $x_j^* = 0$. Then, we have $x_k^* = 0 \ \forall k > j$ (from Proposition 2). Thus, we have $x_1^* + x_2^* + \cdots + x_{j-1}^* = B$ and $\exists i \in \{1, \ldots, j-1\}$ s.t. $x_i^* > x_{ij}^*$. 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 (5), thereby contradicting the optimality of these investments.

Starting with the given nonzero investments on the assets $\{v_1, \ldots, v_{j-1}\}$, the perceived cost in (5) will be:

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

From the asset v_i that had $x_i^* > x_{ij}^*$, 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 (5) under this investment vector will be

$$C_D(\bar{\mathbf{x}}) = \sum_{k \notin \{i,j\}} L_k w(p_k(x_k^*)) + L_i w(p_i(x_i^* - \epsilon)) + L_j w(p_j(\epsilon)).$$

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

$$f(\epsilon) = L_i w(p_i(x_i^* - \epsilon)) + L_j w(p_j(\epsilon)),$$

and note that

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

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

$$\frac{df}{d\epsilon} = -L_i \frac{\partial w(p_i(x))}{\partial x}\bigg|_{x=x_i^*-\epsilon} + L_j \frac{\partial w(p_j(x))}{\partial x}\bigg|_{x=\epsilon}.$$

Since $x_i^* > x_{ij}^*$, we have (from Lemma 1 and the definition of x_{ij}^*)

$$L_i \frac{\partial w(p_i(x))}{\partial x}\bigg|_{x=x_i^*} > L_j \frac{\partial w(p_j(x))}{\partial x}\bigg|_{x=0}.$$

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.

C. 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 (3). In particular, smaller values of α correspond to a larger amount of overweighting and underweighting (see Fig. 1). We now study the impact of probability weighting on the investments (i.e., how the investments change as α changes).

Lemma 2: Suppose Assumption 2 holds, and furthermore that $p(0) \leq \frac{1}{e}$. Then, $\forall i \in \{1,\ldots,n\}$ and $j \in \{1,\ldots,n\}$ with $i<j$, the quantity $x^*_{ij}(\alpha)$ is decreasing in α.

Proof: From Definition 2, the value of $x^*_{ij}(\alpha)$ is given by (9) for all $i<j$. Using the expression for the marginals given by (7), and noting that $p_i(x) = p_j(x) = p(x)$ from Assumption 2, $x^*_{ij}(\alpha)$ satisfies the equation

$$L_i(-\log\big(p(x^*_{ij}(\alpha))\big))^{\alpha-1} w(p(x^*_{ij}(\alpha)))\frac{p'(x^*_{ij}(\alpha))}{p(x^*_{ij}(\alpha))} = L_j(-\log(p(0)))^{\alpha-1} w(p(0))\frac{p'(0)}{p(0)}. \quad (10)$$

In (10), taking the logarithm of both sides and differentiating yields that $\frac{dx^*_{ij}}{d\alpha}$ is given by:

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

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 1, 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 1 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 4: Suppose Assumption 2 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 2. From Lemma 2 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, we have

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

Thus, by Lemma 1, 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.

VI. Numerical Simulations

A. 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

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

where x is the investment on that asset. The above function satisfies the conditions in Assumption 1. The optimal investments in the following scenarios were calculated using Matlab Optimization toolbox [20]. Fig. 2 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 2, 3, and 4 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 $\alpha = 0.6$) 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.

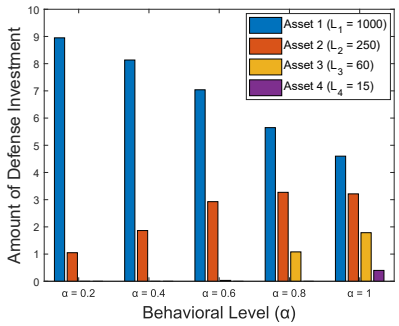

Fig. 2: Effect of behavioral probability weighting on the defense investments on four assets. The asset with the highest loss takes a higher portion of the defense investments as the defender becomes more behavioral (i.e., α decreases). Moreover, the number of assets with positive investment decreases as the defender becomes more behavioral.

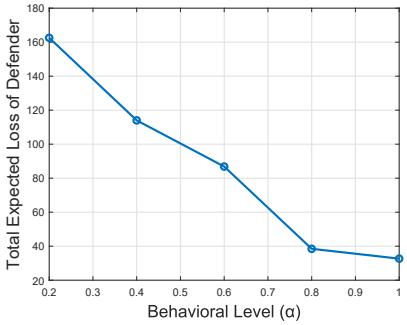

Fig. 3: Effect of behavioral probability weighting on the true expected loss of the defender. The true expected loss of the defender is higher as the defender becomes more behavioral. In particular, the true expected loss of a highly behavioral defender (with $\alpha = 0.4$) is approximately 3.5 times that for the non-behavioral defender (with $\alpha = 1$).

B. 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, 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.

VII. Conclusion

This paper 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.

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 Transactions 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] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[12] 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.

[13] 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.

[14] Y. Baryshnikov, "IT security investment and Gordon-Loeb's 1/e rule." in *Workshop on Economics and Information Security (WEIS)*, 2012.

[15] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Econometrica: Journal of the econometric society*, pp. 263–291, 1979.

[16] A. R. Hota and S. Sundaram, "Interdependent security games on networks under behavioral probability weighting," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 262–273, 2018.

[17] 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.

[18] 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)*, July 2019, pp. 5260–5265.

[19] D. Prelec, "The probability weighting function," *Econometrica*, pp. 497–527, 1998.

[20] T. Coleman, M. A. Branch, and A. Grace, "Optimization toolbox," *For Use with MATLAB. Users Guide for MATLAB 5, Version 2, Relaese II*, 1999.