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

Mustafa Abdallah, Parinaz Naghizadeh, *Member, IEEE*, Ashish R. Hota, Timothy Cason, Saurabh Bagchi, and Shreyas Sundaram

***Abstract*—In this article, 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 certain features of human decision making that have been identified in behavioral economics. In particular, humans have been shown to perceive probabilities in a nonlinear manner, typically overweighting low probabilities and underweighting high probabilities. We show that suboptimal investments can arise under such weighting in certain network topologies. We also show that pure strategy Nash equilibria exist in settings with multiple (behavioral) defenders, and study the inefficiency of the equilibrium investments by behavioral defenders compared to a centralized socially optimal solution.**

***Index Terms*—Cyber-physical systems (CPS), game theory, human decision making, network security, prospect theory.**

Manuscript received January 12, 2020; revised March 10, 2020; accepted March 24, 2020. Date of publication April 16, 2020; date of current version December 16, 2020. This paper was presented in part at the Proceedings of the American Control Conference 2019. Recommended by Associate Editor L. Bushnell. This work was supported by the National Science Foundation under Grant CNS-1718637. *(Corresponding author: Shreyas Sundaram.)*

Mustafa Abdallah, Saurabh Bagchi, and Shreyas Sundaram are with the School of Electrical and Computer Engineering at Purdue University, West Lafayette, IN 47907 USA (e-mail: abdalla0@purdue.edu; sbagchi@purdue.edu; sundara2@purdue.edu).

Parinaz Naghizadeh is with the Integrated Systems Engineering Department and the Electrical and Computer Engineering Department, Ohio State University, Columbus, OH 43210 USA (e-mail: naghizadeh.1@osu.edu).

Ashish R. Hota is with the Department of Electrical Engineering, Indian Institute of Technology (IIT) Kharagpur, Kharagpur 721302, India (e-mail: ashish1789hota@gmail.com).

Timothy Cason is with the Krannert School of Management at Purdue University, West Lafayette, IN 47907 USA (e-mail: cason@purdue.edu).

Digital Object Identifier 10.1109/TCNS.2020.2988007

I. Introduction

Modern cyber-physical systems (CPS) are increasingly facing attacks by sophisticated adversaries. These attackers are able to identify the susceptibility of different targets in the system and strategically allocate their efforts to compromise the security of the network. In response to such intelligent adversaries, the operators (or defenders) of these systems also need to allocate their often limited security budget across many assets to best mitigate their vulnerabilities. This has led to significant research in understanding how to better secure these systems, with game-theoretical models receiving increasing attention due to their ability to systematically capture the interactions of strategic attackers and defenders [1]–[8].

In the context of large-scale interdependent systems, adversaries often use stepping-stone attacks to exploit vulnerabilities within the network in order to compromise a particular target [9]. Such threats can be captured via the notion of *attack graphs* that represent all possible paths that attackers may have to reach their targets within the CPS [10]. The defenders in such systems are each responsible for defending some subset of the assets [2], [11] with their limited resources. These settings have been explored under various assumptions on the defenders and attackers [11]–[13].

In much of the existing literature, the defenders and attackers are modeled as fully rational decision makers who choose their actions to maximize their expected utilities. However, a large body of work in behavioral economics has shown that humans consistently deviate from such classical models of decision making [14]–[16]. A seminal model capturing such deviations is *prospect theory* (introduced by Kahneman and Tversky in [14]), which shows that humans perceive gains, losses, and probabilities in a skewed (nonlinear) manner, typically overweighting low probabilities and underweighting high probabilities. Recent papers have studied the implications of prospect theoretic preferences in the context of CPS security and robustness [17], [18]; energy consumption decisions in the smart grid [19]; pricing in communication networks [20]; and network interdiction games [21].

In this article, we consider the scenario where each (human) defender misperceives the probabilities of successful attack in the attack graph.[1] We characterize the impacts of such misperceptions on the security investments made by each defender. In contrast with prior work on prospect theoretic preferences in the context of CPS security [17], which assumed that each defender is only responsible for the security of a single node, we consider a more general case where each defender is responsible for 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 CPS where the attacker exploits paths through the network to reach certain target nodes.

Specifically, we build upon the recent work [13] where the authors studied a game-theoretic formulation involving attack graph models of interdependent systems and multiple defenders. The authors showed how to compute the optimal defense strategies for each defender using a convex optimization problem. However, they did not investigate the characteristics of optimal investments and the impacts of behavioral biases of the defenders, which are the focus of the present work.

We introduce the attack-graph-based security game framework in Section II, followed by the behavioral security game setting in Section III. 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 Nash equilibrium (PNE) in this class of games.

We primarily investigate the security investments when users with such behavioral biases act in isolation (see Section IV) as well as in a game-theoretic setting (see Section V). 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 [13]. 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 nonbehavioral 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 (nonbehavioral) socially optimal solution, and provide tight bounds for the PoBA. We illustrate the applicability of the proposed framework in a case study involving a distributed energy resource failure scenario, DER.1, identified by the U.S. National Electric Sector Cybersecurity Organization Resource (NESCOR) [27] in Section VI.

This article extends the conference version of this study [28] in the following manner.

[1]While the existing literature on behavioral aspects of information security, such as [22]–[24], 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 the existing vulnerabilities to potential attack scenarios. Specifically, one model that is captured by our formulation is to define vulnerabilities by CVE-IDs [25], and assign attack probabilities using the common vulnerability scoring system (CVSS) [26].

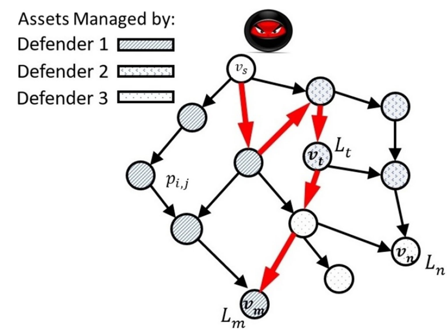

Fig. 1. Overview of the interdependent security game framework. This CPS consists of three interdependent defenders. An attacker tries to compromise critical assets starting from v_s.

1) We rigorously prove the uniqueness of optimal investment decisions for behavioral defenders, and show that behavioral security games can have multiple PNEs in general.
2) We quantify the inefficiency of the Nash equilibria by defining the notion of the PoBA, and provide (tight) bounds on it.
3) We illustrate the theoretical findings via a case study.

II. Security Game Framework

In this section, we describe our general security game framework, including the attack graph and the characteristics of the attacker and the defenders. An overview of our model is shown in Fig. 1.

A. Attack Graph

We represent the assets in a CPS as nodes of a directed graph $G = (V, \mathcal{E})$ where each node $v_i \in V$ represents an asset. A directed edge $(v_i, v_j) \in \mathcal{E}$ 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 Fig. 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.[2]

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 $\{(v_s, v_1), (v_1, v_2), \ldots, (v_k, v_t)\}$. For instance, in Fig. 1, there are two attack paths from v_s to v_t.

Each edge $(v_i, v_j) \in \mathcal{E}$ has an associated weight $p^0_{i,j} \in (0, 1]$, which denotes the probability of successful attack on asset v_j starting from v_i in the absence of any security investments.[3]

[2]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.

[3]In practice, the CVSS [26] can be used for estimating initial probabilities of attack (for each edge in our setting). For example, [10] takes the access complexity submetric in the CVSS (which takes values in {low, medium, high}, representing the complexity of exploiting the vulnerability) and maps it to a probability of exploit (attack) success. The more complex it is to exploit a vulnerability, the less likely an attacker will succeed. Similarly, [29] provides methods and tables to estimate the probability of successful attack from CVSS metrics.

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

B. 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 Fig. 1, there are three defenders with assets shown in different shades, and the loss values of specific nodes are indicated.

To reduce the attack success probabilities on edges interconnecting assets inside the network, a defender can allocate security resources on these edges.[4] We assume that each defender D_k has a security budget $B_k \in [0, \infty)$. Let $x^k_{i,j}$ denote the security investment of the defender D_k on the edge (v_i, v_j). We define

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

thus X_k is the set of feasible investments for the 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 the defender D_k as $x_k \in X_k$. Each entry of x_k denotes the investment on an edge.

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

C. Adversary Model and Defender Cost Function

In networked 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 [9]. 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 that asset (such a path is shown in red in Fig. 1). Such attack models (where the attacker chooses one path to her target asset) have previously been considered in the literature (e.g., [30] and[31]).

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

$$\hat{C}_k(x_k, \mathbf{x}_{-k}) = \sum_{v_m \in V_k} L_m \left(\max_{P \in \mathcal{P}_m} \prod_{(v_i,v_j)\in P} p_{i,j}(x_{i,j}) \right) \tag{2}$$

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.[5]

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 aforementioned security game formulation, and study their impact on the investment decisions and equilibria.

III. Nonlinear Probability Weighting and the Behavioral Security Game

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 [14], [32]. 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 [32], and is given by

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

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. 2. Next, we incorporate this probability weighting function into the security game defined in the last section and define the behavioral security game, which is the focus of this article.

B. 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

[4] Note that v_s does not have any incoming edges, and hence, it cannot be defended.

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

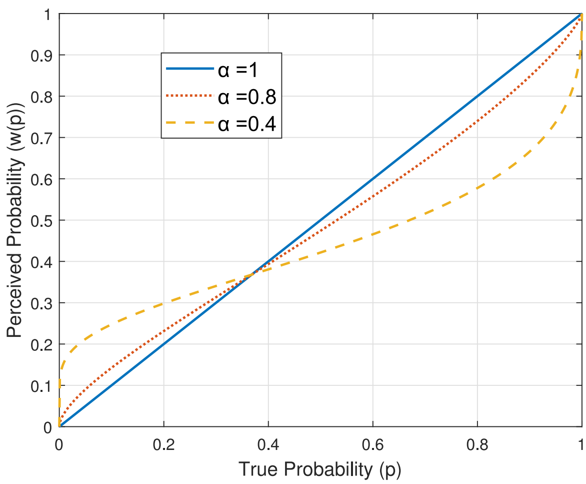

Fig. 2. Prelec probability weighting function (3) that transforms true probabilities p into perceived probabilities $w(p)$. The parameter α controls the extent of overweighting and underweighting.

motivates a broad class of games that incorporate probability weighting, as defined in the following.

Definition 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 (3). Specifically, the perceived attack probability by a defender D_k on an edge (v_i, v_j) is given by

$$w_k(p_{i,j}(x_{i,j})) = \exp\left[-(-\log(p_{i,j}(x_{i,j})))^{\alpha_k}\right] \qquad (4)$$

where $p_{i,j}(x_{i,j}) \in [0, 1]$ 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), each defender D_k seeks to minimize her *perceived expected cost*

$$C_k(x_k, \mathbf{x}_{-k}) = \sum_{v_m \in V_k} L_m \left(\max_{P \in \mathcal{P}_m} \prod_{(v_i,v_j)\in P} w_k\left(p_{i,j}(x_{i,j})\right) \right). \qquad (5)$$

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 compare uncertain outcomes with a reference utility or cost, exhibit risk aversion in gains and risk seeking behavior in losses, and overweight losses compared to gains (loss aversion). A richer behavioral model, referred to as cumulative prospect theory [10], incorporates all these aspects in its cost function. However, in the setting of this article, 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. ■

C. Assumptions on the Probabilities of Successful Attack

The shape of the probability weighting function (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_i, v_j), the probability of successful attack $p_{i,j}(x_{i,j})$ is log-convex,[6] strictly decreasing, and twice continuously differentiable for $x_{i,j} \in [0, \infty)$.

One particular function satisfying the aforementioned conditions is

$$p_{i,j}(x_{i,j}) = p^0_{i,j} \exp(-x_{i,j}). \qquad (6)$$

Such probability functions fall within the class commonly considered in security economics (e.g., [34]), and we will specialize our analysis to this class for certain results in the article. For such functions, the (true) attack success probability of any given path P from the source to a target v_t is given by

$$\prod_{(v_m,v_n)\in P} p_{m,n}(x_{m,n}) = \left(\prod_{(v_m,v_n)\in P} p^0_{m,n} \right) \exp\left(- \sum_{(v_m,v_n)\in P} x_{m,n} \right). \qquad (7)$$

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.

Remark 3: The paper [13] studied this same class of security games for the case of nonbehavioral defenders (i.e., with $\alpha_k = 1 \forall D_k \in \mathcal{D}$). For that case, with probability functions given by (6), [13] 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 article. We omit the details in the interest of space. ■

IV. 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 (5), and subsequently, identify properties of the defender's optimal investment decisions under behavioral (i.e., $\alpha < 1$) and nonbehavioral (i.e., $\alpha = 1$) decision making. This setting will help in understanding the actions (i.e., best responses) of each player in multidefender 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.

[6] This is a common assumption in the literature. In particular, [33] shows that log convexity of the attack probability functions is a necessary and sufficient condition for the optimal security investment result of [34] to hold.

A. 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 $(v_i, v_j) \in \mathcal{E}$, let $h(x_{i,j}) \triangleq (-\log(p_{i,j}(x_{i,j})))^{\alpha_k}$. Then, $h(x_{i,j})$ is strictly concave in $x_{i,j}$ for $x_{i,j} \in [0,\infty)$ under Assumption 1. Moreover, $h(x_{i,j})$ is concave in $x_{i,j}$ for $\alpha_k \in (0,1]$.

Using the aforementioned result, we now establish that the defender's cost function (5) is convex.

Lemma 2: For all $\alpha_k \in (0,1]$ and under Assumption 1, the cost function (5) of the defender D_k is convex in the defense investment x_k.

The proofs of Lemmas 1 and 2 are omitted in the interest of space and can be found in the extended version of this paper [35].

B. Uniqueness of Investments

Having established the convexity of the defender's cost function (5), we now observe the difference in the investment decisions made by behavioral and nonbehavioral defenders. In particular, we first show that the optimal investment decisions by a behavioral defender are unique, and then, contrast that with the (generally) nonunique optimal investments for nonbehavioral defenders.

Proposition 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 (4). Then, the optimal investments by the defender D_k to minimize (5) are unique.

Proof: Consider the defender's optimization problem for the cost function in (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 (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 (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 $h_P(x_{k,P}) \triangleq \sum_{(v_i,v_j)\in P}(-\log(p_{i,j}(x_{i,j})))^{\alpha_k}$. By Lemma 1, each term of the form $(-\log(p_{i,j}(x_{i,j})))^{\alpha_k}$ is strictly concave in $x_{i,j}$ 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 (4), the value of the path P is given by

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

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 (5)]

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

Note that (a) holds from the definition of $\hat{M}$. Also, (b) holds since for each $P \in \bar{\mathcal{P}}_m$, $f_P(x_{k,P}^3) < \frac{1}{2}(f_P(x_{k,P}^1) + f_P(x_{k,P}^2))$ by strict convexity of f_P in $x_{k,P}$ and since $x_{k,P}^3$ is a strict convex combination of $x_{k,P}^1$ and $x_{k,P}^2$ (by definition of $\bar{\mathcal{P}}_m$). Thus, for $v_m \in \hat{M}$, $\max_{P\in\bar{\mathcal{P}}_m} f_P(x_{k,P}^3) < \max_{P\in\bar{\mathcal{P}}_m} \frac{1}{2}(f_P(x_{k,P}^1) + f_P(x_{k,P}^2))$. 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, $C_k(x_k^3) < \frac{1}{2}(C_k(x_k^1) + C_k(x_k^2))$ that yields a contradiction to the optimality of x_k^1 and x_k^2.

In the second case, suppose $\hat{M}$ is empty. Thus, $\forall v_m \in V_k$, $\max_{P\in\bar{\mathcal{P}}_m} f_P(x_{k,P}^3) < \max_{P\in\mathcal{P}_m\setminus\bar{\mathcal{P}}_m} f_P(x_{k,P}^3)$. 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_k^3 has nonzero investments on edges in $\bar{E}$. Thus, x_k^3 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 aforementioned result, the optimal investments by a nonbehavioral 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 (6). As argued in (7), the probability of the 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 nonbehavioral defender, any other set of investments that maintains the same total investment on each path of the graph is also optimal.

C. Locations of Optimal Investments for Behavioral and Nonbehavioral Defenders

We next study differences in the *locations* of the optimal investments by behavioral and nonbehavioral defenders. In particular, we first characterize the optimal investments by a nonbehavioral 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 [36].

Proposition 2: Consider an attack graph $G = (V, \mathcal{E})$. Let the attack success probability under security investments be given by $p_{i,j}(x_{i,j}) = e^{-x_{i,j}}$, where $x_{i,j} \in \mathbb{R}_{\geq 0}$ is the investment on edge (v_i, v_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 nonbehavioral defender D_k to distribute all her investments equally only on the edge set $\mathcal{E}_c$ in order to minimize (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.

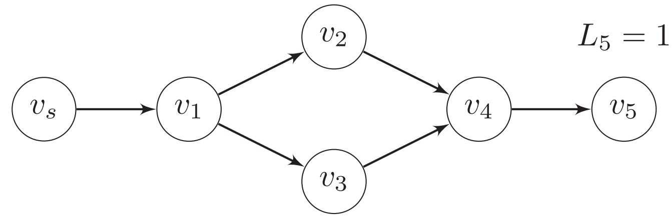

Fig. 3. An attack graph where a behavioral defender makes suboptimal investment decisions.

Consider any optimal investment of that budget. Recall from (7) that for probability functions of the form (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 [36], 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 nonequally on edges in $\mathcal{E}_c$ where an edge $(v_i, v_j) \in \mathcal{E}_c$ has investment $x_{i,j} < \frac{B}{N}$. 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 path with the highest probability of attack has a probability of attack larger than $\exp(-\frac{B}{N})$ (which would be obtained when investing $\frac{B}{N}$ equally on each edge in $\mathcal{E}_c$). Therefore, the true expected cost in (2) is higher with this nonequal 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 aforementioned result will continue to hold for more general probability functions $p_{m,n}(x_{m,n}) = p_{m,n}^0 e^{-x_{m,n}}$ with $p_{m,n}^0 \neq 1$ if $\prod_{(v_m,v_n)\in P} p_{m,n}^0$ 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 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 Fig. 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_i, v_j) be given by $p_{i,j}(x_{i,j}) = e^{-x_{i,j}}$, where $x_{i,j}$ 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, it is optimal for a nonbehavioral defender to put all of her budget on either one of these edges.

Now consider a behavioral defender with $\alpha < 1$. With the aforementioned expression for $p_{i,j}(x_{i,j})$ and using the Prelec function (4), we have $w(p_{i,j}(x_{i,j})) = e^{-x_{i,j}^{\alpha}}$. Thus, the perceived expected cost function (5) is given by

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

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

$$\begin{aligned} x_{1,2} &= x_{2,4} = x_{1,3} = x_{3,4} = 2^{\frac{1}{\alpha-1}} x_{s,1} \\ x_{4,5} &= x_{s,1} = \frac{B - 4x_{1,2}}{2} = \frac{B}{2 + 4(2^{\frac{1}{\alpha-1}})}. \end{aligned} \tag{8}$$

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

The aforementioned 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 nonbehavioral defender) that lie entirely on the min-cut edges. Indeed, by taking the limit as $\alpha \uparrow 1$, we have

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

for edges (v_i, v_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 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 $(v_i, v_j) \in \mathcal{E}$ be given by $p_{i,j}(x_{i,j}) = e^{-x_{i,j}}$, where $x_{i,j}$ 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, it is optimal to invest the entire budget uniformly on edges in $\mathcal{E}_c$ in order to minimize the cost function (2). We will show that this investment is not optimal with respect to the behavioral defender's cost function (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), 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 the path P will be

$$f_1(\mathbf{x}) \triangleq \exp\left(-\sum_{\substack{(v_i,v_j)\in\mathcal{E}_c,\\ (v_i,v_j)\in P}} x_{i,j}^{\alpha}\right).$$

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 the path P will be

$$f_2(\mathbf{x}) \triangleq \exp\left(-\sum_{\substack{(v_i,v_j)\in\mathcal{E}_c^{'},\\ (v_i,v_j)\in P}} \left(\frac{N\epsilon}{M}\right)^{\alpha} - \sum_{\substack{(v_i,v_j)\in\mathcal{E}_c,\\ (v_i,v_j)\in P}} (x_{i,j}-\epsilon)^{\alpha}\right).$$

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

$$\sum_{\substack{(v_i,v_j)\in\mathcal{E}_c^{'},\\ (v_i,v_j)\in P}} \left(\frac{N\epsilon}{M}\right)^{\alpha} + \sum_{\substack{(v_i,v_j)\in\mathcal{E}_c,\\ (v_i,v_j)\in P}} (x_{i,j}-\epsilon)^{\alpha} > \sum_{\substack{(v_i,v_j)\in\mathcal{E}_c,\\ (v_i,v_j)\in P}} x_{i,j}^{\alpha}. \tag{9}$$

If we define

$$f(\epsilon) \triangleq \sum_{\substack{(v_i,v_j)\in\mathcal{E}_c^{'},\\ (v_i,v_j)\in P}} \left(\frac{N\epsilon}{M}\right)^{\alpha} + \sum_{\substack{(v_i,v_j)\in\mathcal{E}_c,\\ (v_i,v_j)\in P}} (x_{i,j}-\epsilon)^{\alpha}$$

we see that inequality (9) is equivalent to showing that $f(\epsilon) > f(0)$. We have

$$\frac{df}{d\epsilon} = \frac{\alpha N}{M} \sum_{\substack{(v_i,v_j)\in\mathcal{E}_c^{'},\\ (v_i,v_j)\in P}} \left(\frac{N\epsilon}{M}\right)^{\alpha-1} - \alpha \sum_{\substack{(v_i,v_j)\in\mathcal{E}_c,\\ (v_i,v_j)\in P}} (x_{i,j}-\epsilon)^{\alpha-1}.$$

Note that $\lim_{\epsilon\downarrow 0} \frac{df}{d\epsilon} = \infty$ that 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 Fig. 3 satisfies the conditions in the aforementioned 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 nonbehavioral defenders, we next turn our attention to the behavioral security game with multiple defenders, introduced in Section III.

V. Analysis of Multidefender Games

A. 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 III. 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 4: 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.

(a) (b)

Fig. 4. 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.

Proof: The feasible defense strategy space X_k in (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 (5) is convex in $x_k \in X_k$; this follows from Lemma 2 and the fact that the investment $x_{i,j}$ 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 [37]. ∎

Note that in contrast to the best responses by each player (which were unique when $\alpha_k \in (0,1)$, as shown in Proposition 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 Fig. 4. There are two defenders, D_1 and D_2, where the defender D_1 wishes to protect node v_4, and the defender D_2 wishes to protect node v_5. Suppose that D_1 has a budget $B_1 = 16$ and D_2 has $B_2 = 12$. Fig. 4(a) and (b) illustrates two distinct PNE for this game. We obtained multiple Nash equilibria by varying the starting investment decision of the 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 Fig. 4(a), defender D_1's perceived expected cost, given by (5), is equal to $\exp(-4)$, while her true expected cost, given by (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 Fig. 4(b), the defender D_1 has a perceived expected cost of $\exp(-2\sqrt{5})$ 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 Fig. 4(a) is preferred by the defender D_2, while the equilibrium in Fig. 4(b) has a lower expected cost (both perceived and real) for the 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 Fig. 4(b); that is, the PNE of Fig. 4(b) would be preferred from a social planner's perspective.

B. Measuring the Inefficiency of PNE: The PoBA

The notion of price of anarchy (PoA) is often used to quantify the inefficiency of Nash equilibrium compared to the socially optimal outcome [38]. Specifically, the PoA 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 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 nonbehavioral 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)] is the true expected cost faced by the defender D_k under the investment vector $\mathbf{x}$. Let $X^{\mathtt{NE}} := \{\bar{\mathbf{x}} \in \mathbb{R}_{\geq 0}^{|\mathcal{D}||\mathcal{E}|} | \bar{x}_k \in \operatorname{argmin}_{x \in X_k} C_k(x, \bar{\mathbf{x}}_{-k}) \forall D_k \in \mathcal{D}\}$, i.e., $X^{\mathtt{NE}}$ is the set of all investments that constitute a PNE. We now define the PoBA as

$$\text{PoBA} = \frac{\sup_{\bar{\mathbf{x}} \in X^{\mathtt{NE}}} \hat{C}(\bar{\mathbf{x}})}{\hat{C}(\mathbf{x}^*)} \tag{10}$$

where $\mathbf{x}^*$ denotes the investments at the social optimum (computed by a nonbehavioral social planner with access to the sum of all defenders' budgets). Mathematically, let $X^{\mathsf{Soc}} := \{\mathbf{x}^* \in \mathbb{R}_{\geq 0}^{|\mathcal{D}||\mathcal{E}|} | \mathbf{1}^T \mathbf{x}^* \leq \sum_{D_k \in \mathcal{D}} B_k\}$, i.e., X^{Soc} is the set of all feasible investments by the social planner, and $\mathbf{x}^* \in \operatorname{argmin}_{\mathbf{x} \in X^{\mathsf{Soc}}} \hat{C}(\mathbf{x})$. 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 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).

Proposition 5: Let the sum of the budgets available to all defenders be B, and let the probability of successful attack on each edge $(v_i, v_j) \in \mathcal{E}$ be given by $p_{i,j}(x_{i,j}) = e^{-x_{i,j}}$. 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 (10) (the total true expected cost at the worst PNE). Recall that each

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

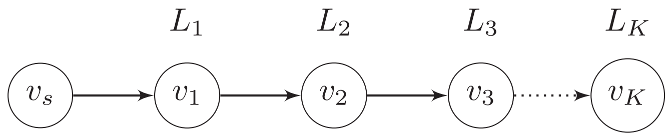

Fig. 5. Attack graph where PoBA is lower bounded by $(1-\epsilon)\exp(B)$.

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 $(\sum_{D_k \in \mathcal{D}} \sum_{v_m \in V_k} L_m)\exp(-B)$ (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 (10), we obtain PoBA $\leq \exp(B)$. ■

Next, we show that the upper bound on the PoBA obtained in Proposition 5 is asymptotically tight.

Proposition 6: 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 Fig. 5, where the probability of the successful attack on each edge (v_i, v_j) is given by (6) with $p^0_{i,j} = 1$. This graph contains K defenders, and each defender D_k is responsible for defending the 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 (10) is $\sum_{i=1}^{K} L_i \exp(-B) = (K+1)\exp(-B)$.

We now characterize a lower bound on the cost under a PNE [i.e., the numerator of (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 the node v_1, it is optimal for the 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 (5). Thus, D_2's optimization problem, given D_1's investment, is

$$\underset{x_{s,1}^2 + x_{1,2}^2 = \frac{B}{K}}{\text{minimize}} \quad e^{-\left(\frac{B}{K} + x_{s,1}^2\right)^{\alpha_2} - \left(x_{1,2}^2\right)^{\alpha_2}}. \tag{11}$$

The unique optimal solution of (11) (for all $\alpha_2 \in (0,1)$) would be to put all $\frac{B}{K}$ into $x_{1,2}^2$ and zero on $x_{s,1}^2$. 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 the 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 $L_1 \exp(-\frac{B}{K}) = K\exp(-\frac{B}{K})$. Thus, the PoBA is lower bounded by

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

As the length of the chain grows, we have $\lim_{K\to\infty} \frac{K\exp(-\frac{B}{K})}{(K+1)} = 1$. 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 5 is agnostic to the structure of the network, the number of defenders, and their degree of misperception of probabilities. In Proposition 6, our result shows that the upper bound obtained in Proposition 5 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 Fig. 6 (a) and (b) with two defenders, D_1 and D_2. The defender D_1 wishes to protect the node v_3, and the defender D_2 wishes to protect the 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 the defender D_1 has a budget $B_1 = 5$, while the defender D_2 has a budget $B_2 = 20$. The optimal investments in the following scenarios were calculated using CVX [39].

Suppose both defenders are nonbehavioral. In this case, Proposition 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 Fig. 6(a). On the other hand, as indicated by Proposition 3, investing solely on the min-cut is no longer optimal for a behavioral defender. Indeed, Fig. 6(b) shows a PNE for the case where D_2 is behavioral with $\alpha_2 = 0.6$, 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 nonbehavioral (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 nonbehavioral 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.

VI. Case Study

Here, we examine the outcomes of behavioral decision making in a case study involving a distributed energy resource failure

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

Fig. 6. Numbers above (below) each edge represent investments by defender D_1 (D_2). (a) Nonbehavioral defender D_1 does not receive any investment contributions from the nonbehavioral defender D_2. (b) Nonbehavioral defender D_1 benefits from the investment contributions of the behavioral defender D_2.

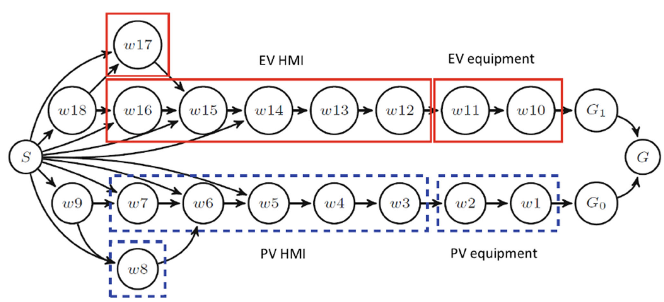

Fig. 7. Attack graph of a DER.1 failure scenario adapted from [27]. It shows stepping-stone attack steps that can lead to the compromise of a photovoltaic generator (PV) (i.e., G_0) or an electric vehicle charging station (EV) (i.e., G_1).

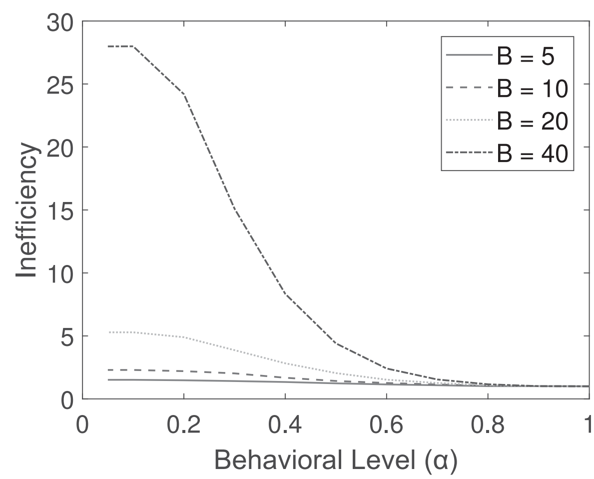

Fig. 8. The inefficiency for different behavioral levels of the defenders. We observe that the inefficiency increases as the security budget increases, and as the defenders become more behavioral.[8]

scenario, DER.1, identified by the U.S. National Electric Sector Cybersecurity Organization Resource (NESCOR) [27]. Fig. 7 is replicated from the attack graph for the DER.1 (see[27, Fig. 4]). Suppose the probability of successful attack on each edge is $p_{i,j}(x_{i,j}) = e^{-x_{i,j}}$. 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 (10) to measure the inefficiency of the corresponding equilibrium.

Fig. 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 (nonbehavioral), 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 IV. Furthermore, Fig. 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 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; this reduces the total cost faster toward zero as the budget increases.

Our results may be applicable to other practical scenarios (such as deploying moving-target defense) [13]. While the inefficiency strictly increased with the budget in the aforementioned case study, this phenomenon may not occur in all networks. We omit further discussions about these aspects in the interest of space.

VII. Summary of Findings

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

[8]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 (nonbehavioral) social optimum.

in order to protect their assets, whereas behavioral decision makers will choose to spread their investments over other edges in the network, potentially making their assets more vulnerable. Third, we showed that multidefender games possess a PNE (under appropriate conditions on the game), and introduced a metric that we termed the 'PoBA' to quantify the inefficiency of the (behavioral) PNE as compared to the security outcomes under socially optimal investments. We provided a tight bound on the PoBA, which depended only on the total budget across all defenders. However, we 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, we presented a case study where the inefficiency of the equilibrium increased as the defenders became more behavioral.

Overall, our analysis shows that human decision making (as 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. In other words, the insights that are provided by our 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 to perform human experiments to test our predictions. Moreover, studying the properties of security investments when different edges have different degrees of misperception of attack probabilities is another avenue for future research.

References

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

[2] A. Laszka, M. Felegyhazi, and L. Buttyan, "A survey of interdependent information security games," *ACM Comput. Surv.*, vol. 47, no. 2, pp. 23:1–23:38, 2015.

[3] T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach*. New York, NY, USA: Cambridge Univ. Press, 2010.

[4] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2038–2049, Jul. 2016.

[5] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "A hybrid stochastic game for secure control of cyber-physical systems," *Automatica*, vol. 93, pp. 55–63, 2018.

[6] J. Milosevic, M. Dahan, S. Amin, and H. Sandberg, "A network monitoring game with heterogeneous component criticality levels," 2019, *arXiv:1903.07261*.

[7] P. N. Brown, H. P. Borowski, and J. R. Marden, "Security against impersonation attacks in distributed systems," *IEEE Trans. Control Netw. Syst.*, vol. 6, no. 1, pp. 440–450, May 2018.

[8] J. R. Riehl and M. Cao, "A centrality-based security game for multihop networks," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 4, pp. 1507–1516, Jul. 2017.

[9] 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. Smart Grid*, vol. 3, no. 4, pp. 1790–1799, Dec. 2012.

[10] J. Homer *et al.*, "Aggregating vulnerability metrics in enterprise networks using attack graphs," *J. Comput. Secur.*, vol. 21, no. 4, pp. 561–597, 2013.

[11] P. Naghizadeh and M. Liu, "Opting out of incentive mechanisms: A study of security as a non-excludable public good," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 12, pp. 2790–2803, Dec. 2016.

[12] R. J. La, "Interdependent security with strategic agents and cascades of infection," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1378–1391, Jun. 2016.

[13] 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*. New York, NY, USA: Springer, 2018, pp. 157–184.

[14] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Econometrica.*, vol. 47, pp. 263–291, 1979.

[15] S. Dhami, *The Foundations of Behavioral Economic Analysis*. New York, NY, USA: Oxford Univ. Press, 2016.

[16] N. C. Barberis, "Thirty years of prospect theory in economics: A review and assessment," *J. Econ. Perspectives*, vol. 27, no. 1, pp. 173–96, 2013.

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

[18] A. R. Hota, S. Garg, and S. Sundaram, "Fragility of the commons under prospect-theoretic risk attitudes," *Games Econ. Behav.*, vol. 98, pp. 135–164, 2016.

[19] S. R. Etesami, W. Saad, N. B. Mandayam, and H. V. Poor, "Stochastic games for the smart grid energy management with prospect prosumers," *IEEE Trans. Autom. Control*, vol. 63, no. 8, pp. 2327–2342, Aug. 2018.

[20] Y. Yang, L. T. Park, N. B. Mandayam, I. Seskar, A. L. Glass, and N. Sinha, "Prospect pricing in cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 1, no. 1, pp. 56–70, Mar. 2015.

[21] A. Sanjab, W. Saad, and T. Başar, "Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game," in *Proc. IEEE Int. Conf. Commun.*, 2017, pp. 1–6.

[22] M. Baddeley, "Information security: Lessons from behavioural economics," in *Proc. Workshop Econ. Inf. Secur.*, 2011, pp. 1–20.

[23] R. Anderson, "Security economics: A personal perspective," in *Proc. 28th Annu. Comput. Secur. Appl. Conf.*, 2012, pp. 139–144.

[24] B. Schneier, "The psychology of security," in *Proc. Int. Conf. Cryptol. Africa*, 2008, pp. 50–79.

[25] R. A. Martin, "Managing vulnerabilities in networked systems," *Computer*, vol. 34, no. 11, pp. 32–38, 2001.

[26] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Secur. Privacy*, vol. 4, no. 6, pp. 85–89, Nov./Dec. 2006.

[27] S. Jauhar *et al.*, "Model-based cybersecurity assessment with NESCOR smart grid failure scenarios," in *Proc. IEEE 21st Pacific Rim Int. Symp. Dependable Comput.*, 2015, pp. 319–324.

[28] 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 *Proc. Amer. Control Conf.*, Jul. 2019, pp. 5260–5265.

[29] H. Zhang, F. Lou, Y. Fu, and Z. Tian, "A conditional probability computation method for vulnerability exploitation based on CVSS," in *Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace*, Jun. 2017, pp. 238–241.

[30] 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 *Proc. 10th Int. Conf. Auton. Agents Multiagent Syst.-Vol. 1*, 2011, pp. 327–334.

[31] G. Brown, M. Carlyle, A. Abdul-Ghaffar, and J. Kline, "A defender-attacker optimization of port radar surveillance," *Naval Res. Logistics*, vol. 58, no. 3, pp. 223–235, 2011.

[32] D. Prelec, "The probability weighting function," *Econometrica*, vol. 66, pp. 497–527, 1998.

[33] Y. Baryshnikov, "IT security investment and Gordon-Loeb's 1/e rule," in *Proc. Workshop Econ. Inf. Secur.*, 2012, pp. 1–7.

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

[35] 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," 2020, *arXiv:2001.03213*.

[36] D. B. West *et al.*, *Introduction to Graph Theory*, vol. 2. Englewood Cliffs, NJ, USA: Prentice-Hall, 2001.

[37] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica*, vol. 33, pp. 520–534, 1965.

[38] T. Roughgarden, "The price of anarchy is independent of the network topology," *J. Comput. Syst. Sci.*, vol. 67, no. 2, pp. 341–364, 2003.

[39] M. Grant and S. Boyd, "CVX: MATLAB software for disciplined convex programming, version 2.1," Mar. 2014. [Online]. Available: http://cvxr.com/cvx

Mustafa Abdallah received the B.Sc. degree in electronics and communications engineering and the M.Sc. degree in engineering mathematics from the Faculty of Engineering, Cairo University, Giza, Egypt, in 2012 and 2016, respectively. He is currently working toward the Ph.D. degree in electrical and computer engineering with Purdue University, West Lafayette, IN, USA.

His research interests include game theory, behavioral decision making, and deep learning, with applications including cyber security and speech recognition.

Mr. Abdallah was the recipient of the Best Fresher Award from DCSL lab, Purdue University, in 2017 and a M.Sc. fellowship from the Faculty of Engineering, Cairo University, in 2013.

Parinaz Naghizadeh (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Michigan, Ann Arbor, MI, USA, in 2016.

She is an Assistant Professor with the Department of Integrated Systems Engineering and the Department of Electrical and Computer Engineering, Ohio State University, Columbus, OH, USA. Her research interests include network economics, game theory, reinforcement learning, and data analytics, with applications including cyber security and edge computing.

Dr. Naghizadeh was the recipient of the Barbour Scholarship in 2014 and a Rising Star in electrical engineering and computer science in 2017.

Ashish R. Hota received the B.Tech. and M.Tech. degrees (dual degree) in electrical engineering from the Indian Institute of Technology (IIT) Kharagpur, Kharagpur, India, in 2012, and the Ph.D. degree from Purdue University, West Lafayette, IN, USA, in 2017.

He is an Assistant Professor with the Department of Electrical Engineering, IIT Kharagpur. He was a Postdoctoral Researcher with the Automatic Control Laboratory, ETH Zürich, Zürich, Switzerland, in 2018. From 2012 to 2014, he was a Research Assistant with the University of Waterloo, Waterloo, ON, Canada. His research interests include the areas of game theory, stochastic optimization, distributed control, and security and robustness of networked systems.

Dr. Hota was the recipient of the Outstanding Graduate Researcher Award from the College of Engineering, Purdue University, in 2017 and the Institute Silver Medal from the IIT Kharagpur in 2012.

Timothy Cason received the Ph.D. degree in economics from the University of California-Berkeley, Berkeley, CA, USA, in 1991.

He is a Distinguished Professor and Robert and Susan Gadomski Chair in economics with Purdue University, West Lafayette, IN, USA. He was an Assistant and Associate Professor with the University of Southern California, before joining Purdue University in 1998. His research interests include experimental and behavioral economics, environmental economics, and industrial organization, including applied research in market design, environmental regulation, and antitrust.

Dr. Cason is a former Co-Editor for the *Journal of Public Economics* and a past Editor for the *Journal Experimental Economics*, and has also served on numerous other editorial boards. He has also served as the President of the Economic Science Association (2009–2011), which is the international society of experimental economists. He is a Fellow of the Society for the Advancement of Economic Theory, a Fulbright Commission Senior Scholar, and was the recipient of dozens of grants, awards, and fellowships.

Saurabh Bagchi received the M.S. and Ph.D. degrees from the Department of Computer Science, University of Illinois, Urbana-Champaign, IL, USA, in 1998 and 2001, respectively.

He is a Professor with the School of Electrical and Computer Engineering and the Department of Computer Science, Purdue University, West Lafayette, IN, USA. He has been the Founding Director of a university-wide resilience center called CRISP, Purdue University, since 2017. He also co-leads the WHIN-SMART center, Purdue University, for Internet of Things and data analytics. He is proud of the 21 Ph.D. students and 50 Masters thesis students who have graduated from his research group and who are in various stages of building wonderful careers in industry or academia. His research interests include dependable computing and distributed systems.

Prof. Bagchi was elected to the IEEE Computer Society Board of Governors for the 2017–2019 term and re-elected in 2019.

Shreyas Sundaram received the Ph.D. degree in electrical engineering from the University of Illinois at Urbana-Champaign, Champaign, IL, USA, in 2009.

He is an Associate Professor with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA. He was a Postdoctoral Researcher with the University of Pennsylvania from 2009 to 2010 and an Assistant Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, from 2010 to 2014. His research interests include network science, analysis of large-scale dynamical systems, fault-tolerant and secure control, linear systems, and estimation theory and game theory.

Dr. Sundaram was the recipient of the NSF CAREER award. At Purdue, he was the recipient of the HKN Outstanding Professor Award, the Outstanding Mentor of Engineering Graduate Students Award, the Hesselberth Award for Teaching Excellence, and the Ruth and Joel Spira Outstanding Teacher Award. At Waterloo, he was the recipient of the Department of Electrical and Computer Engineering Research Award and the Faculty of Engineering Distinguished Performance Award. He was also the recipient of the M. E. Van Valkenburg Graduate Research Award and the Robert T. Chien Memorial Award from the University of Illinois. He was a finalist for the Best Student Paper Award at the 2007 and 2008 American Control Conferences.