2021 European Control Conference (ECC)
June 29 - July 2, 2021. Rotterdam, Netherlands

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

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

Abstract— **We consider a 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).**

I. Introduction

Today's cyber-physical systems (CPS) are increasingly facing attacks by sophisticated adversaries, who are able to evaluate the susceptibility of different goal targets in the system and strategically allocate their efforts to compromise the security of the CPS [1], [2]. In response to such intelligent adversaries, the operators (or defenders) of CPS need to allocate their (limited) security budget across many assets to best mitigate their vulnerabilities. This motivates the need to capture such interactions between attackers and defenders and study their effects on system security. In this context, significant research has been conducted for understanding how to better secure these systems, with game-theoretical models receiving increasing attention due to their power in capturing the interactions of players (strategic attackers and defenders) in different settings [3]–[6].

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 [7] 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, [8] 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 [5].

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. However, a seminal model called *prospect theory* (introduced by Kahneman and Tversky in [9]) offers a descriptive theory of how people actually make decisions showing 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, relatively little research has investigated such behavioral decision-making by defenders and/or attackers, and its effects on CPS security (exceptions include [10]–[13]). These exceptions have focused on the impact of probability weighting on a single defender's decisions via decision-theoretic analysis (with no strategic attacker) [10], on multiple defenders' investments in networks (with the emphasis being on understanding the role of the network structure) [11], [13], or on behavioral decision-making by both players for settings with a single target [12]. In contrast to these works, we consider the effects of behavioral decision-making in a setting with multiple targets with different values to players, i.e., the defender and the attacker.

In this paper, 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.

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

II. The Multi-Target Security Game Framework

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

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 $B \in \mathbb{R}_{\geq 0}$. Thus, we define the defense strategy space of the defender by

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

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 $\mathbf{x} \in X$.

B. Strategic Attacker

Let $\mathcal{A}$ be an attacker who is attempting to compromise the set V of assets.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

$$Y \triangleq \{\mathbf{y} \in \mathbb{R}^n_{\geq 0} : \sum_{v_i \in V} y_i \leq P\}. \tag{2}$$

We denote the attacker's investment vector by $\mathbf{y} \in Y$.

C. 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 $p_i : \mathbb{R}^2_{\geq 0} \to [0, 1]$ 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

$$\overline{C}_{\mathcal{D}}(\mathbf{x}, \mathbf{y}) = \sum_{v_i \in V} L_i \; p_i(x_i, y_i) \tag{3}$$

subject to $\mathbf{x} \in X$. 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

$$\overline{U}_{\mathcal{A}}(\mathbf{x}, \mathbf{y}) = \sum_{v_i \in V} G_i \; p_i(x_i, y_i) \tag{4}$$

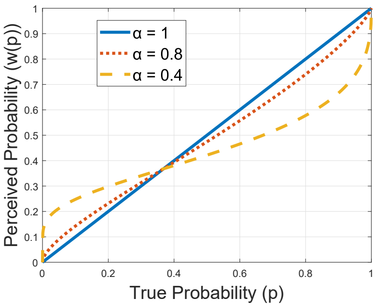

Fig. 1: Prelec Probability weighting function which transforms true probabilities p into perceived probabilities $w(p)$. The parameter α controls the extent of overweighting and underweighting.

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 [5] studies this setting and provides a method to calculate the optimal investments (with respect to the cost (3) and utility (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.

III. 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 $\mathcal{A}$.

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 [9], [14]. 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 [14], and is given by

$$w(p) = \exp\Big[-(-\log(p))^{\alpha}\Big], \quad p \in [0, 1], \tag{5}$$

where $\alpha \in (0, 1]$ 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 (i.e., rational defender). 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, 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.

B. Behavioral Multi-Target Security Game Formulation

Definition 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 (5). Specifically, the perceived attack probability on an asset $v_i \in V$ by player $k \in \{\mathcal{A}, \mathcal{D}\}$ is given by:

$$w_k(p_i(x_i, y_i)) = \exp\Big[-(-\log(p_i(x_i, y_i)))^{\alpha_k}\Big],$$

where $p_i(x_i, y_i) \in [0, 1]$, $\alpha_k \in (0, 1]$.
Now, we present the optimization problem perceived by the behavioral defender and the behavioral attacker, respectively.

1) Defender Cost Function Minimization Problem:

$$\underset{\mathbf{x} \in X}{\text{minimize}} \quad C_{\mathcal{D}}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} L_i \;\, w_{\mathcal{D}}(p_i(x_i, y_i)). \tag{6}$$

2) Attacker Utility Function Maximization Problem:

$$\underset{\mathbf{y} \in Y}{\text{maximize}} \quad U_{\mathcal{A}}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} G_i \;\, w_{\mathcal{A}}(p_i(x_i, y_i)). \tag{7}$$

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 (8) and (9) below are satisfied simultaneously:

$$\mathbf{x}^* \in \underset{\mathbf{x} \in X}{\text{argmin}} \;\, C_{\mathcal{D}}(\mathbf{x}, \mathbf{y}^*) \tag{8}$$

$$\mathbf{y}^* \in \underset{\mathbf{y} \in Y}{\text{argmax}} \;\, U_{\mathcal{A}}(\mathbf{x}^*, \mathbf{y}). \tag{9}$$

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 paper (e.g., as considered in [5] and the literature on Colonel Blotto games [7]), and leave a similar investigation of sequential games for future work.[1]

IV. Existence of Pure Strategy Nash Equilibrium

We now prove the existence of a PNE for the Behavioral Multi-Target Security Game. Throughout, let the function $p_i(x_i, y_i)$ represent the true probability of successful attack on an asset $v_i \in V$ when the total defense and attack investments on that asset are x_i and y_i, respectively. We make the following assumption on $p_i(x_i, y_i)$.

Assumption 1: 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 [5], [10].

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

$$p_i(x_i, y_i) = \exp(-x_i - a_i)(1 - \exp(-y_i)), \tag{10}$$

where $a_i \in \mathbb{R}_{\geq 0}$ in (10) 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 [16], [17], and satisfy the conditions in Assumption 1.

Lemma 1: 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 1.

Lemma 2: Under Assumption 1, if $p_i(x_i, y_i) \in [0, \frac{1}{e}) \forall x_i, y_i \in \mathbb{R}_{\geq 0}$, then

i) The perceived probability $w(p_i(x_i, y_i))$ will be concave in the attack investment y_i.
ii) The partial derivative $\dfrac{\partial^2 w(p(x_i, y_i))}{\partial x_i \partial y_i}$ is negative.

The proof of Lemmas 1 and 2 follow by using the second partial derivative formula and Assumption 1, and can be found on the extended version of this paper [18].

Note that for attack success probabilities given by (10), the condition $p_i(x_i, y_i) \in [0, \frac{1}{e})$ is guaranteed when the inherent defenses of the asset (given by parameter a_i) satisfy $a_i \geq 1$.

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

Theorem 1: Under Assumption 1, if $p_i(x_i, y_i) \in [0, \frac{1}{e}) \forall x_i, y_i \in \mathbb{R}_{\geq 0}$, a PNE exists in the Behavioral Multi-Target Security Game.

Proof: From (1) and (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)) and $U_{\mathcal{A}}(\mathbf{x}, \mathbf{y})$ (in (7)) be $H_{\mathcal{D}}$ and $H_{\mathcal{A}}$, respectively. Both $H_{\mathcal{D}}$ and $H_{\mathcal{A}}$ are diagonal by definition since $p_i(x_i, y_i)$ for each asset only depends on x_i and y_i. Moreover, from Lemma 1, 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 2 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 [19]. ■

[1] The recent work [15] studied such sequential game, however with only two assets. Studying the general case with many assets would be of interest.

[2] This is a common assumption in the literature [16], [17].

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.

V. Properties of the Optimal Investment Decisions

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

A. Uniqueness of PNE

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

Theorem 2: 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 1, if $p_i(x_i, y_i) \in [0, \frac{1}{e}) \forall x_i, y_i \in \mathbb{R}_{\geq 0}$, 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 [19] 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:

$$\sigma(\mathbf{x}, \mathbf{y}, \mathbf{r}) = \sum_{i=1}^{2} r_i \ \phi_i(\mathbf{x}, \mathbf{y})$$
$$= -r_1 \sum_{i=1}^{n} L_i \ w_{\mathcal{D}}(p_i(x_i, y_i)) + r_2 \sum_{i=1}^{n} G_i \ w_{\mathcal{A}}(p_i(x_i, y_i)).$$

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 $g(\mathbf{x}, \mathbf{y}, \mathbf{r})$ [19].

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 $\mathbf{u} = \begin{bmatrix} u_1 & u_2 & \ldots & u_{2n} \end{bmatrix}^\mathsf{T}$ as follows:

$$\begin{aligned} \mathbf{u}^T M(\mathbf{x}, \mathbf{y}, \mathbf{r}) \mathbf{u} &= -2r_1 \left(\sum_{i=1}^{n} u_i^2 L_i \frac{\partial^2 w_{\mathcal{D}}(p(x_i, y_i))}{\partial x_i^2} \right) \\ &+ 2r_2 \left(\sum_{i=1}^{n} u_{n+i}^2 G_i \frac{\partial^2 w_{\mathcal{A}}(p(x_i, y_i))}{\partial y_i^2} \right) \\ &+ 2 \sum_{i=1}^{n} u_i u_{n+i} \left(-r_1 L_i \frac{\partial^2 w_{\mathcal{D}}(p(x_i, y_i))}{\partial x_i \partial y_i} \right. \\ &\left. + r_2 G_i \frac{\partial^2 w_{\mathcal{A}}(p(x_i, y_i))}{\partial y_i \partial x_i} \right). \end{aligned} \quad (11)$$

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

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

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

where (x_i^*, y_i^*) denote the investments on asset v_i with minimum $\frac{\partial^2 w_{\mathcal{D}}(p(x_i, y_i))}{\partial x_i \partial y_i}$ across the n assets and $(\bar{x}_i, \bar{y}_i)$ denote the investments on asset v_i with maximum $\frac{\partial^2 w_{\mathcal{A}}(p(x_i, y_i))}{\partial y_i \partial x_i}$ across the n assets. Note that this choice minimizes r_1 by choosing the maximum possible value of its denominator since $\frac{\partial^2 w_{\mathcal{D}}(p(x_i, y_i))}{\partial x_i \partial y_i} < 0$. Similarly, this choice maximizes r_2 by choosing the minimum possible value of its denominator since $\frac{\partial^2 w_{\mathcal{A}}(p(x_i, y_i))}{\partial y_i \partial x_i} < 0$. 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 [19], 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. ■

B. 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 1: Consider a defender $\mathcal{D}$. Let the true probability of successful attack on each asset be given by (10). 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), denoted $\mathbf{x}^*(\alpha_{\mathcal{D}}) = \begin{bmatrix} x_1^*(\alpha_{\mathcal{D}}) & x_2^*(\alpha_{\mathcal{D}}) & \ldots & x_n^*(\alpha_{\mathcal{D}}) \end{bmatrix}^{\mathsf{T}}$, has the property that $x_1^*(\alpha_{\mathcal{D}}) \geq x_2^*(\alpha_{\mathcal{D}}) \geq \cdots \geq x_n^*(\alpha_{\mathcal{D}})$.

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 invested more on those assets) under certain conditions, namely when there are significant differences in the values of the assets to the attacker.

Proposition 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 (10). 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 $\frac{G_i}{G_j} \geq \frac{L_i}{L_j}$ $\forall i < j$. 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 $y_i^* = y_j^* + \log\left(\frac{G_i}{G_j}\right) - \log\left(\frac{L_i}{L_j}\right) \forall i, j \in \{1, \ldots, k_{\mathcal{A}}\}$ 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 $P - \log\left(\frac{\prod_{i=1}^k G_i}{G_k^k}\right) + \log\left(\frac{\prod_{i=1}^k L_i}{L_k^k}\right) > 0$.

ii) The defender's investment at the PNE is given by $x_i^* = x_j^* + \log\left(\frac{L_i}{L_j}\right) \forall i, j \in \{1, \ldots, k_{\mathcal{D}}\}$ 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 $B - \log\left(\frac{\prod_{i=1}^k L_i}{L_k^k}\right) > 0$.

The proofs of Propositions 1 and 2 can be found in the extended version of this paper [18].

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., $\frac{G_i}{G_j} = \frac{L_i}{L_j} \forall i < j$). 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 VI.

VI. Numerical Simulations

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

A. 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

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

where x and y are the defense and attack investment on that asset, respectively. The above function satisfies the conditions in Assumption 1. 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.

B. 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 1). Fig. 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. 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 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 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.

C. 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. We consider different loss

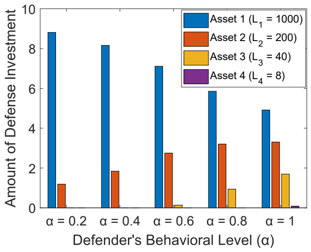

Fig. 2: Effect of behavioral probability weighting on the defense investments. The asset with the highest financial loss takes higher portion of the defense investments as the defender becomes more behavioral (i.e., α decreases) while the attacker is non-behavioral.

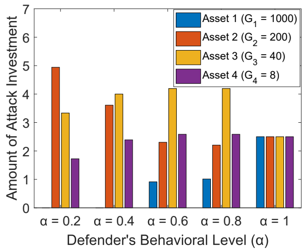

Fig. 3: Effect of defender's behavioral probability weighting on the attack investments. The asset with the highest financial gain takes much lower portion of the attack investments as the defender becomes more behavioral while the attacker is non-behavioral.

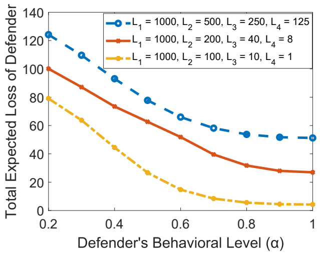

Fig. 4: Effect of behavioral probability weighting on the true expected loss of the defender for different loss values for the assets. The cost of the defender is worse if the defender becomes more behavioral while the attacker is non-behavioral.

valuations scenarios (including our previously considered loss valuations). Fig. 4 shows that when the defender is non-behavioral $E_T = 26.96$, 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 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.

VII. Conclusion

This paper 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, validating our findings via human subject experiments (similar to [20] on attack graphs) would be another avenue for future research.

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] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[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] 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.

[6] B. An, M. Tambe, and A. Sinha, "Stackelberg security games (ssg) basics and application overview," in *Improving Homeland Security Decisions*. Cambridge Univ. Press, 2016.

[7] B. Roberson, "The colonel blotto game," *Economic Theory*, vol. 29, no. 1, pp. 1–24, 2006.

[8] G. Schwartz, P. Loiseau, and S. S. Sastry, "The heterogeneous colonel blotto game," in *2014 7th International Conference on NETwork Games, COntrol and OPtimization*, Oct 2014, pp. 232–238.

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

[10] 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.

[11] 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.

[12] A. Sanjab, W. Saad, and T. Başar, "Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game," in *Communications (ICC), 2017 IEEE International Conference on*. IEEE, 2017, pp. 1–6.

[13] 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)*. IEEE, 2019, pp. 5260–5265.

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

[15] 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.

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

[17] 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.

[18] M. Abdallah, T. Cason, S. Bagchi, and S. Sundaram, "The effect of behavioral probability weighting in a simultaneous multi-target attacker-defender game," *arXiv preprint arXiv:2103.03392*, 2021.

[19] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica: Journal of the Econometric Society*, pp. 520–534, 1965.

[20] D. Woods, M. Abdallah, S. Bagchi, S. Sundaram, and T. Cason, "Network defense and behavioral biases: An experimental study," 2020.