Effects of Degree Distributions on Network Security Investments and Internalization of Externalities

Richard J. La

***Abstract*—We study the following three questions: (1) How do the node degrees in a network affect security investments when nodes are strategic and have different security investment choices? (2) How can we provide an incentive to selfish nodes to increase their security investments in order to improve the overall security and reduce the social cost? (3) How much inefficiency does the selfish nature of nodes cause? Making use of a population game model based on the well-known Chung-Lu random graph model, we first examine how the *degree distribution* of nodes influences their security investments at Nash equilibria (NEs) and overall network security measured by *risk exposure* from a neighbor. Here, the risk exposure quantifies the average risk or threat posed by a neighbor. We demonstrate several structural properties exhibited by both the NEs of population games and social optima that minimize the overall social cost. We show that, under some mild assumption, as the degrees of neighbors become (stochastically) larger, somewhat surprisingly, the risk exposure *decreases* at both NEs and social optima even though the security investments by a node of a *fixed* degree diminish. Secondly, we illustrate the relation between the NEs of population games and social optima. This relation offers a possible means of *internalizing* the externalities so as to enhance overall network security and reduce the social cost. Finally, we derive an upper bound on the *price of anarchy*, which is an affine function of the *average* degree of nodes.**

***Index Terms*—Game theory, interdependent security, internalization of externalities.**

I. Introduction

Interdependent security (IDS) [23] has recently emerged as an active research area. IDS refers to scenarios where the security of an agent or system depends not only on its own security measures, but also on those of others. It arises naturally in many areas including cybersecurity [10], [24], [31], [32], cyber-physical systems security (e.g., power grids) [2], [11], epidemiology [39], [42], financial networks and systems [6], [12], [13], homeland security [22], [28], and supply chain and transportation system security (e.g., airline security) [19], [23], [25], [27], just to name a few.

Some of key challenges to tackling IDS in large networks are: (i) participating agents are often strategic and are interested only in their own security and/or objectives, rather than the security of the overall network/system, and (ii) any attempt to model *detailed* interactions among many (strategic) agents suffers from the *curse of dimensionality*.

We are interested in studying the security of a network consisting of many nodes that represent, for instance, individual users or organizations. The edges in the network are not necessarily physical links. Instead, they could represent *logical* or *relational* links. The degree of a node is defined to be the number of neighbors or incident edges it has in the network.[1]

We assume that there are malicious entities, called *attackers*, which launch attacks against the nodes, for example, in hopes of infecting the machines or gaining unauthorized access to information of victims. Not only can nodes suffer damages or losses due to *direct* attacks from the attackers, but the victims of successful direct attacks may also unknowingly help the attackers launch *indirect* attacks on their neighbors.

In the face of possible attacks, nodes can try to manage the risks from such attacks in various ways. For instance, a node can invest in various security measures with the goal of protecting itself from malicious attacks. In other cases, it may be able to purchase *insurance* to transfer (some of) its risk from successful attacks.

We use the following examples to motivate our study:

E1. Spread of email viruses and malwares: When a user is infected by a computer virus, it can scan the user's emails and hard disk drive and send the user's personal or other confidential information to criminals interested in stealing, for instance, the user's identify (ID) or trade secrets. Moreover, the virus can browse the user's contact list and either forward it to the attackers or send out bogus emails, i.e., email spoofing, with a link or an attachment to those on the contact list. When a recipient clicks on the link or opens the attachment, it too becomes infected.

In order to reduce the risks or threats posed by malicious viruses and malwares, users can purchase and install an anti-virus software on their devices. This also reduces the risk to those on their contact lists, in the process producing *positive network externalities* or *network effects* [44].

E2. Organizational networks: Organizational information networks are typically protected via various security measures, including replication of data storage and information, network monitoring systems and incoming traffic monitoring. The choices of employed security measures may depend on the magnitude of possible financial and other losses (e.g., damages to reputation), desired network/system dependability as well as available budget for security [4].

Organizational networks are interconnected and, in many cases, share information. Thus, when some networks are more vulnerable, they may serve as stepping stones for sophisticated

This work was supported in part by the National Science Foundation under Grant CCF 08-30675 and a grant from National Institute of Standards and Technology.

Author is with the Department of Electrical & Computer Engineering (ECE) and the Institute for Systems Research (ISR) at the University of Maryland, College Park. E-mail: hyongla@umd.edu

[1]We assume that the network is modeled as an *undirected* graph in the paper. If the network was modeled as a *directed* graph instead, the degree distribution of players we are interested in would be that of *in-degrees*.

hackers to gain access to even better protected networks by using known vulnerabilities [1] or zero-day exploits [8].

We assume that the nodes are rational and interested in minimizing their own costs. But, when the network comprises many nodes, it is challenging to model the details of strategic interactions among all nodes. To skirt this difficulty, we employ a *population game* model [41] with the help of the Chung-Lu random graph model [17]. A population game is often used to model the strategic interactions between many players, possibly from different populations. This new framework allows for an exploration of intricacies of the complex problem of network security with many nodes. We adopt a well known solution concept, namely *Nash equilibrium* (NE) of the population game, as an approximation to nodes' behavior in practice.

Our goal is to understand (a) the structure of the NEs of population games and social optima and (b) the resultant network security as a function of *node degree distribution*. To this end, we adopt *risk exposure*, i.e., the risk a node sees from a (randomly chosen) neighbor, as a measure of network security. In addition, we investigate how the NEs of population games are related to the social optima. In doing so, we also offer a possible means of *internalizing* the (negative) externalities produced by nodes [46] to improve network security and reduce overall social cost.

Our main contributions can be summarized as follows.

1) We reveal several interesting properties and structure of both the NEs of population games and social optima. In particular, we show that, while NEs may not be unique, the risk exposure is identical at all NEs. Similarly, the social optima are not necessarily unique, but the risk exposure and social cost are the same at all social optima. Furthermore, the security investments are nondecreasing in the degrees of the nodes at both NEs and social optima (Section IV).
2) As the weighted node degree distribution, where the weights are the node degrees, becomes (stochastically) larger [43], the risk exposure at both NEs and social optima diminishes. This finding suggests that the *local* security seen by nodes with fixed degrees improves as the network connectivity becomes denser (Section IV).
3) We uncover an intriguing relation between the NEs of a population game and social optima. More specifically, we prove that the social optima are the NEs of a slightly modified population game, where the risk from indirect attacks is doubled from that of the original population game. This finding hints at the possibility of enforcing the socially optimal policy with strategic agents by an appropriate change of their cost function (Section V).
4) We derive an upper bound on the price of anarchy/price of stability (POA/POS) [26], which is an affine function of the average node degree (Section VI).

To the best of our knowledge, our work (along with [29]) is the first study to (i) look at how the node degree distribution influences network security at resulting NEs and social optima with a large number of nodes, (ii) provide a (tight) upper bound on the POA/POS as a function of average node degree, and (iii) reveal the interesting relation between NEs and social optima, which also explains the aforementioned similarity in their structural properties revealed by our study.

It is true that our study is conducted using a simplified model under several, perhaps unrealistic assumptions for analytical tractability. For this reason, we do not claim that our model accurately represents the complex reality and the *quantitative* aspects of our findings will hold in practice. Instead, our hope is that even this simple model will help us understand the *qualitative* nature of *aggregate* behavior of nodes and shed some light on how the underlying structure of interdependency in security among the nodes shapes their security investments and overall network security in more realistic settings.

The rest of the paper is organized as follows. We briefly summarize some of existing studies that are most closely related to our study in Section II. Section III describes the population game model we adopt for our analysis. Our main findings on the structural properties of both NEs and social optima are presented in Section IV. We analyze the relation between the NEs of population games and social optima in Section V. A (tight) upper bound on the POA/POS is offered in Section VI. We conclude in Section VII with a few remarks on future directions.

II. Related literature

Kunreuther and Heal [23], [27] studied the scenarios where the security of involved parties is interdependent, dubbing it IDS. The IDS scenarios with strategic players are often studied in game theoretic settings [21], [23], [24], [25], [27], [33], [34], [35], [37], [38]. We refer an interested reader to a survey paper by Laszka et al. [30] and references therein for a succinct discussion of these and other related studies. Here, we attempt to summarize just a few studies most relevant to ours.

In an interesting study [24], Jiang et al. examine a network security game and characterize the POA under *effective investment* and *bad traffic* models and shed some light on how the cost functions and mutual influence of players affect the POA. Then, they show that more efficient equilibria can be supported in repeated games through cooperation.

Naghizadeh and Liu [35] study the problem of internalizing the (negative) externalities produced by strategic players in IDS games. They propose an *incentive-compatible* algorithm that allows the players to converge to a socially efficient state at an NE. However, the proposed scheme is not individually rational, and the existence of an algorithm that simultaneously achieves i) incentive compatibility, ii) efficiency and iii) individual rationality remains an open problem.

Some of the existing studies also inspect either how cybersecurity insurance (CSI) can be used to promote security investments or how system parameters influence security investments, including CSI, e.g., [31], [32], [37]. We refer an interested reader to [9] and references therein for a discussion on a general framework and market models for CSI.

Lelarge and Bolot [31] use a model that captures epidemic propagation of viruses/worms and network effects. They show that organizations do not have a strong incentive to invest in

security at equilibria. In addition, they derive the POA for large sparse random graphs and demonstrate the presence of free riding similar to that shown in [45]. In a follow-up study [32], they investigate the problem of incentivizing organizations to invest in security through taxation and insurance. They show that, *in the absence of moral hazard*, insurance may be used to encourage organizations to protect themselves.

Ogut et al. [37] investigate the impact of interdependency of security on the choices for security investments and CSI. Their findings suggest that the interdependence of security tends to reduce the organizations' incentive to invest in security measures and CSI. Furthermore, they indicate that a more mature or developed CSI market may not promote CSI unless the price of insurance comes down and that the CSI market may fail due to correlated damages/incidents that may result in catastrophic losses for insurers.

We note that none of the aforementioned studies considers (a) the effects of *node degree distribution* on resulting equilibria and network security, (b) the relation between the average node degree and inefficiency of equilibria, or (c) the relation between the NEs of population games and social optima. On the other hand, while CSI may be one of possible tools to either incentivize or require nodes to invest more in security in the future, it is not clear yet what form of CSI will emerge. For this reason, we do not explicitly model or examine the effects of the availability of CSI in our study and instead leave it for a future study.

We study in [29] a related problem, namely how various network parameters shape the *(global) cascade* probability. We argue that the cascade probability can be considered a *global* measure of network security, for it measures how likely an infection, starting with one or a small number of initially infected nodes, may spread to a large portion of the network. Not only are the emphasis and findings of [29] different from those of the current study, but also the model we employ in [29] is different from that used here in two ways. First, we allow only binary security choices to facilitate analysis in [29], whereas there are N available security choices in this study, where N can be any arbitrary positive integer. Second, while we assume that infections can spread only to immediate neighbors for mathematical tractability here, in [29] we allow infections to transmit multiple hops and study how the infection propagation rate affects resulting cascade probabilities at NEs.

III. Model and problem formulation

We model the interaction among the nodes as a *noncooperative game*, in which players are the nodes in the network.[2] This is reasonable because, in many cases, it may be difficult for nodes to cooperate with each other and take coordinated countermeasures to attacks. In addition, even if they could coordinate their actions, they would be unlikely to do so in the absence of clear incentives for coordination.

We are interested in scenarios where the number of nodes is large. Unfortunately, modeling detailed *microscale* interactions among many nodes in a large network and analyzing ensuing games is difficult; the number of possible strategy profiles increases exponentially with the number of players and finding the NEs of noncooperative games is often challenging even with a moderate number of players.

For analytical tractability, we employ a *population game* model. Population games provide a unified framework and tools for studying *strategic interactions* among *a large number of agents* under following assumptions [41]. First, the choice of an individual agent has very little effect on the payoffs of other agents. Second, there are finitely many populations of agents, and each agent is a member of exactly one population. Third, the payoff of each agent depends only on the *distribution* of actions chosen by members of each population. For a detailed discussion of population games, we refer an interested reader to the manuscript by Sandholm [41]. We will follow the language of [41] throughout the paper.

Our population game does not capture the *edge level* interactions between every pair of neighbors in a fixed network. Instead, it is a simplification of complicated reality and only attempts to capture the *average* or *mean* behavior of different populations with varying degrees. A key advantage of this model is that it provides a *scalable* model that enables us to study the effects of network properties on *aggregate* behavior of the players, resulting NEs and social optima, *regardless of* the network size.

A. Population game

We assume that the maximum degree among all players is $D_{\max} < \infty$. For each $d \in \{1, 2, \ldots, D_{\max}\} =: \mathcal{D}$, s_d denotes the *size* or *mass* of population with degree d, and $\mathbf{s} := \big(s_d;\ d \in \mathcal{D}\big)$ tells us the sizes of populations with varying degrees. Note that s_d does *not* necessarily represent the *number* of agents in population d; instead, an implicit modeling assumption of a population game is that each population consists of so many agents that a population $d \in \mathcal{D}$ can be approximated as a *continuum* of *mass* or *size* $s_d \in (0, \infty)$.

Pure action/strategy space – All players have the identical set of pure actions/strategies, which is denoted by $\mathcal{A}$. Each action in the action space $\mathcal{A}$ represents some *combination of security measures* a player can adopt. We assume that one of the actions is doing nothing, which we denote by a_1. For notational simplicity, we denote the number of available actions by $N = |\mathcal{A}|$. The costs of different actions are given by a mapping $c : \mathcal{A} \to \mathbb{R}_+ := [0, \infty)$ with $c(a_1) = 0$, i.e., the cost of adopting action $a \in \mathcal{A}$ is equal to $c(a)$. We assume that the costs of the actions are distinct.

Population states and social state – We denote by $\mathbf{x}_d = \big(x_{d,a};\ a \in \mathcal{A}\big)$, where $\sum_{a\in\mathcal{A}} x_{d,a} = s_d$, the *population state* of population d. The elements $x_{d,a}$, $a \in \mathcal{A}$, represent the mass or size of population d which employs action a. Let $\mathcal{X}_d := \big\{\mathbf{x}_d \in \mathbb{R}_+^N \mid \sum_{a\in\mathcal{A}} x_{d,a} = s_d\big\}$, $d \in \mathcal{D}$, where $\mathbb{R}_+ := [0, \infty)$, and $\mathcal{X} := \prod_{d\in\mathcal{D}} \mathcal{X}_d$. A social state $\mathbf{x} := (\mathbf{x}_d;\ d \in \mathcal{D}) \in \mathcal{X}$ consists of population states for all populations.

Cost function – The cost function of the game is denoted by $\mathbf{C} : \mathcal{X} \to \mathbb{R}^{N\cdot D_{\max}}$. For each social state $\mathbf{x} \in \mathcal{X}$, the cost of a player from population d playing action $a \in \mathcal{A}$ is equal to $\mathbf{C}_{d,a}(\mathbf{x})$. As we will show shortly, besides the cost

[2] We will use the words *nodes* and *players* interchangeably hereafter.

of investing in different security measures, our cost function also reflects (expected) losses from attacks.

As mentioned earlier, we are interested in exploring how network properties affect players' decisions. To this end, we model two different types of attacks players suffer from – *direct* and *indirect*. While the first type of attacks are not dependent on the network, the latter depends critically on the underlying network, allowing us to capture the desired *network effects* on players' choices.

a) Direct attacks: We assume that malicious attackers launch an attack against each player with probability τ_A, independently of other players.[3] We call this a *direct* attack. When a player experiences a direct attack, its expected losses from the attack depend on its action. When a player adopts action $a \in \mathcal{A}$, it is infected with probability $p(a) \in [0,1]$. Also, each time a player is infected, it incurs an (average) cost of L. Hence, the expected losses of a player from a single attack is $L(a) := L \cdot p(a)$.

It is shown [5] that, under some technical assumptions, the security breach probability or probability of loss is a *log-convex* (hence, strictly convex) decreasing function of the investments. Based on this finding, we introduce the following assumption on the infection probabilities $p(a)$, $a \in \mathcal{A}$.

Assumption 1: (i) We assume that the infection probabilities $p(a)$, $a \in \mathcal{A}$, are given by some *strictly convex, decreasing* function $g : \mathbb{R}_+ \to [0,1]$ of the cost. In other words, $p(a) = g(c(a))$ for all $a \in \mathcal{A}$. (ii) In addition, the actions are ordered by increasing cost $c(a)$ (equivalently, decreasing infection probability $p(a)$), and we denote the ℓth action by a_ℓ, $\ell \in \{1, 2, \ldots, N\} =: \mathcal{L}$.

b) Indirect attacks: Besides the direct attacks initiated by the attackers, a player may also experience *indirect* attacks from its neighbors that have sustained successful direct attacks and are infected. We assume that each infected node will launch an indirect attack against each of its neighbors with probability $\beta_I \in [0,1]$, independently of each other.

We assume that the infections from direct attacks spread only to immediate neighbors and do not propagate any further. While this may not be true with some attacks, we introduce this assumption for two reasons: First, it allows us to avoid the difficult issue of accurately modeling the propagation of infections in a network beyond the first hop, in particular the correlation in infection between neighbors of a victim due to the presence of triangles and other cycles in the network. We also point out that the precise manner in which infection spreads can vary drastically from one setting to another.

Secondly, it enables us to prove critical properties that are used to establish our *analytical* results on a comparison of network security under varying node degree distributions[4] and to prove the relation between the NEs of a population game and social optima. For instance, the convexity of the social cost (as a function of the social state) is crucial for proving that the risk exposure is identical at all social optima when there are two or more social optima (Theorem 5) and that the set of social optima coincides with the set of NEs of a modified population game (Theorem 8). However, such convexity of the social cost does not always hold when multi-hop propagation is allowed.

Even though we suspect that similar results continue to hold in many cases even when infections can propagate over multiple hops, unfortunately we have not yet been able to prove them. We will revisit this issue and discuss how relaxing this assumption may affect our model shortly.

We denote the mapping that yields the degree distribution of populations by $\mathbf{f} : \mathbb{R}_+^{D_{\max}} \to [0,1]^{D_{\max}}$, where

$$f_d(\mathbf{s}) = \frac{s_d}{\sum_{d' \in \mathcal{D}} s_{d'}}, \ \mathbf{s} \in \mathbb{R}_+^{D_{\max}} \text{ and } d \in \mathcal{D},$$

is the fraction of total population with degree d. Similarly, define $\mathbf{w} : \mathbb{R}_+^{D_{\max}} \to [0,1]^{D_{\max}}$, where

$$w_d(\mathbf{s}) = \frac{d \cdot s_d}{d_{\text{avg}}(\mathbf{s})}, \ \mathbf{s} \in \mathbb{R}_+^{D_{\max}} \text{ and } d \in \mathcal{D}, \tag{1}$$

and $d_{\text{avg}}(\mathbf{s}) := \sum_{d' \in \mathcal{D}} d' \cdot f_{d'}(\mathbf{s})$ is the average degree of nodes. From the above definition, $\mathbf{w}$ gives us the *weighted* node degree distribution of populations, where the weights are the degrees.

It is easy to show that both $\mathbf{f}$ and $\mathbf{w}$ are scale invariant. In other words, $\mathbf{f}(\mathbf{s}) = \mathbf{f}(\phi \cdot \mathbf{s})$ and $\mathbf{w}(\mathbf{s}) = \mathbf{w}(\phi \cdot \mathbf{s})$ for all $\phi > 0$. When there is no confusion, we write $\mathbf{f}$, $\mathbf{w}$, and d_{avg} in place of $\mathbf{f}(\mathbf{s})$, $\mathbf{w}(\mathbf{s})$, and $d_{\text{avg}}(\mathbf{s})$, respectively.

Let us explain the role of the mapping $\mathbf{w}$ briefly. Suppose that we fix a social state $\mathbf{x} \in \mathcal{X}$ and choose a player. The probability that a randomly picked neighbor of the player belongs to population $d \in \mathcal{D}$ can be approximated using w_d because it is proportional to the degree d [14].[5] Hence, the probability that the neighbor has degree d and plays action $a \in \mathcal{A}$ is approximately $w_d \cdot x_{d,a}/s_d$.

This degree-based model is also known as the Chung-Lu model in the literature [17] and has been used extensively in other existing studies, e.g., [20], [47], [48]. In particular, Watts in his seminal paper [47] utilized a similar degree-based model to study cascades of infection in a network with a given degree distribution. He demonstrated that the analytical results he derived using the generating function method based on this model closely match the numerical results he obtained using random graphs.

Based on the above observation, we approximate the probability that a player experiences an indirect attack from a *single* neighbor with

$$\gamma(\mathbf{x}) = \tau_A \cdot e(\mathbf{x}),$$

where

$$e(\mathbf{x}) = \beta_I \left(\sum_{d \in \mathcal{D}} w_d \left(\sum_{a \in \mathcal{A}} \frac{x_{d,a}}{s_d} p(a) \right) \right). \tag{2}$$

Note that $\sum_{d \in \mathcal{D}} w_d \left(\sum_{a \in \mathcal{A}} \frac{x_{d,a}}{s_d} p(a) \right)$ is the probability that a randomly selected neighbor of a node will be infected if it

[3] Our model can be easily altered to capture the intensity or frequencies of attacks instead, with appropriate changes to cost functions of the players.

[4] This comparison is carried out using the risk exposure defined in eq. (2).

[5] This implicitly assumes that the network is *neutral*. When a network is either assortative or disassortative, this assumption does not hold. However, we leave the effects of network assortativity for future study.

experiences a direct attack (which happens with probability τ_A in our model).

We call $e(\mathbf{x})$ the (risk) *exposure* from a neighbor at social state $\mathbf{x}$. It captures the conditional probability that a player faces an indirect attack from a single neighbor *given* that the neighbor suffers a direct attack. Thus, it allows us to quantify and compare the overall risk perceived by a node with a *fixed* degree, say $d \in \mathcal{D}$, at different social states or under different network settings. For this reason, we use it as a measure of *local* network security for comparison *from the viewpoint of a node with a fixed degree*.[6]

When the assumption that a successful direct attack spreads only to immediate neighbors is replaced by another weaker assumption that it can propagate only to neighbors within K hops, where $K \in \{2, 3, \ldots\}$, the risk exposure $e(\mathbf{x})$ will be higher, and the exact relation between $e(\mathbf{x})$ and K will depend on how infections are assumed to transmit over multiple hops in the network. However, the exposure seen by *all* players will scale in the identical manner with increasing K in our model. Thus, in this case, the end effects on our model would be similar to scaling the risk exposure experienced by the nodes.

We assume that the costs of a player due to multiple successful attacks are additive. The additivity of costs is reasonable in many scenarios, including the earlier examples of email viruses and corporate networks; each time a user is infected or its ID is stolen, the user will need to spend time and incur expenses to deal with the problem. Similarly, when a corporate network is infected, besides any financial losses or legal costs, the network operator will need to assess the damages and take corrective measures.

From these assumptions, the expected cost of a player from indirect attacks is proportional to $\gamma(\mathbf{x})$ and its degree. Hence, we adopt the following cost function for our population game: For any given social state $\mathbf{x} \in \mathcal{X}$, the cost of a player with degree $d \in \mathcal{D}$ playing $a \in \mathcal{A}$ is given by

$$\mathbf{C}_{d,a}(\mathbf{x}) = \tau_A \left(1 + d \cdot e(\mathbf{x})\right) L(a) + c(a). \tag{3}$$

Note that $\tau_A(1 + d \cdot e(\mathbf{x}))$ is the *expected* number of attacks experienced by a node with degree d. Also, it is clear from (2) and (3) that the cost of a player depends on both its own security measures and those of other players via the risk exposure $e(\mathbf{x})$.

As mentioned in Section I, we focus on the NEs of population games as an approximation to nodes' behavior in practice. A social state $\mathbf{x}^\star$ is an NE if it satisfies the condition that, for all $d \in \mathcal{D}$ and $a \in \mathcal{A}$,

$$x^\star_{d,a} > 0 \text{ implies } \mathbf{C}_{d,a}(\mathbf{x}^\star) = \min_{a' \in \mathcal{A}} \mathbf{C}_{d,a'}(\mathbf{x}^\star). \tag{4}$$

The existence of an NE of a population game is always guaranteed [41, Theorem 2.1.1, p. 24].

Some of questions we are interested in exploring with help of the population game model described in this section are:

- Q1 Is there a unique NE? If not, are there common properties among all NEs?
- Q2 How does the node degree distribution affect NEs and social optima and their respective network security and social costs?
- Q3 What is the POA/POS? How does the degree distribution of nodes shape the POA/POS?
- Q4 Is there any relation between an NE and social optimum? If so, how can we exploit it to internalize players' externalities in order to improve network security and lower social cost?

[6]To the best of our knowledge, there are no standard metrics experts agree on for quantifying network security.

B. Preliminaries

There is an important observation we should mention. From (2) and (3), the cost function also has a scale invariance property, i.e., $\mathbf{C}(\mathbf{x}) = \mathbf{C}(\phi \cdot \mathbf{x})$ for all $\phi > 0$. This scale invariance property of the cost function implies the following: Suppose that $\mathcal{NE}^\star$ denotes the set of NEs for a given population size vector $\mathbf{s}^1$. Then, the set of NEs for another population size vector $\mathbf{s}^2 = \phi \cdot \mathbf{s}^1$ for some $\phi > 0$ is given by $\{\phi \cdot \tilde{\mathbf{x}} \mid \tilde{\mathbf{x}} \in \mathcal{NE}^\star\}$. This in turn means that the set of NEs scaled by the inverse of the total population size is the same for all population size vectors with the identical degree distribution. As a result, it suffices to study the NEs for population size vectors whose sum is equal to one, i.e., $\sum_{d \in \mathcal{D}} s_d = 1$. For this reason, we impose the following assumption in the remainder of the paper.

Assumption 2: The population size vectors are normalized so that the total population size is one.

Let $\Psi : \mathbb{R}_+ \to 2^{\mathcal{A}}$, where

$$\Psi(\nu) = \arg\min_{a \in \mathcal{A}} \Big(\tau_A(1 + \nu)L(a) + c(a)\Big). \tag{5}$$

In other words, given the expected number of *indirect* attacks ν, the mapping $\Psi(\nu)$ gives us the set of optimal actions that minimize the expected cost.

Define $\nu_{\max} := D_{\max} \cdot \beta_I \cdot p(a_1)$. We first introduce a lemma that tells us that, under the assumed settings, there are $1 \le \ell_\star \le \ell^\star \le N$ such that, for every $a \in \{a_{\ell_\star}, \ldots, a_{\ell^\star}\}$, there exists a nonempty interval $J_a \subset [0, \nu_{\max}]$ so that, if the (expected) number of indirect attacks experienced by a player falls in the interval, then action a is an optimal action for the player.

For every $a \in \mathcal{A}$, define a function $\check{\mathbf{C}}_a : \mathbb{R} \to \mathbb{R}$, where

$$\check{\mathbf{C}}_a(\nu) = \tau_A \; L(a) + c(a) + \tau_A \; L(a) \; \nu. \tag{6}$$

It is clear that the functions $\check{\mathbf{C}}_a$, $a \in \mathcal{A}$, are obtained from the cost function in (3) after replacing $d \cdot e(\mathbf{x})$ with ν. In other words, $\check{\mathbf{C}}_a(\nu)$ provides us with the cost of a player from population d playing action a when $d \cdot e(\mathbf{x}) = \nu$.[7]

Let $\nu^\star_0 = -\infty$ and $\nu^\star_N = \infty$ and, for each $\ell \in \{1, 2, \ldots, N-1\} =: \mathcal{L}^-$, define $\nu^*_\ell \in \mathbb{R}$ to be the x-coordinate of the intersection of $\check{\mathbf{C}}_{a_\ell}$ and $\check{\mathbf{C}}_{a_{\ell+1}}$.

[7]Here, we allow ν to be negative for convenience. However, the expected number of indirect attacks $d \cdot e(\mathbf{x})$ in our population game model will be nonnegative.

Lemma 1: (i) The x-coordinates of the intersection points, i.e., ν_ℓ^*, increase with ℓ. In other words, $-\infty = \nu_0^* < \nu_1^* < \nu_2^* < \cdots < \nu_{N-1}^* < \nu_N^* = \infty$. (ii) For each $\ell \in \mathcal{L}$, define

$$\mathcal{J}_{a_\ell} = [\nu_{\ell-1}^\star, \nu_\ell^\star] \cap [0, \nu_{\max}].$$

If $\nu \in \mathcal{J}_{a_\ell}$, then $a_\ell \in \Psi(\nu)$.

Proof: A proof of the lemma is given in Appendix A. ∎

An important implication of Lemma 1 is the following corollary.

Corollary 1: The infection probability of an optimal action does not increase with the expected number of attacks. In other words, given $0 < \nu_1 < \nu_2 \le \nu_{\max}$, we have

$$\min\{p(a) \mid a \in \Psi(\nu_1)\} \ge \max\{p(a') \mid a' \in \Psi(\nu_2)\}$$

or, equivalently,

$$\max\{\ell \in \mathcal{L} \mid a_\ell \in \Psi(\nu_1)\} \le \min\{\ell' \in \mathcal{L} \mid a_{\ell'} \in \Psi(\nu_2)\}.$$

As we will see shortly, this corollary leads to several interesting findings reported in the following sections.

IV. Population games and social optimum

In this section, we first explore the structural properties of both the NEs of population games and social optima and examine the relation between the weighted node degree distribution and the risk exposure at NEs and social optima.

A. Population games

For notational convenience, for each $a \in \mathcal{A}$, we define $\mathcal{A}^+(a) := \{a' \in \mathcal{A} \mid p(a') \le p(a)\}$ in the remainder of the paper. In other words, if $a = a_\ell$, then $\mathcal{A}^+(a) = \{a_\ell, a_{\ell+1}, \ldots, a_N\}$. The following theorem establishes a degree threshold for each available action.

Theorem 1: Let $\mathbf{s} \in \mathbb{R}_+^{D_{\max}}$ be a population size vector and $\mathbf{x}^\star \in \mathcal{X}$ be a corresponding NE. Suppose that $x_{d,a}^\star > 0$ for some $d \in \mathcal{D}$ and $a \in \mathcal{A}$. Then, for all $d' > d$,

$$\sum_{a' \in \mathcal{A}^+(a)} x_{d',a'}^\star = s_{d'}.$$

In other words, no player with a larger degree selects an action with higher infection probability.

Proof: A proof is provided in Appendix B. ∎

The following theorem establishes the uniqueness of the risk exposure at the NEs of the population game. In addition, it proves the uniqueness of an NE under a mild technical condition.

Theorem 2: Suppose that $\mathbf{x}^1$ and $\mathbf{x}^2$ are two NEs for a population size vector $\mathbf{s}$. Then, $e(\mathbf{x}^1) = e(\mathbf{x}^2)$. Moreover, assume that, for every $\mu \in [0, e_{\max}]$, where $e_{\max} = \beta_I \cdot p(a_1)$, we have $|\Psi(d \cdot \mu)| = 1$ for all $d \in \mathcal{D}$ except for at most one population. Then, there exists a unique NE of the population game.

Proof: Please see Appendix C for a proof. ∎

Since we are interested in understanding how the degree distribution of nodes affects the security measured by the risk exposure and it is identical at all NEs by Theorem 2, for our purpose, we can take any NE of the population game. With a little abuse of notation, we denote an arbitrary NE of the population game for a given population size by $\mathbf{N}(\mathbf{s})$. The next theorem sheds some light on how the *weighted* node degree distribution shapes the local security seen by individual nodes with fixed degrees.

Theorem 3: Let $\mathbf{s}^1$ and $\mathbf{s}^2$ be two population size vectors that satisfy

$$\sum_{\ell=1}^{d} w_\ell(\mathbf{s}^1) \le \sum_{\ell=1}^{d} w_\ell(\mathbf{s}^2) \quad \text{for all } d \in \mathcal{D} \tag{7}$$

and $\mathbf{x}^i = \mathbf{N}(\mathbf{s}^i)$, $i = 1, 2$. Then, $e(\mathbf{x}^1) \le e(\mathbf{x}^2)$. In addition, suppose that the condition in Theorem 2 holds. For every $a \in \mathcal{A}$, let $d_a^i := \min\{d \in \mathcal{D} \mid \sum_{a' \in \mathcal{A}^+(a)} x_{d,a'}^i > 0\}$, $i = 1, 2$. If the set on the right-hand side (RHS) is empty, we set $d_a^i = D_{\max} + 1$. Then, $d_a^1 \ge d_a^2$ for all $a \in \mathcal{A}$.

Proof: A proof is given in Appendix D. ∎

The first part of Theorem 3 states that, as the weighted node degree distribution becomes larger, the risk exposure at an NE tends to decline. What is somewhat surprising from the second part of the theorem is that the risk exposure drops even though each population d invests *less* in security, i.e., in cheaper security options that are less effective in lowering the infection probability. The intuition behind these perhaps counterintuitive findings is that, as the degrees of neighbors rise (with an increasing weighted node degree distribution), a node with a fixed degree, say d, experiences reduced risk from its neighbors because nodes with higher degrees are better protected (Theorem 1). As a consequence, the node reduces its own security investments, thereby explaining the second part of the theorem.

The claims in Theorem 3 do not always hold when we replace the weighted node degree distributions in (7) with the node degree distributions of two population sizes. In other words, we can find two population size vectors $\tilde{\mathbf{s}}^1$ and $\tilde{\mathbf{s}}^2$ such that

$$\sum_{\ell=1}^{d} \tilde{s}_\ell^1 \le \sum_{\ell=1}^{d} \tilde{s}_\ell^2 \quad \text{for all } d \in \mathcal{D},$$

but the claims in Theorem 3 fail to hold.

The following lemma provides a sufficient condition for (7).

Lemma 2: Suppose that two population size vectors $\mathbf{s}^1$ and $\mathbf{s}^2$ satisfy

$$\frac{s_d^2}{s_d^1} \ge \frac{s_{d+1}^2}{s_{d+1}^1} \quad \text{for all } d \in \mathcal{D}^- := \{1, 2, \ldots, D_{\max} - 1\}. \tag{8}$$

Then, the condition (7) in Theorem 3 is satisfied.

Proof: Please see Appendix E for a proof. ∎

The finding in Lemma 2 can be applied to several well known families of distributions. For example, consider a family of (truncated) power law degree distributions $\{\mathbf{s}^\alpha;\ \alpha \in \mathbb{R}_+\}$, where $s_d^\alpha \propto d^{-\alpha}$, $d \in \mathcal{D}$. Suppose that $\alpha_1 \le \alpha_2$. Then, one can easily show that $\mathbf{s}^{\alpha_1}$ and $\mathbf{s}^{\alpha_2}$ satisfy (8) as follows:

$$\frac{d^{-\alpha_2}}{d^{-\alpha_1}} = d^{-(\alpha_2 - \alpha_1)} \ge (d+1)^{-(\alpha_2 - \alpha_1)} = \frac{(d+1)^{-\alpha_2}}{(d+1)^{-\alpha_1}}$$

because $\alpha_2 - \alpha_1 \geq 0$. Hence, the monotonicity properties of the degree threshold and the risk exposure shown in Theorem 3 are true for the family of power law degree distributions.

B. Social optimum

We define the overall social cost at social state $\mathbf{x} \in \mathcal{X}$ to be the sum of (i) expected losses from attacks and (ii) the costs of security measures adopted by players, which is given by

$$C(\mathbf{x}) = \sum_{d \in \mathcal{D}} \left(\sum_{a \in \mathcal{A}} x_{d,a} \cdot \mathbf{C}_{d,a}(\mathbf{x}) \right). \tag{9}$$

The goal of the social player (SP) is to minimize the social cost in (9) over $\mathcal{X}$:

SP-OPT PROBLEM:

$$\min_{\mathbf{y} \in \mathcal{X}} \; C(\mathbf{y})$$

Suppose that $\mathbf{y}^\star$ is a minimizer of the social cost. The following theorem suggests that the minimizer possesses a degree threshold for each available action, similar to those of NEs.

Theorem 4: Suppose that $y^\star_{d,a} > 0$ for some $d \in \mathcal{D}$ and $a \in \mathcal{A}$. Then, for all $d' > d$,

$$\sum_{a' \in \mathcal{A}^+(a)} y^\star_{d',a'} = s_{d'}.$$

Proof: See Appendix F for a proof. ∎

Unfortunately, the social optimum is not necessarily unique.[8] However, our next theorem suggests that, even though there may be multiple social optima, they all achieve the same risk exposure. Thus, for the reason explained earlier, we can still examine how node degrees affect network security at a social optimum.

Theorem 5: Suppose that $\mathbf{y}^{1\star}$ and $\mathbf{y}^{2\star}$ are two minimizers of the social cost. Then, $e(\mathbf{y}^{1\star}) = e(\mathbf{y}^{2\star})$.

Proof: A proof is provided in Appendix G. ∎

We use $\mathbf{y}^\star(\mathbf{s})$ to denote an arbitrary minimizer of the social cost for fixed population size vector $\mathbf{s}$. When there is no confusion, we simply denote it by $\mathbf{y}^\star$. The following theorem tells us that the risk exposure at social optima tends to diminish as the weighted node degree distribution becomes larger.

Theorem 6: Let $\mathbf{s}^1$ and $\mathbf{s}^2$ be two population size vectors that satisfy

$$\sum_{\ell=1}^{d} w_\ell(\mathbf{s}^1) \leq \sum_{\ell=1}^{d} w_\ell(\mathbf{s}^2) \;\; \text{for all } d \in \mathcal{D}. \tag{10}$$

Then, $e\big(\mathbf{y}^\star(\mathbf{s}^1)\big) \leq e\big(\mathbf{y}^\star(\mathbf{s}^2)\big)$.

Proof: Please see Appendix H for a proof. ∎

Theorems 3 and 6 state that the risk exposure at both NEs and social optima tends to diminish as the weighted node degree distribution becomes larger. Hence, our results suggest that both in the distributed case with selfish agents and in the centralized case with SP, higher network connectivity will likely improve network security measured by risk exposure.

At the same time, our findings in [29] reveal that the *global* or *network-level* security may in fact deteriorate; a key observation of [29] is that as the weighted node degree distribution becomes larger, the cascade probability (i.e., the probability that a random single infection leads to a cascade of infection to a large number of nodes) rises. Hence, together, these findings suggest that, as the weighted node degree distribution gets larger, individual nodes with fixed degrees may perceive improved *local* security as the average number of attacks they see falls, whereas the *global* network security degrades in that even a single infection may spread to a large number of other nodes in the network with higher probability.

V. Internalization of Externalities

An important question in the field of IDS is how one can encourage selfish players to make adequate investments in security in order to enhance overall security. In other words, what types of incentive mechanisms can be employed, for instance, with the help of regulatory policies, to *incentivize* selfish players so that they would invest more in security than they would otherwise at an NE? In this section, we offer a partial answer to this question by exploring how we may be able to *internalize* externalities [46].

To this end, we first compare the risk exposures at an NE and a social optimum and show that the selfish nature of players leads to under-investments in security. Then, we illustrate the relation between a social optimum and an NE of the population game, which offers a possible way of correctly internalizing the externalities caused by players [46].

Theorem 7: Fix the population size vector $\mathbf{s}$. Let $\mathbf{x}^\star = \mathbf{N}(\mathbf{s})$ and $\mathbf{y}^\star = \mathbf{y}^\star(\mathbf{s})$. Then, $e(\mathbf{y}^\star) \leq e(\mathbf{x}^\star)$.

Theorem 7 affirms that free riding by some players at NEs causes a degradation in network security. We will first introduce our main finding of this section before presenting the proof of Theorem 7.

We proceed to illustrate how the externalities produced by players, which are partially responsible for under-investments in security at NEs, can be internalized to reduce the social cost and enhance network security. In general, a main challenge to internalizing externalities is that, in many cases, it is difficult to correctly estimate the externalities players cause to other players. However, we will show that, in the scenarios under consideration, we can send a correct signal to the players by *using information that is already available to the players*.

To illustrate this, we first investigate the relation between a social optimum and an NE of the population game. Consider the following modified population game with a slightly different cost function $\hat{\mathbf{C}} : \mathcal{X} \to \mathbb{R}^{N \cdot D_{\max}}$, where

$$\hat{\mathbf{C}}_{d,a}(\mathbf{x}) = \tau_A(1 + 2\; d \cdot e(\mathbf{x}))L(a) + c(a) \tag{11}$$

for all $d \in \mathcal{D}$ and $a \in \mathcal{A}$. Note that the only difference between the cost function in (3) and the above modified cost function in (11) is that the expected loss from *indirect* attacks a player bears, namely $\tau_A \; d \; e(\mathbf{x}) \; L(a)$, is doubled.

[8] In the following section, we will offer a hint as to why there may be multiple minimizers of the social cost in the general case.

Denote the set of NEs of the population game with the altered cost function in (11) by $\mathcal{NE}^m(\mathbf{s})$.

Theorem 8: The set of minimizers of the social cost and $\mathcal{NE}^m(\mathbf{s})$ coincide. In other words,

$$\mathcal{NE}^m(\mathbf{s}) = \arg\min_{\mathbf{y}\in\mathcal{X}} \; C(\mathbf{y}).$$

Proof: A proof is provided in Appendix I. ∎

Theorem 8 sheds some light on the structural relation between a social optimum and an NE. Also, it hints at how we may strengthen network security, for example, by levying penalties or taxes on the players for indirect attacks they suffer. In other words, the expected damages and losses players undergo as a result of *indirect* attacks coming from their neighbors are equal to the negative network externalities they produce. Thus, they can be used to internalize the externalities so as to achieve the social optimum [46].

Theorem 8 also offers some intuition behind Theorem 7; since the infection probability at an optimal action chosen by players at an NE is nondecreasing in the risk they see from indirect attacks, players would overall invest at least as much in security at an NE of the modified population game as they would at an NE of the original population game. This is because the risk from indirect attacks is doubled in the modified population game. Since an NE of the modified population game is a minimizer of the social cost by Theorem 8, this leads to Theorem 7. Building upon this intuition, we provide a proof of Theorem 7 in Appendix J.

Finally, Theorem 8 presents a possible explanation as to why the NEs of population games and social optima possess similar properties as hinted by Theorems 1 through 6; social optima can be viewed as the NEs of related population games with modified cost functions.

VI. Price of Anarchy/Stability

Our findings in the previous section suggest that the selfish nature of the players will likely result in *under-investments* in security and, as a result, the overall network security will degrade and the social cost will increase. In light of these findings, a natural question that arises is: How good/bad is an NE compared to the social optimum?

Inefficiency of NEs is well documented in many cases, e.g., [18], [36, Chap. 17-21], and can be easily demonstrated using a simple example of the *Prisoner's Dilemma* [40]. Over the last decade or so, there has been much interest in understanding just how inefficient an NE could be compared to the system optimum and quantifying the suboptimality brought on by the selfish nature of players [26].

Two popular ways to measure the inefficiency of NE(s) are POA and POS. The POA (resp. POS) is defined to be the *largest* (resp. *smallest*) ratio between the social cost at an NE and the minimum social cost. The POS can be viewed as the minimum price one needs to pay for *stability* among the players so that no player would have an incentive to deviate from its strategy unilaterally.

Recall that, in our population games, all NEs achieve the same social cost by virtue of Theorem 2 and (9) and, hence, POA and POS are identical. In this section, we investigate how large the POA can be in our population games and whether or not there exists a tight upper bound on POA. In particular, we are interested in understanding the relation between the (upper bound on) POA and the average node degree.

Define

$$\ell_\star = \min\left\{\ell \in \mathcal{L}^- \;\middle|\; \frac{c(a_{\ell+1}) - c(a_\ell)}{L(a_\ell) - L(a_{\ell+1})} \geq \tau_A\right\}.$$

If the set on the RHS is empty, we set $\ell_\star = N$. The importance of $\ell_\star$ is that, for all $\ell < \ell_\star$, we have $\nu^\star_\ell < 0$ and, hence, $\mathcal{J}_{a_\ell} = \emptyset$. Therefore, for all $\ell < \ell_\star$ and $\nu \in [0, \nu_{\max}]$, we have $\check{\mathbf{C}}_{a_\ell}(\nu) > \check{\mathbf{C}}_{a_{\ell_\star}}(\nu)$, and consequently $x^\star_{d,a_\ell} = y^\star_{d,a_\ell} = 0$ for all $\ell < \ell_\star$.

Theorem 9: Let $\mathbf{s}$ be a population size vector. Then,

$$\frac{C\big(\mathbf{N}(\mathbf{s})\big)}{C\big(\mathbf{y}^\star(\mathbf{s})\big)} \leq 1 + d_{\text{avg}} \cdot \beta_I \cdot p(a_{\ell_\star}). \tag{12}$$

Proof: A proof is given in Appendix K ∎

The upper bound on POA in (12) is tight in the sense that there are (perhaps artificial) cases where the POA is equal to the bound. A numerical example with binary security choices is provided in [29, Section V.C], which illustrates this point.[9] The intuition (from the proof of the theorem in Appendix K) is that, in the binary case with $\mathcal{A} = \{a_1, a_2\}$, the upper bound can be achieved when (a) all nodes choose a_1 at the NE of the population game and (b) they select a_2 at the social optimum and a node is perfectly protected when adopting a_2, i.e., $p(a_2) = 0$. Hence, the upper bound on POA in (12) tells us that the POA is an affine function of the average degree of nodes in such cases. Furthermore, our numerical studies indicate that, even when the bound is not achieved, i.e., the POA is strictly smaller than the bound in (12), the POA tends to increase almost linearly with the average node degree, suggesting that the POA in many cases rises with the increasing network connectivity among nodes.

As pointed out in [29], there is an interesting trade-off one can observe: When node degrees vary significantly as in a power law degree distribution often observed in both natural and engineered networks [3], the network is held together by nodes with high degrees. Such networks are shown to be robust against random attacks, but are more vulnerable to coordinated attacks targeting high-degree nodes [15], [16]. A potential remedy to this problem is to increase the connectivity of the network, hence, the average node degree. But, our findings here and in [29] suggest that increasing network connectivity is likely to lead to a higher social cost and greater POA as well as larger probability of an infection spreading to a large number of other nodes.

VII. Conclusions

We studied the effects of (weighted) node degree distributions on security investments in IDS games. We demonstrated several structural properties exhibited by both the NEs of population games and social optima. Our findings suggest that,

[9] The example in [29] has some small separation between the POA and its upper bound so as to improve the readability of the plot. However, the example can be modified to achieve the upper bound as well.

under a mild technical assumption, the risk seen by a node with a fixed degree tends to abate with increasing network connectivity. Furthermore, the externalities produced by security investments of some players reduce the incentive for other players to invest in security, leading to *free riding* observed in related studies. Finally, we illustrated an interesting relation between social optima and the NEs of population games, which also suggests a possible explanation for their common properties and a means of enhancing network security.

Appendix A
Proof of Lemma 1

From its definition, ν_ℓ^*, $\ell \in \mathcal{L}^-$, is the unique value that satisfies $\check{\mathbf{C}}_{a_\ell}(\nu_\ell^*) = \check{\mathbf{C}}_{a_{\ell+1}}(\nu_\ell^*)$. Using the expression in (6) for $\check{\mathbf{C}}$, we obtain

$$\nu_\ell^* = -1 + \frac{c(a_{\ell+1}) - c(a_\ell)}{\tau_A(L(a_\ell) - L(a_{\ell+1}))}. \tag{13}$$

Since $L(a_\ell) = L \cdot g(c(a_\ell))$, where (i) $c(a_\ell)$ increases with ℓ and (ii) g is assumed to be strictly convex and decreasing, $(c(a_{\ell+1}) - c(a_\ell))/(L(a_\ell) - L(a_{\ell+1}))$ strictly increases with ℓ. This proves the first claim of the lemma. The second claim of the lemma is a direct consequence of the first claim and Assumption 1.

Appendix B
Proof of Theorem 1

We consider two cases: (i) $\sum_{a' \in \mathcal{A}^+(a)} x^\star_{d,a'} = s_d$ and (ii) $\sum_{a' \in \mathcal{A}^+(a)} x^\star_{d,a'} < s_d$. In the first case, the claim follows directly from Lemma 1 because $d' \cdot e(\mathbf{x}) > d \cdot e(\mathbf{x})$. In the second case, note that $\sum_{a' \in \mathcal{A}^+(a)} x^\star_{d,a'} < s_d$ is possible only if (a) $d \cdot e(\mathbf{x}^\star)$ is equal to ν_ℓ^* for some $\ell \in \mathcal{L}^-$, and both $x^\star_{d,a_\ell}$ and $x^\star_{d,a_{\ell+1}}$ are strictly positive. In this case, because $d' \cdot e(\mathbf{x}^\star) > d \cdot e(\mathbf{x}^\star)$, no player from population d' will choose a_ℓ as a best response at $\mathbf{x}^\star$ (as $\mathbf{C}_{d',a_\ell}(\mathbf{x}^\star) > \mathbf{C}_{d',a_{\ell+1}}(\mathbf{x}^\star)$ from the assumption that $p(a_l)$ strictly decreases with l) and instead choose action(s) only from the set $\{a_{\ell+1}, \ldots, a_N\}$.

Appendix C
Proof of Theorem 2

Suppose that the claim is false and there exist two distinct NEs $\mathbf{x}^1$ and $\mathbf{x}^2$ such that $e(\mathbf{x}^1) < e(\mathbf{x}^2)$. Then, by Corollary 1, the indices of actions chosen by a population should not be higher at $\mathbf{x}^1$ than at $\mathbf{x}^2$. In other words, for all $d \in \mathcal{D}$ and $\ell \in \mathcal{L}^-$, we have

$$\sum_{\ell'=\ell}^{N} x^1_{d,a_{\ell'}} \leq \sum_{\ell'=\ell}^{N} x^2_{d,a_{\ell'}}.$$

This inequality in turn implies $e(\mathbf{x}^1) \geq e(\mathbf{x}^2)$ according to (2) because $p(a_\ell)$ decreases with ℓ, thereby contradicting the earlier assumption $e(\mathbf{x}^1) < e(\mathbf{x}^2)$.

The second part of the theorem is a direct consequence of the imposed assumption and the first part of the theorem. Since the equilibrium risk exposure is identical at all NEs from the first part, only populations with two best responses at an NE can choose from them. However, by the assumption in Theorem 2, there could be at most one such population, say $d^* \in \mathcal{D}$, for which the set of best responses contains two pure actions and, for all other populations, there must be a *unique* best response they will select at the NEs. Thus, if we do not have $x^1_{d^*,a} = x^2_{d^*,a}$ for all $a \in \mathcal{A}$, we cannot satisfy $e(\mathbf{x}^1) = e(\mathbf{x}^2)$ because $p(a) \neq p(a')$ if $a \neq a'$, which contradicts the first part of the theorem.

Appendix D
Proof of Theorem 3

Suppose that the first part of theorem is false and $e(\mathbf{x}^1) > e(\mathbf{x}^2)$. By Corollary 1, this implies, for every $d \in \mathcal{D}$,

$$\frac{1}{s^1_d} \sum_{\ell=1}^{N} x^1_{d,a_\ell}\, p(a_\ell) \leq \frac{1}{s^2_d} \sum_{\ell=1}^{N} x^2_{d,a_\ell}\, p(a_\ell). \tag{14}$$

Using the definition of risk exposure in (2),

$$\begin{aligned} e(\mathbf{x}^2) &= \beta_I \sum_{d \in \mathcal{D}} w^2_d \left(\sum_{\ell=1}^{N} \frac{x^2_{d,a_\ell}}{s^2_d} p(a_\ell) \right) \\ &\geq \beta_I \sum_{d \in \mathcal{D}} w^2_d \left(\sum_{\ell=1}^{N} \frac{x^1_{d,a_\ell}}{s^1_d} p(a_\ell) \right) \qquad (15) \\ &\geq \beta_I \sum_{d \in \mathcal{D}} w^1_d \left(\sum_{\ell=1}^{N} \frac{x^1_{d,a_\ell}}{s^1_d} p(a_\ell) \right) \qquad (16) \\ &= e(\mathbf{x}^1), \end{aligned}$$

which contradicts the earlier assumption. The first inequality in (15) follows from (14), and the second inequality in (16) is a consequence of the condition (7) in Theorem 3 and Corollary 1.

The second part of the theorem follows from Corollary 1 and the first part of the theorem. Suppose that the claim is not true and there exists $a^* = a_{\ell^*} \in \mathcal{A}$ such that $d^1_{a^*} < d^2_{a^*}$. We will show that this results in a contradiction by considering two disjoint cases:

(i) $e(\mathbf{x}^1) < e(\mathbf{x}^2)$ – We have $d \cdot e(\mathbf{x}^1) < d \cdot e(\mathbf{x}^2)$ for all $d \in \mathcal{D}$, and Corollary 1 states that the index of action chosen by each population at $\mathbf{x}^2$ cannot be smaller than that at $\mathbf{x}^1$, i.e., $\min\{\ell \mid x^2_{d,a_\ell} > 0\} \geq \max\{\ell \mid x^1_{d,a_\ell} > 0\}$. Therefore, it immediately implies $d^1_a \geq d^2_a$ for all $a \in \mathcal{A}$.

(ii) $e(\mathbf{x}^1) = e(\mathbf{x}^2)$ – In this case, $d \cdot e(\mathbf{x}^1) = d \cdot e(\mathbf{x}^2)$ for all $d \in \mathcal{D}$. Hence, since $d^1_{a^*} < d^2_{a^*}$ by assumption, we know $|\Psi(d^1_{a^*} \cdot e(\mathbf{x}^i))| > 1$ and, from the assumption in the theorem, the following holds.

- $|\Psi(d \cdot e(\mathbf{x}^i))| = 1$, for all $d \neq d^1_{a^*}$ and $i = 1, 2$, and consequently

$$\frac{x^1_{d,a}}{s^1_d} = \frac{x^2_{d,a}}{s^2_d} \tag{17}$$

  for all $d \neq d^1_{a^*}$ and $a \in \mathcal{A}$.
- $d^1_{a^*} \cdot e(\mathbf{x}^1)$ is equal to $\nu^*_{\ell^*}$ and

$$\sum_{a \in \mathcal{A}} \frac{x^1_{d^1_{a^*},a}}{s^1_{d^1_{a^*}}} p(a) < \sum_{a \in \mathcal{A}} \frac{x^2_{d^1_{a^*},a}}{s^2_{d^1_{a^*}}} p(a) \tag{18}$$

because population $d^1_{a^*}$ chooses action(s) only from $\{a_1, \ldots, a_{\ell^*-1}\}$ at $\mathbf{x}^2$.

As a consequence of these observations, we have

$$\begin{aligned} e(\mathbf{x}^2) &= \beta_I \left(\sum_{d\in\mathcal{D}} w_d^2 \left(\sum_{a\in\mathcal{A}} \frac{x^2_{d,a}}{s_d^2} p(a) \right) \right) \\ &\geq \beta_I \left(\sum_{d\in\mathcal{D}} w_d^1 \left(\sum_{a\in\mathcal{A}} \frac{x^2_{d,a}}{s_d^2} p(a) \right) \right) \qquad (19) \\ &> \beta_I \left(\sum_{d\in\mathcal{D}} w_d^1 \left(\sum_{a\in\mathcal{A}} \frac{x^1_{d,a}}{s_d^1} p(a) \right) \right) \qquad (20) \\ &= e(\mathbf{x}^1), \end{aligned}$$

which contradicts the assumption $e(\mathbf{x}^1) = e(\mathbf{x}^2)$. The first inequality (19) follows from the condition (7) in the theorem (which implies that $\mathbf{w}^1$ is stochastically larger than $\mathbf{w}^2$) and Corollary 1 (i.e., the security investments do not decrease with increasing degree), and the second inequality in (20) is a consequence of (17) and (18).

Appendix E
Proof of Lemma 2

The following lemma will be used to prove Lemma 2.

Lemma 3: Suppose that $\mathbf{a} = (a_\ell; \ell = 1, \ldots, K)$ and $\mathbf{b} = (b_\ell; \ell = 1, \ldots, K)$ are two finite sequences of nonnegative real numbers of length $K > 1$ and satisfy

$$\frac{b_{\ell+1}}{a_{\ell+1}} \leq \frac{b_\ell}{a_\ell} \quad \text{for all } \ell = 1, \ldots, K-1. \qquad (21)$$

Then,

$$\frac{\sum_{\ell=1}^k b_\ell}{\sum_{\ell=1}^k a_\ell} \geq \frac{\sum_{\ell=1}^K b_\ell}{\sum_{\ell=1}^K a_\ell} \quad \text{for all } k = 1, \ldots, K. \qquad (22)$$

Proceeding with the proof of Lemma 2, recall that the condition (8) in Lemma 2 states

$$\frac{(d+1)\ s^2_{d+1}}{(d+1)\ s^1_{d+1}} \leq \frac{d \cdot s_d^2}{d \cdot s_d^1} \quad \text{for all } d \in \mathcal{D}^-. \qquad (23)$$

From the definition of $\mathbf{w}_d$, the condition (7) is equivalent to

$$\frac{\sum_{\ell=1}^d \ell \cdot s_\ell^2}{\sum_{\ell=1}^d \ell \cdot s_\ell^1} \geq \frac{\sum_{\ell=1}^{D_{\max}} \ell \cdot s_\ell^2}{\sum_{\ell=1}^{D_{\max}} \ell \cdot s_\ell^1} \quad \text{for all } d \in \mathcal{D}. \qquad (24)$$

Let $\mathbf{a} = (a_d;\ d \in \mathcal{D})$ and $\mathbf{b} = (b_d;\ d \in \mathcal{D})$, where $a_d = d \cdot s_d^1$ and $b_d = d \cdot s_d^2$. The inequalities in (24) can be rewritten in terms of $\mathbf{a}$ and $\mathbf{b}$ as

$$\frac{\sum_{\ell=1}^d b_\ell}{\sum_{\ell=1}^d a_\ell} \geq \frac{\sum_{\ell=1}^{D_{\max}} b_\ell}{\sum_{\ell=1}^{D_{\max}} a_\ell} \quad \text{for all } d \in \mathcal{D}. \qquad (25)$$

Moreover, (23) implies $(b_{d+1}/a_{d+1}) \leq (b_d/a_d)$, $d \in \mathcal{D}^-$. The claim of Lemma 2 in (25) now follows directly from Lemma 3.

Appendix F
Proof of Theorem 4

Suppose that the theorem is false and there exists $d' > d$ such that $\sum_{a' \in \mathcal{A}^+(a)} y^\star_{d',a'} < s_{d'}$. Assume $a = a_{\ell'}$. Then, clearly there exists $\ell^* < \ell'$ such that $y^\star_{d',a^*_\ell} > 0$. We will show that this contradicts the assumption that $\mathbf{y}^\star$ minimizes the social cost.

Let ϵ be a constant satisfying $0 < \epsilon < \min\{y^\star_{d,a'_\ell}, y^\star_{d',a^*_\ell}\}$. Then, clearly $s_{d'} - y^\star_{d',a'_\ell} > \epsilon$ and $s_d - y^\star_{d,a^*_\ell} > \epsilon$.

Let $\mathbf{u}_{d,\ell} \in \mathbb{R}^{N \cdot D_{\max}}$, $d \in \mathcal{D}$ and $\ell \in \mathcal{L}$, denote the zero-one vector, whose only nonzero element is the one that corresponds to population d and action a_ℓ. Define

$$\mathbf{y}^+ = \mathbf{y}^\star + \epsilon(\mathbf{u}_{d',\ell'} - \mathbf{u}_{d,\ell'}) + \epsilon(\mathbf{u}_{d,\ell^*} - \mathbf{u}_{d',\ell^*}).$$

From its construction, the total investments in security does not change from $\mathbf{y}^\star$ to $\mathbf{y}^+$ because, for every $\ell \in \mathcal{L}$, $\sum_{d\in\mathcal{D}} y^\star_{d,a_\ell} = \sum_{d\in\mathcal{D}} y^+_{d,a_\ell}$. However, we can show $e(\mathbf{y}^+) < e(\mathbf{y}^\star)$ as follows.

$$\begin{aligned} &e(\mathbf{y}^\star) - e(\mathbf{y}^+) \\ &= \frac{\beta_I \cdot \epsilon}{d_{\text{avg}}} \big(d'(p(a_{\ell^*}) - p(a_{\ell'})) + d(p(a_{\ell'}) - p(a_{\ell^*})) \big) \\ &= \frac{\beta_I \cdot \epsilon}{d_{\text{avg}}} (d' - d)(p(a_{\ell^*}) - p(a_{\ell'})) > 0 \end{aligned}$$

As a result, after a little algebra, we get $C(\mathbf{y}^+) < C(\mathbf{y}^\star)$, which is a contradiction.

Appendix G
Proof of Theorem 5

Suppose that the claim is not true and there exist two distinct minimizers $\mathbf{y}^1$ and $\mathbf{y}^2$ such that $e(\mathbf{y}^1) \neq e(\mathbf{y}^2)$. Let $\alpha \in (0,1)$ and $\mathbf{y}^3 = \alpha \cdot \mathbf{y}^1 + (1-\alpha)\mathbf{y}^2$. We will show that $C(\mathbf{y}^3) < C(\mathbf{y}^1) = C(\mathbf{y}^3)$, leading to a contradiction.

First, note that $e(\mathbf{y}^3) = \alpha \cdot e(\mathbf{y}^1) + (1-\alpha) e(\mathbf{y}^2)$ because the risk exposure is a linear function of $\mathbf{y}$. From (9), we have

$$\begin{aligned} &C(\mathbf{y}^3) \\ &= \sum_{d\in\mathcal{D}} \left(\sum_{a\in\mathcal{A}} y^3_{d,a} \Big(\tau_A(1 + d \cdot e(\mathbf{y}^3)) L(a) + c(a) \Big) \right) \qquad (26) \end{aligned}$$

and

$$\begin{aligned} &\alpha \cdot C(\mathbf{y}^1) + (1-\alpha) C(\mathbf{y}^2) \\ &= \alpha \left(\sum_{d\in\mathcal{D}} \left(\sum_{a\in\mathcal{A}} y^1_{d,a} \big(\tau_A(1 + d \cdot e(\mathbf{y}^1)) L(a) + c(a) \big) \right) \right) \\ &\quad + (1-\alpha) \left(\sum_{d\in\mathcal{D}} \left(\sum_{a\in\mathcal{A}} y^2_{d,a} \Big(\tau_A(1 + d \cdot e(\mathbf{y}^2)) L(a) \right. \right. \\ &\qquad \left. \left. + c(a) \big) \Big) \right). \qquad (27) \end{aligned}$$

Subtracting (26) from (27),

$$\begin{aligned} &\alpha \cdot C(\mathbf{y}^1) + (1-\alpha) C(\mathbf{y}^2) - C(\mathbf{y}^3) \\ &= \tau_A \sum_{d\in\mathcal{D}} d \Big(\sum_{a\in\mathcal{A}} \big(\alpha \cdot y^1_{d,a}\ e(\mathbf{y}^1) + (1-\alpha) y^2_{d,a}\ e(\mathbf{y}^2) \\ &\qquad - y^3_{d,a}\ e(\mathbf{y}^3) \big) L(a) \Big). \end{aligned}$$

Making use of the equalities

$$e(\mathbf{y}^1) - e(\mathbf{y}^3) = (1-\alpha)(e(\mathbf{y}^1) - e(\mathbf{y}^2))$$

and

$$e(\mathbf{y}^2) - e(\mathbf{y}^3) = -\alpha(e(\mathbf{y}^1) - e(\mathbf{y}^2)),$$

we obtain

$$\begin{aligned}&\alpha \cdot C(\mathbf{y}^1) + (1-\alpha)C(\mathbf{y}^2) - C(\mathbf{y}^3)\\ &= \tau_A \alpha(1-\alpha)(e(\mathbf{y}^1) - e(\mathbf{y}^2)) \sum_{d\in\mathcal{D}} d\Big(\sum_{a\in\mathcal{A}} (y^1_{d,a} - y^2_{d,a})L(a)\Big).\end{aligned}$$

Substituting

$$e(\mathbf{y}^1) - e(\mathbf{y}^2) = \frac{\beta_I}{d_{\rm avg}} \sum_{d\in\mathcal{D}} d\Big(\sum_{a\in\mathcal{A}} (y^1_{d,a} - y^2_{d,a})p(a)\Big),$$

we get

$$\begin{aligned}&\alpha \cdot C(\mathbf{y}^1) + (1-\alpha)C(\mathbf{y}^2) - C(\mathbf{y}^3)\\ &= \frac{\beta_I\ \tau_A\ \alpha(1-\alpha)L}{d_{\rm avg}} \left(\sum_{d\in\mathcal{D}} d\Big(\sum_{a\in\mathcal{A}} (y^1_{d,a} - y^2_{d,a})p(a)\Big)\right)^2\\ &\geq 0.\end{aligned}$$

Note that the equality holds if and only if $\sum_{d\in\mathcal{D}} d\Big(\sum_{a\in\mathcal{A}} (y^1_{d,a} - y^2_{d,a})p(a)\Big) = 0$. From (2), for $i = 1, 2$,

$$e(\mathbf{y}^i) = \frac{\beta_I}{d_{\rm avg}} \sum_{d\in\mathcal{D}} d \sum_{a\in\mathcal{A}} y^i_{d,a} \cdot p(a). \tag{28}$$

Thus, it is clear that $\sum_{d\in\mathcal{D}} d\Big(\sum_{a\in\mathcal{A}} (y^1_{d,a} - y^2_{d,a})p(a)\Big) = 0$ if any only if $e(\mathbf{y}^1) = e(\mathbf{y}^2)$.

Appendix H
Proof of Theorem 6

Suppose that the claim is false and $e(\mathbf{y}^1) > e(\mathbf{y}^2)$. We show that this leads to a contradiction. The condition (10) in the theorem tells us that if

$$\sum_{\ell'=\ell}^{N} \frac{y^1_{d,a_{\ell'}}}{s^1_d} \geq \sum_{\ell'=\ell}^{N} \frac{y^2_{d,a_{\ell'}}}{s^2_d} \quad \text{for all } d\in\mathcal{D} \text{ and } \ell\in\mathcal{L},$$

then $e(\mathbf{y}^1) \leq e(\mathbf{y}^2)$. Therefore, there must exist $d^\star \in \mathcal{D}$ and $\ell^\star \in \mathcal{L}$ such that

$$\sum_{\ell=\ell^\star}^{N} \frac{y^1_{d^\star,a_\ell}}{s^1_{d^\star}} < \sum_{\ell=\ell^\star}^{N} \frac{y^2_{d^\star,a_\ell}}{s^2_{d^\star}}. \tag{29}$$

Assume that $y^2_{d^\star,a_{\ell^\star}} > 0$. Otherwise, we can consider the smallest $\ell' \geq \ell^\star$ satisfying $y^2_{d^\star,a_{\ell'}} > 0$. Inequality in (29) implies that there exists $\ell^+ < \ell^\star$ such that $y^1_{d^\star,a_{\ell^+}} > 0$.

Fix $0 < \delta < \min\{y^1_{d^\star,a_{\ell^+}}, y^2_{d^\star,a_{\ell^\star}}, s^1_d - y^1_{d^\star,a_{\ell^\star}}, s^2_{d^\star} - y^2_{d^\star,a_{\ell^+}}\}$ and let $\bar{\mathbf{y}}^1 = \mathbf{y}^1 + \delta\left(\mathbf{u}_{d^\star,\ell^\star} - \mathbf{u}_{d^\star,\ell^+}\right)$ and $\bar{\mathbf{y}}^2 = \mathbf{y}^2 - \delta\left(\mathbf{u}_{d^\star,\ell^\star} - \mathbf{u}_{d^\star,\ell^+}\right)$. Because $e(\mathbf{y}^2) - e(\bar{\mathbf{y}}^2) = \beta_I\ d^\star\ \delta\big(p(a_{\ell^+}) - p(a_{\ell^\star})\big)/d_{\rm avg} > 0$ from (28), Theorem 5 states $C(\mathbf{y}^2) < C(\bar{\mathbf{y}}^2)$. We will now prove that, for sufficiently small positive δ,

$$C(\bar{\mathbf{y}}^1) - C(\mathbf{y}^1) \leq C(\mathbf{y}^2) - C(\bar{\mathbf{y}}^2) < 0, \tag{30}$$

leading to a contradiction that $\mathbf{y}^1$ is not a minimizer.

Using (9), we obtain

$$\begin{aligned}&C(\mathbf{y}^2) - C(\bar{\mathbf{y}}^2) - (C(\bar{\mathbf{y}}^1) - C(\mathbf{y}^1))\\ &= \sum_{d\in\mathcal{D}} \Big(\sum_{a\in\mathcal{A}} y^2_{d,a} \cdot \mathbf{C}_{d,a}(\mathbf{y}^2) - \bar{y}^2_{d,a} \cdot \mathbf{C}_{d,a}(\bar{\mathbf{y}}^2)\\ &\qquad -\bar{y}^1_{d,a} \cdot \mathbf{C}_{d,a}(\bar{\mathbf{y}}^1) + y^1_{d,a} \cdot \mathbf{C}_{d,a}(\mathbf{y}^1)\Big)\\ &= \tau_A \sum_{d\in\mathcal{D}} d\Big(\sum_{a\in\mathcal{A}} \big(y^2_{d,a}(e(\mathbf{y}^2) - e(\bar{\mathbf{y}}^2))\\ &\qquad +y^1_{d,a}(e(\mathbf{y}^1) - e(\bar{\mathbf{y}}^1))\big)L(a)\Big) \qquad (31)\\ &\quad +\tau_A \sum_{d\in\mathcal{D}} d\Big(\sum_{a\in\mathcal{A}} \big((y^2_{d,a} - \bar{y}^2_{d,a})e(\bar{\mathbf{y}}^2)\\ &\qquad +(y^1_{d,a} - \bar{y}^1_{d,a})e(\bar{\mathbf{y}}^1))\big)L(a)\Big). \qquad (32)\end{aligned}$$

First,

$$(32) = \delta\ \tau_A\ d^\star(e(\bar{\mathbf{y}}^2) - e(\bar{\mathbf{y}}^1))\big(L(a_{\ell^\star}) - L(a_{\ell^+})\big).$$

Since $e(\mathbf{y}^1) > e(\mathbf{y}^2)$ by assumption, for sufficiently small δ, we have $e(\bar{\mathbf{y}}^1) > e(\bar{\mathbf{y}}^2)$. Also, because $\ell^+ < \ell^\star$, we have $L(a_{\ell^+}) > L(a_{\ell^\star})$ and, hence, (32) > 0.

Second, we can show (31) $= 0$ as follows. Note that

$$\begin{aligned}e(\mathbf{y}^2) - e(\bar{\mathbf{y}}^2) &= \frac{\beta_I}{d_{\rm avg}} d^\star\ \delta(p(a_{\ell^\star}) - p(a_{\ell^+}))\\ &= e(\bar{\mathbf{y}}^1) - e(\mathbf{y}^1).\end{aligned}$$

Substituting these in (31), we get

$$\begin{aligned}(31) &= \beta_I\ \tau_A\ d^\star\ \delta\ \big(p(a_{\ell^+}) - p(a_{\ell^\star})\big)\\ &\qquad \times \left(\sum_{d\in\mathcal{D}} d \sum_{a\in\mathcal{A}} \left(\frac{y^1_{d,a}}{d^1_{\rm avg}} - \frac{y^2_{d,a}}{d^2_{\rm avg}}\right)\right)\\ &= \beta_I\ \tau_A\ d^\star\ \delta\ \big(p(a_{\ell^+}) - p(a_{\ell^\star})\big)\\ &\qquad \times \left(\sum_{d\in\mathcal{D}} d\left(\frac{s^1_d}{d^1_{\rm avg}} - \frac{s^2_d}{d^2_{\rm avg}}\right)\right)\\ &= 0.\end{aligned}$$

This completes the proof of (30).

Appendix I
Proof of Theorem 8

Any minimizer $\mathbf{y}^\star$ of the social cost must satisfy the Karush-Kuhn-Tucker (KKT) first-order condition [7]: There exist KKT multipliers $\boldsymbol{\lambda} = (\lambda_{d,a};\ d\in\mathcal{D} \text{ and } a\in\mathcal{A}) \in \mathbb{R}_+^{N\cdot D_{\max}}$, $\boldsymbol{\mu} = (\mu_{d,a};\ d\in\mathcal{D} \text{ and } a\in\mathcal{A}) \in \mathbb{R}_+^{N\cdot D_{\max}}$ and $\boldsymbol{\eta} = (\eta_d;\ d\in\mathcal{D}) \in \mathbb{R}^{D_{\max}}$ such that, for all $d\in\mathcal{D}$ and $a\in\mathcal{A}$,

1) $\bigtriangledown_{d,a} C(\mathbf{y}^\star) = \lambda_{d,a} - \mu_{d,a} + \eta_d$; and
2) $\lambda_{d,a}\ y_{d,a} = 0$ and $\mu_{d,a}(s_d - y_{d,a}) = 0$.

From (9), (2) and (3), after a little algebra, we obtain

$$\bigtriangledown_{d,a} C(\mathbf{y}^\star) = \tau_A(1 + 2\ d\ e(\mathbf{y}^\star))L(a) + c(a).$$

Hence, the first part of the KKT condition states that $\tau_A(1 + 2\ d\ e(\mathbf{y}^\star))L(a) + c(a) = \lambda_{d,a} - \mu_{d,a} + \eta_d$ for all $d\in\mathcal{D}$ and

$a \in \mathcal{A}$. Because the KKT multipliers $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ are nonnegative, this implies

$$\begin{aligned}&\tau_A(1+2\ d\ e(\mathbf{y}^\star))L(a)+c(a)\\&=\min_{a'\in\mathcal{A}}\big(\tau_A(1+2\ d\ e(\mathbf{y}^\star))L(a')+c(a')\big)\ \text{ if } y^\star_{d,a}>0.\end{aligned}$$

However, by definition any social state $\mathbf{x} \in \mathcal{X}$ that satisfies this condition is an NE of the modified population game with the cost function given by (11), thereby proving that $\mathbf{y}^\star$ is an NE of the modified population game.

To prove the converse, note that because the social cost is a convex function as shown in the proof of Theorem 5 (Appendix G) and the inequality constraints are given by affine functions, the KKT conditions are also sufficient for optimality [7]. It is easy to see that any NE of the altered population game satisfies the KKT condition and, hence, is a minimizer of the social cost.

Appendix J
Proof of Theorem 7

Assume that Theorem 7 is not true and $e(\mathbf{y}^\star) > e(\mathbf{x}^\star)$. This necessarily implies that there exists $d \in \mathcal{D}$ and $\ell^\dagger \in \mathcal{L}$ such that

$$\sum_{\ell'=1}^{\ell^\dagger} y^\star_{d,a_{\ell'}} > \sum_{\ell'=1}^{\ell^\dagger} x^\star_{d,a_{\ell'}}. \tag{33}$$

Otherwise, we would have $e(\mathbf{y}^\star) \le e(\mathbf{x}^\star)$. The inequality in (33) means that there exists $\ell^* > \ell^\dagger$ with $x^\star_{d,a_{\ell^*}} > 0$. Without loss of generality, we assume $y^\star_{d,a_{\ell^\dagger}} > 0$; if not, we can consider the largest $\ell' < \ell^\dagger$ with $y^\star_{d,a_{\ell'}} > 0$.

From the definition of NE in (4),

$$\begin{aligned}&\tau_A(1+d\ e(\mathbf{x}^\star))L(a_{\ell^*})+c(a_{\ell^*})\\&=\min_{a\in\mathcal{A}}\ \big(\tau_A(1+d\ e(\mathbf{x}^\star))L(a)+c(a)\big)\end{aligned} \tag{34}$$

We also know from the proof of Theorem 8 in Appendix I

$$\begin{aligned}&\tau_A(1+2\ d\ e(\mathbf{y}^\star))L(a_{\ell^\dagger})+c(a_{\ell^\dagger})\\&=\min_{a\in\mathcal{A}}\ \big(\tau_A(1+2\ d\ e(\mathbf{y}^\star))L(a)+c(a)\big).\end{aligned} \tag{35}$$

We can show that (34) and (35) together lead to a contradiction when $e(\mathbf{y}^\star) > e(\mathbf{x}^\star)$ as follows. Eqs. (34) and (35) imply

$$\begin{aligned}&\tau_A(1+d\ e(\mathbf{x}^\star))L(a_{\ell^*})+c(a_{\ell^*})\\&\le\tau_A(1+d\ e(\mathbf{x}^\star))L(a_{\ell^\dagger})+c(a_{\ell^\dagger})\end{aligned}$$

and

$$\begin{aligned}&\tau_A(1+2\ d\ e(\mathbf{y}^\star))L(a_{\ell^\dagger})+c(a_{\ell^\dagger})\\&\le\tau_A(1+2\ d\ e(\mathbf{y}^\star))L(a_{\ell^*})+c(a_{\ell^*}).\end{aligned}$$

These two inequalities yield

$$\begin{aligned}&\tau_A\ d(2\ e(\mathbf{y}^\star)-e(\mathbf{x}^\star))L(a_{\ell^\dagger})\\&\le\tau_A\ d(2\ e(\mathbf{y}^\star)-e(\mathbf{x}^\star))L(a_{\ell^*}).\end{aligned}$$

Because $e(\mathbf{y}^\star) > e(\mathbf{x}^\star)$ by assumption, the above inequality means $L(a_{\ell^\dagger}) \le L(a_{\ell^*})$, which is a contradiction since $\ell^\dagger < \ell^*$.

Appendix K
Proof of Theorem 9

Let $\mathbf{x}^\star = \mathbf{N}(\mathbf{s})$ and $\mathbf{y}^\star = \mathbf{y}^\star(\mathbf{s})$. We will first upper bound the difference $C(\mathbf{x}^\star) - C(\mathbf{y}^\star)$ and then find a lower bound to $C(\mathbf{y}^\star)$, which will give us the upper bound on POA in the theorem.

Using the definition of the social cost in (9), subtracting $C(\mathbf{y}^\star)$ from $C(\mathbf{x}^\star)$, we get

$$\begin{aligned}&C(\mathbf{x}^\star)-C(\mathbf{y}^\star)\\&=\sum_{d\in\mathcal{D}}\sum_{a\in\mathcal{A}}(x^\star_{d,a}-y^\star_{d,a})\,(\tau_A L(a)+c(a))\\&\quad+\tau_A\sum_{d\in\mathcal{D}}\sum_{a\in\mathcal{A}}d\cdot L(a)\big(x^\star_{d,a}e(\mathbf{x}^\star)-y^\star_{d,a}e(\mathbf{y}^\star)\big).\end{aligned} \tag{36}$$

Lemma 4: If $\ell_\star < N$, then $\tau_A \cdot L(a_\ell) + c(a_\ell)$ is nondecreasing in $\ell \in \{\ell_\star, \ell_\star + 1, \dots, N\}$.

Proof: Suppose that there exists $\ell' \in \{\ell_\star, \dots, N-1\}$ such that $\tau_A \cdot L(a_{\ell'}) + c(a_{\ell'}) > \tau_A \cdot L(a_{\ell'+1}) + c(a_{\ell'+1})$ or, equivalently, $(c(a_{\ell'+1}) - c(a_{\ell'}))/(L(a_{\ell'}) - L(a_{\ell'+1})) < \tau_A$. Recall from the proof of Lemma 1 in Appendix A that $(c(a_{\ell+1}) - c(a_\ell))/(L(a_\ell) - L(a_{\ell+1}))$ strictly increases with ℓ. Since $\ell_\star$ satisfies $(c(a_{\ell_\star+1}) - c(a_{\ell_\star}))/(L(a_{\ell_\star}) - L(a_{\ell_\star+1})) \ge \tau_A$ from its definition, we must have $(c(a_{\ell+1}) - c(a_\ell))/(L(a_\ell) - L(a_{\ell+1})) \ge \tau_A$ for all $\ell \ge \ell_\star$, leading to a contradiction. ∎

By Theorems 7 and 8 and Corollary 1, we have, for all $d \in \mathcal{D}$ and $\ell' \in \mathcal{L}$,

$$\sum_{\ell=\ell'}^{N} y^\star_{d,a_\ell} \ge \sum_{\ell=\ell'}^{N} x^\star_{d,a_\ell}.$$

Together with Lemma 4, this inequality implies that the first term in (36) is less than or equal to zero. Thus, letting $e_\star = \beta_I \cdot p(a_{\ell_\star})$ and $e_{\min} = \beta_I \cdot p(a_N) = \beta_I \cdot \min_{a\in\mathcal{A}} p(a)$, we obtain

$$\begin{aligned}&C(\mathbf{x}^\star)-C(\mathbf{y}^\star)\\&\le\tau_A\sum_{d\in\mathcal{D}}\sum_{a\in\mathcal{A}}d\cdot L(a)\big(x^\star_{d,a}e(\mathbf{x}^\star)-y^\star_{d,a}e(\mathbf{y}^\star)\big)\\&\le\tau_A\ L(a_{\ell_\star})\ e_\star\sum_{d\in\mathcal{D}}d\sum_{a\in\mathcal{A}}x^\star_{d,a}\\&\qquad-\tau_A\ L(a_N)\ e_{\min}\sum_{d\in\mathcal{D}}d\sum_{a\in\mathcal{A}}y^\star_{d,a}\\&\le\tau_A\ d_{\text{avg}}\ L(a_{\ell_\star})\ e_\star-\tau_A\ d_{\text{avg}}\ L(a_N)\ e_{\min}\\&\le\tau_A\ d_{\text{avg}}\ L(a_{\ell_\star})\ e_\star.\end{aligned} \tag{37}$$

In addition, we obtain the following lower bound on $C(\mathbf{y}^\star)$ from the definition of the social cost in (9) and Lemma 4.

$$\begin{aligned}C(\mathbf{y}^\star)&\ge\sum_{d\in\mathcal{D}}\sum_{a\in\mathcal{A}}y^\star_{d,a}\,(\tau_A L(a)+c(a))\\&\ge\tau_A\ L(a_{\ell_\star})+c(a_{\ell_\star}),\end{aligned} \tag{38}$$

where the second inequality follows from Lemma 4.

Using the bounds in (37) and (38), we get

$$\begin{aligned}\frac{C(\mathbf{x}^\star)}{C(\mathbf{y}^\star)}&=1+\frac{C(\mathbf{x}^\star)-C(\mathbf{y}^\star)}{C(\mathbf{y}^\star)}\\&\le 1+d_{\text{avg}}\cdot e_\star.\end{aligned}$$

REFERENCES

[1] National Vulnerability Database. http://nvd.nist.gov.

[2] *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*, Sep. 2010.

[3] R. Albert, H. Jeong and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, 406:378-382, Jul. 2000.

[4] R. Anderson and T. Moore, "Information security economics - and beyond," Lecture Notes in Computer Science Volume 4622, pp 68-91, 2007.

[5] Y. Baryshnikov, "IT security investment and Gordon-Loev's $1/e$ rule," Proc. of the 11th Annual Workshop on the Economics of Information Security (WEIS), Berlin (Germany), Jun. 2012.

[6] N. Beale, D.G. Rand, H. Battey, K. Croxson, R.M. May and M.A. Nowak, "Individual versus systemic risk and the regulator's dilemma," *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*, 108(31):12647-12652, Aug. 2011.

[7] D.P. Bertsekas, *Nonlinear Programming*, Athena Scientific, 1995.

[8] L. Bilge and T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world," Proc. of ACM Conference on Computer and Communications Security (CCS), Oct. 2012.

[9] R. Böhme and G. Schwartz, "Modeling cyber-insurance: towards a unifying framework," Proc. of the 4th Workshop on the Economics of Information Security (WEIS), Cambridge (MA), Jun. 2010.

[10] J.C. Bolot and M. Lelarge, "A new perspective on Internet security using insurance," Proc. of IEEE INFOCOM, Phoenix (AZ), Apr. 2008.

[11] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine*, pp. 42-49, Jan. 2013.

[12] F. Caccioli, T.A. Catanach, and J.D. Farmer, "Heterogeneity, correlations and financial contagion," arXiv:1109.1213, Sep. 2011.

[13] F. Caccioli, T.A. Catanach, and J.D. Farmer, "Stability analysis of financial contagion due to overlapping portfolios," arXiv:1210.5987, Oct. 2012.

[14] D.S. Callaway, M.E.J. Newman, S.H. Strogatz and D.J. Watts, "Network robustness and fragility: percolation and random graphs," *Physical Review Letters*, 85(25):5468-5471, Dec. 2000.

[15] R. Cohen, K. Erez, D. ben-Avraham and S. Havlin, "Resilience of the Internet to random breakdowns," *Physical Review Letters*, 85(21):4626-4628, Nov. 2000.

[16] R. Cohen, K. Erez, D. ben-Avraham and S. Havlin, "Breakdown of the Internet under intentional attack," *Physical Review Letters*, 86(16):3682-3685, Apr. 2001.

[17] F. Chung and L. Lu, "Connected components in random graphs with given expected degree sequences," *Annals of Combinatorics*, 6(2):125-145, Nov. 2002.

[18] P. Dubey, "Inefficiency of Nash equilibria," *Mathematics of Operations Research*, 11(1):1-8, 1986.

[19] K.G. Gkonis and H.N. Psaraftis, "Container transportation as an interdependent security problem," *Journal of Transportation Security*, 3(4):197-211, Dec. 2010.

[20] J.P. Gleeson and D.J. Cahalane, "Seed size strongly affects cascades on random networks," *Physical Review E*, 75, 056103, 2007.

[21] J. Grossklags, N. Christin and J. Chuang, "Secure or insecure? a game-theoretic analysis of information security games," Proc. of of the 17th International Conference on World Wide Web, pp. 209-218, Beijing (China), Apr. 2008.

[22] G. Heal, H.C. Kunreuther and P.R. Orszag, "Interdependent security: Implications for homeland security policy and other areas," Brookings Policy Brief Series, #108, Oct. 2002.

[23] G. Heal and H. Kunreuther, "Interdependent security: a general model," National Bureau of Economic Research (NBER) Working Paper No. 10706, Aug. 2004.

[24] L. Jiang, V. Anantharam and J. Walrand, "How bad are selfish investments in network security?", *IEEE/ACM Transactions on Networking*, 19(2):549-560, Apr. 2011.

[25] M. Kearns and L.E. Ortiz, "Algorithms for interdependent security games," *Advances in Neural Information Processing Systems 16*, 2003.

[26] E. Koutsoupias and C.H. Papadimitriou, "Worst-case equilibria," Proc. of the 16th Annual Symposium on Theoretical Aspects of Computer Science (STACS), pp. 404-413, 1999.

[27] H. Kunreuther and G. Heal, "Interdependent Security," *The Journal of Risk and Uncertainty*, 26(2/3):231-249, 2003.

[28] H.C. Kunreuther and E.O. Michel-Kerjan, "Assessing, managing and benefiting from global interdependent risks: The case of terrorism and natural disasters," *Global Business and the Terrorist Threat*, edited by H.W. Richardson, P. Gordon and J.E. Moore, Edward Elgar Publishing, 2009.

[29] R.J. La, "Interdependent security with strategic agents and global cascade," accepted for publication in *IEEE/ACM Trans. on Networking*. A preprint available at http://www.ece.umd.edu/∼hyongla/publication.shtml.

[30] A. Laszka, M. Felegyhazi and L. Buttyán, "A survey of interdependent information security games," *ACM Computing Surveys*, 47(2):23:1-23:38, Jan. 2015.

[31] M. Lelarge and J. Bolot, "A local mean field analysis of security investments in networks," Proc. of the 3rd International Workshop on Economics of Networked Systems (NetEcon), pp. 25-30, Seattle (WA), Aug. 2008.

[32] M. Lelarge and J. Bolot, "Economic incentives to increase security in the Internet: the case for insurance," Proc. of IEEE INFOCOM, Rio de Janeiro (Brazil), Apr. 2009.

[33] R.A. Miura-Ko, B. Yolken, N. Bambos and J. Mitchell, "Security investment games of interdependent organizations," Proc. of Annual Allerton Conference, pp. 252-260, Monticello (IL), Sep. 2008.

[34] R.A. Miura-Ko, B. Yolken, J. Mitchell and N. Bambos, "Security decision-making among interdependent organizations," Proc. of the 21st IEEE Computer Security Foundations Symposium, pp. 66-80, Pittsburgh (PA), Jun. 2008.

[35] P. Naghizadeh and M. Liu, "Closing the price of anarchy gap in the interdependent security game," Information Theory and Applications (ITA) Workshop, San Diego (CA), Feb. 2014.

[36] N. Nisan, T. Roughgarden, É. Tardos, and V.V. Vazirani, *Algorithmic Game Theory*, Cambridge University Press, 2007.

[37] H. Ogut, N. Menon and S. Raghunathan, "Cyber insurance and IT security investment: impact of interdependent risk," Proc. of the 4th Workshop on the Economics of Information Security (WEIS), Cambridge (MA), Jun. 2005.

[38] R. Pal and P. Hui, "Modeling internet security investments: tackling topological information uncertainty," Proc. of the 2nd International Conference on Decision and Game Theory for Security (GameSec), pp. 239-257, College Park (MD), Nov. 2011.

[39] R. Pastor-Satorras and A. Vespignani, "Epidemics and immunization in scale-free networks," *Handbook of Graphs and Networks: From the Genome to the Internet*, Wiley, 2005.

[40] W. Poundstone, *Prisoner's Dilemma*, Anchor, 1993.

[41] W.H. Sandholm *Population Games and Evolutionary Dynamics*, The MIT Press, 2010.

[42] C.M. Schneider, M. Tamara, H. Shlomo, H.J. Herrmann, "Suppressing epidemics with a limited amount of immunization units," *Physical Review E*, **84**, 061911, Dec. 2011.

[43] M. Shaked and J.G. Shanthikumar, *Stochastic Orders*, Springer Series in Statistics, Springer, 2007.

[44] C. Shapiro and H.R. Varian, *Information Rules*, Harvard Business School Press, 1999.

[45] H.R. Varian, "System reliability and free riding," *Economics of Information Security*, 12:1-15, 2004.

[46] H.R. Varian, *Microeconomic Analysis*, 3rd edition, W.W. Norton & Company, 1992.

[47] D.J. Watts, "A simple model of global cascades on random networks," *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*, 99(9):5766-5771, Apr. 2002.

[48] O. Yağan and V. Gligor, "Analysis of complex contagions in random multiplex networks," *Physical Review E*, 86, 036103, Sep. 2012.

PLACE PHOTO HERE

Richard J. La received his B.S.E.E. from the University of Maryland, College Park in 1994 and M.S. and Ph.D. degrees in Electrical Engineering from the University of California, Berkeley in 1997 and 2000, respectively. From 2000 to 2001 he was with the Mathematics of Communication Networks group at Motorola Inc,. Since 2001 he has been on the faculty of the Department of Electrical and Computer Engineering at the University of Maryland, where he is currently an Associate Professor.

He received an NSF CAREER award in 2003 and is currently an associate editor for IEEE Transactions on Mobile Computing and an editor for IEEE Communications Surveys and Tutorials.