Automatica 49 (2013) 186–192

Contents lists available at SciVerse ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Brief paper

# Security of interdependent and identical networked control systems☆

Saurabh Amin [a,1], Galina A. Schwartz [b], S. Shankar Sastry [b]

[a] Department of Civil and Environmental Engineering, MIT, USA

[b] Department of Electrical Engineering and Computer Sciences, UC Berkeley, USA

ARTICLE INFO

*Article history:*
Received 17 July 2010
Received in revised form
21 June 2012
Accepted 20 July 2012
Available online 29 October 2012

*Keywords:*
Interdependent security
Nash games
Network reliability
Networked control systems
System security

ABSTRACT

This article studies security decisions of identical plant-controller systems, when their security is interdependent due to network induced risks. Each plant is modeled by a discrete-time stochastic linear system, with the systems controlled over a shared communication network. We formulate the problem of security choices of the individual system operators (also called players) as a non-cooperative game. We consider a two-stage game, in which on the first stage the players decide whether to invest in security or not; and on the second stage, they apply control inputs to minimize the average operational costs. We characterize the equilibria of the game, which includes the determination of the individually optimal security levels. Next, we solve the problem of finding the socially optimal security levels. The presence of interdependent security causes a negative externality, and the individual players tend to under invest in security relative to the social optimum. This leads to a gap between the individual and the socially optimal security levels for a wide range of security costs. From our results, regulatory impositions to incentivize higher security investments are desirable.



## 1. Introduction

We approach the security of networked control systems (NCS) from a game-theoretic perspective. While the usefulness of game theory methods in modeling cyber-security issues in networked systems is well-established (Alpcan & Başar, 2011), the novelty of our approach is integration of ideas from economics of security (Anderson, Böhme, Clayton, & Moore, 2008; Varian, 2004) and networked control theory (Hespanha, Naghshtabrizi, & Xu, 2007). In particular, we build on earlier literature that deals with the interdependence of security-related risks (Heal & Kunreuther, 2004; Honeyman, Schwartz, & Van Assche, 2007; Miura-Ko, Yolken, Mitchell, & Bambos, 2008b; Mounzer, Alpcan, & Bambos, 2010), and investigate security choices of the individual NCS operators when security interdependencies are present due to network induced risks.

Several factors exacerbate the severity of the losses caused by security interdependencies. First, NCS are subject to information technology (IT) insecurities due to the prevalence of commercial off-the-shelf devices (sensors and actuators). These IT devices are prone to correlated failures, including software flaws and hardware malfunctions (Cárdenas, Amin, & Sastry, 2008). Such failures can result in the loss of NCS stability and performance (Antsaklis & Baillieul, 2007). Second, since the NCS will soon govern the operation of critical infrastructures, their interdependencies can be exploited by cyber criminals. So far, such occurrences have been recorded only a few times (e.g., Langner, 2011), but the presence of cyber-security risks to NCS is well documented (Owens, Dam, & Lin, 2009), and cannot be ignored. The risks of such rare but extremely disruptive events are similar to risks of terrorist attacks (Bier, Oliveros, & Samuelson, 2007), and it is established that private mitigation of such risks fails (Heal & Kunreuther, 2004). Thus, government interventions are likely to be required.

We model the problem of operator's security choice as a non-cooperative two-stage game between $m \geqslant 2$ plant-controller systems (or players). Each of these players is modeled in a standard NCS setting (Imer, Yüksel, & Başar, 2006; Schenato, Sinopoli, Franceschetti, Poolla, & Sastry, 2007). In the first stage, each player has a binary choice of investing versus not investing into enhanced security measures at his plant. In the second stage, players choose optimal control inputs for their respective plants. Each player's objective is to minimize the average long-term cost, which is comprised of the plant operating costs and the cost of security measures. We compare the individually optimal choices with that of the social planner, whose objective is to minimize the sum of aggregate costs of all the players (which includes the costs of security measures). The approach in this article compliments

☆ The material in this paper was partially presented at the First International Conference on Decision and Game Theory for Security (GameSec 2010), November 22–23, 2010, Berlin, Germany. This paper was recommended for publication in revised form by Associate Editor Hideaki Ishii under the direction of Editor Ian R. Petersen.

*E-mail addresses:* amins@mit.edu (S. Amin), schwartz@eecs.berkeley.edu (G.A. Schwartz), sastry@coe.berkeley.edu (S. Shankar Sastry).

[1] Tel.: +1 617 253 8003; fax: +1 617 253 8978.

0005-1098/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.automatica.2012.09.007

the existing and growing literature on strategies for security investments in networked systems (Alpcan & Başar, 2011; Cavusoglu, Mishra, & Raghunathan, 2005; Miura-Ko, Yolken, Bambos, & Mitchell, 2008a).

We use a probabilistic failure model of packet losses in both sensor and control channels of NCS. Earlier literature has considered independent and memoryless failure models to analyze NCS stability and performance under unreliable communication networks (Gupta, Dana, Hespanha, Murray, & Hassibi, 2009; Imer et al., 2006). In this article, we introduce an additional *interdependence term* aiming to account for network insecurity. This term, which reflects security driven failures, is dependent on security choices of other systems. Our modeling of security interdependencies builds on Heal and Kunreuther's interdependent security model (Heal & Kunreuther, 2003, 2004). We refer the readers to Hofmann (2007); Mounzer et al. (2010) for similar approaches.

The importance of network externalities for incentives to invest in security has been noted and modeled by numerous researchers (e.g., see Anderson et al., 2008, Böhme & Schwartz, 2010 and the references therein). The relevance of these effects for critical infrastructures, and in particular, the provision of electricity was raised in Anderson and Fuloria (2009). To the best of our knowledge, the existing literature lacks a formal model of security interdependencies in NCS. The closest models to ours are the application of security interdependencies to Internet security (Lelarge & Bolot, 2008), where the authors apply (Heal & Kunreuther, 2004), and present an analytical model, which permits them to study the deployment of security features and protocols in the sub-nets with different network topologies. Also, Lelarge (2009) expands on Heal and Kunreuther (2004) to study economics of malware, i.e., the propagation of computer viruses.

In our setting, individually optimal security choices differ from socially optimal ones; this reflects the presence of externalities. Indeed, in general, when player costs are affected by other player's choices, players impose externalities on each other. The externalities manifest by the gap between the individually and socially optimal security choices (Alpcan & Başar, 2011). In the case of negative externalities, players tend to under invest in security. In the literature, several instruments have been proposed to induce individually optimal player choices to coincide with the socially optimal ones (Alpcan & Başar, 2011; Heal & Kunreuther, 2004; Honeyman et al., 2007).

This article is organized as follows: In Section 2, we formulate the game between NCS when interdependencies are present. In Sections 3 and 4 we present the analysis of the game of 2 and m players, respectively. Concluding remarks are drawn in Section 5.

## 2. Problem setup

### 2.1. The game

We consider an m-player two-stage game. The players are denoted by **P**1, **P**2, ..., **P**m, and the index set $\{1, \ldots, \mathrm{m}\}$ is denoted by $\boldsymbol{M}$. Player **P***i* operates the $i$-th NCS, and his plant and controller communicate over a shared network; see Fig. 1.

In the *first stage*, each **P***i*($i \in \boldsymbol{M}$) chooses to make a security investment ($\mathcal{S}$) or not ($\mathcal{N}$). Let $\mathcal{V}^i$ denote the security choice of **P***i*, i.e.,

$$\mathcal{V}^i := \begin{cases} \mathcal{S}, & \textbf{P}i \text{ invests in security,} \\ \mathcal{N}, & \textbf{P}i \text{ does not invest in security,} \end{cases}$$

and let $\mathcal{V}$ denote the set of player security choices, i.e.,

$$\mathcal{V} := \{\mathcal{V}^1, \ldots, \mathcal{V}^{\mathrm{m}}\}.$$

Once the player security choices are made, they are irreversible and observable by all the players. The **P***i*'s first stage investment is given by

$$J_{\mathrm{I}}^i(\mathcal{V}) := (1 - \mathcal{I}^i)\ell, \quad i \in \boldsymbol{M}, \tag{1}$$

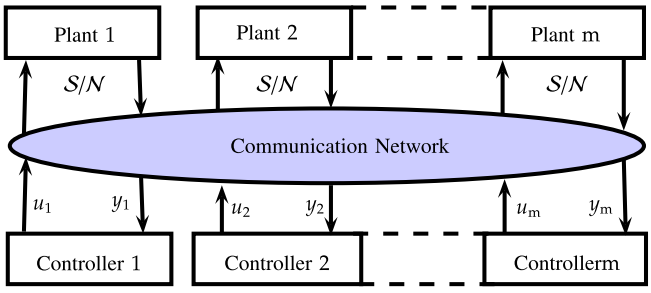


**Fig. 1.** Interdependent Networked Control Systems (NCS).

where $\mathcal{I}^i$ is the indicator function for **P***i*'s security choice, i.e.,

$$\mathcal{I}^i := \begin{cases} 0, & \mathcal{V}^i = \mathcal{S} \\ 1, & \mathcal{V}^i = \mathcal{N}, \end{cases} \tag{2}$$

and $\ell \in \mathbb{R}_+$ is security investment (measures) incurred by **P***i* only if he has chosen $\mathcal{S}$, i.e., $\mathcal{V}^i = \mathcal{S}$.

The plant of **P***i* is modeled as the discrete-time stochastic linear system:

$$\begin{aligned} x_{t+1}^i &= Ax_t^i + \nu_t^i Bu_t^i + w_t^i \\ y_t^i &= \gamma_t^i Cx_t^i + v_t^i \end{aligned} \quad t \in \mathbb{N}_0,\ i \in \boldsymbol{M}, \tag{3}$$

where $x_t^i \in \mathbb{R}^d$ denotes the system state, $u_t^i \in \mathbb{R}^m$ the control input, $w_t^i \in \mathbb{R}^d$ the process noise, $y_t^i \in \mathbb{R}^p$ the measured output, $v_t^i \in \mathbb{R}^p$ the measurement noise, for **P***i* at the $t$-th time step. The matrices $A \in \mathbb{R}^{d\times d}$, $B \in \mathbb{R}^{d\times m}$, $C \in \mathbb{R}^{p\times d}$ are given. We assume that $w_t^i$ (resp. $v_t^i$), for any $i \in \boldsymbol{M}$ and $t \in \mathbb{N}_0$, are independent and identically distributed (i.i.d.) Gaussian random vectors with mean 0 and covariance $Q \in \mathbb{R}^{d\times d}$ (resp. $R \in \mathbb{R}^{p\times p}$). The initial state $x_0^i$ is also Gaussian with mean $\bar{x}_0 \in \mathbb{R}^d$ and covariance $P_0 \in \mathbb{R}^{d\times d}$. We assume uncorrelated $x_0^i$, $w_t^i$, and $v_t^i$. For a fixed $i \in \boldsymbol{M}$ and any $t \in \mathbb{N}_0$, the random variables $\gamma_t^i$ (resp. $\nu_t^i$) are i.i.d. Bernoulli with the failure probability $\tilde{\gamma}^i$ (resp. $\tilde{\nu}^i$), and model the packet loss in the sensor (resp. control) communication channel.

We assume that the failure probabilities $\tilde{\gamma}^i$ and $\tilde{\nu}^i$ are interdependent between the players due to the exposure to network induced insecurities. To reflect security interdependencies, in our model, these failure probabilities depend on the **P***i*'s own security choice $\mathcal{V}^i$ *and* on the other players' security choices $\{\mathcal{V}^j, j \neq i\}$ (chosen in the first stage). We denote the failure probabilities for **P***i* by $\tilde{\gamma}_i(\mathcal{V})$ and $\tilde{\nu}_i(\mathcal{V})$, i.e.,

$$\tilde{\gamma}^i(\mathcal{V}) := \mathsf{P}[\gamma_t^i = 0 \mid \mathcal{V}], \qquad \tilde{\nu}^i(\mathcal{V}) := \mathsf{P}[\nu_t^i = 0 \mid \mathcal{V}].$$

The security interdependencies in failure probabilities $\tilde{\gamma}_i(\mathcal{V})$ and $\tilde{\nu}_i(\mathcal{V})$ are modeled by (9) in Section 2.2.

In the *second stage*, each **P***i* ($i \in \boldsymbol{M}$) chooses a control input sequence $\mathcal{U}^i := \{u_t^i,\ t \in \mathbb{N}_0\}$ for its plant based on the available information defined as:

$$\zeta_t^i = \zeta_{t-1}^i \cup \left\{y_t^i, \nu_{t-1}^i, \gamma_t^i\right\}, \quad t \in \mathbb{N}, \tag{4}$$

with $\zeta_0^i = \left\{\mathcal{V}, y_0^i, \gamma_0^i\right\}$. This information set corresponds to the packet acknowledgment behavior of TCP-like protocols (see Imer et al., 2006). The class of control policies considered here consist of the sequence of functions $\mu_0^i, \mu_1^i, \ldots$ such that each $\mu_t^i$ maps $\zeta_t^i$ into $\mathbb{R}^m$, i.e.,

$$u_t^i = \mu_t^i(\zeta_t^i), \quad t \in \mathbb{N}_0,\ i = 1 \ldots \mathrm{m}. \tag{5}$$

Let $\mathcal{U}$ denote the set of player control input sequences:

$$\mathcal{U} := \mathcal{U}^1 \cup \cdots \cup \mathcal{U}^{\mathrm{m}}.$$

For given $\mathcal{V}$ and $\mathcal{U}$, the **P***i*'s second stage cost is given by the average Linear Quadratic Gaussian (LQG) cost:

$$J_{\mathbb{I}}^i(\mathcal{V},\mathcal{U}) := \limsup_{T\longrightarrow\infty} \frac{1}{T}\mathsf{E}\left[\sum_{t=0}^{T-1} {x_t^i}^\top G x_t^i + v_t^i {u_t^i}^\top H u_t^i\right], \tag{6}$$

where $G \geqslant 0$ (resp. $H > 0$) is a known matrix in $\mathbb{R}^{d\times d}$ (resp. $\mathbb{R}^{m\times m}$).

To summarize, in the first stage, each **P***i* makes a security choice $\mathcal{V}^i$. In the subgame that starts after the first stage, each **P***i* chooses the control input sequence $\mathcal{U}^i$ to minimize the average cost (6). The objective of each **P***i* is to minimize his total cost:

$$J^i(\mathcal{V},\mathcal{U}) = J_{\mathbb{I}}^i(\mathcal{V}) + J_{\mathbb{I}}^i(\mathcal{V},\mathcal{U}), \quad i \in \boldsymbol{M}, \tag{7}$$

where $J_{\mathbb{I}}^i(\mathcal{V})$ (resp. $J_{\mathbb{I}}^i(\mathcal{V},\mathcal{U})$) is given by (1) (resp. (6)). The solution concept for the game is subgame perfect Nash equilibrium, i.e., the strategy profile given by players' optimal control input sequences is a Nash equilibrium in the subgame that starts after the first stage.

Next, we introduce the baseline case of a *social planner* whose objective is to minimize the aggregate cost of all players:

$$J^{\mathrm{so}}(\mathcal{V},\mathcal{U}) = \sum_{i=1}^{\mathrm{m}} J^i(\mathcal{V},\mathcal{U}). \tag{8}$$

### 2.2. Security interdependence

Let the shared network of NCS (see Fig. 1) be subjected to a Denial-of-Service (DoS) attack, and let this attack be implemented by a malicious attacker who floods the network with a large volume of packets to overwhelm the network resources. In general, the effects of a given DoS attack on NCS will depend on the network configuration.[2] Here we consider the case of an uninformed attacker, who knows that the NCS are identical, but lacks information about the network configuration and the player security choices.

We model the failure probabilities for **P***i* as follows:

$$\begin{aligned}\tilde{\gamma}^i(\mathcal{V}) &= \mathcal{I}^i\bar{\gamma} + (1-\mathcal{I}^i\bar{\gamma})\alpha(\eta^{-i})\\ \tilde{v}^i(\mathcal{V}) &= \underbrace{\mathcal{I}^i\bar{v}}_{\text{direct failure}} + \underbrace{(1-\mathcal{I}^i\bar{v})\alpha(\eta^{-i})}_{\text{indirect failure}},\end{aligned} \tag{9}$$

where $\eta^{-i} := \sum_{j\neq i}\mathcal{I}^j$ denotes the number of players (excluding **P***i*) who have chosen $\mathcal{N}$. In (9), the first term reflects the probability of a direct failure, and the second term reflects the probability of an indirect failure. The second term in (9) reflects player interdependence due to being networked and subjected to communication losses at each time step. We assume that the failure probabilities are identical for all $t \in \mathbb{N}_0$.

Next, we relate the terms in (9) with reliability and security. We suggest that the *first term* in (9) models the probability of reliability failure for **P***i*. Here $\bar{\gamma}$ (resp. $\bar{v}$) is the failure probability of **P***i*'s sensor (resp. control) communication channel when all other players **P***j* ($j \neq i$) choose to secure ($\eta^{-i} = 0$). Under this interpretation, the failure probabilities in our model coincide with the existing NCS literature (Imer et al., 2006; Schenato et al., 2007), i.e., no interdependence. From (9), the probability of reliability failure becomes 0 when **P***i* invests in security. However, our results easily extend to cases when **P***i*'s investment reduces this probability to a non-zero (residual) value.

Similarly, we suggest that the *second term* in (9) models the probability of security failure. Here $\alpha(\eta^{-i})$ is the failure probability of **P***i*'s communication channels when $\eta^{-i}$ players (excluding **P***i*) are insecure. We assume that $\alpha : \{0, 1, \ldots, \mathrm{m}-1\} \longrightarrow (0, 1)$ is a strictly increasing function, and define

$$\underline{\alpha} := \alpha(0), \qquad \bar{\alpha} := \alpha(\mathrm{m}-1).$$

Thus, in our model, the probability of security failure increases when more players are insecure. To justify this assumption, consider our game with an additional stage, on which an attacker chooses his flooding rates on each link of the shared network. Let this attacker choose the flooding rate to maximize the average operational costs of each NCS, minus his cost of mounting the attack. In a symmetric attacker equilibrium, an uninformed attacker described above will flood the network uniformly. Moreover, if the cost of attack is continuous and monotone increasing in flooding rate, a higher flooding rate is optimal for the attacker when the network is more insecure (i.e., $\eta$ is higher). This gives two distinct (yet complementary) explanations for our model (9) of NCS security interdependence:

(i) In general, if a player invests in security, the security levels of other players sharing the same network improve as well.[3] Thus, with a higher number of secure players, probabilities of security failure are lower. This corresponds to our assumption that $\alpha(\eta^{-i})$ increases with $\eta^{-i}$, and $\alpha(\eta^{-i})$ depends on the number of insecure players (and not on their identities).

(ii) In addition, since in an equilibrium of the game with an uninformed strategic attacker, a higher flooding rate is optimal for the attacker when the network is more insecure, the term $\alpha(\eta^{-i})$ increases with $\eta^{-i}$ even faster than if one assumes that flooding rate is constant (does not change with $\eta^{-i}$).

Thus, although our model *does not* explicitly consider a strategic attacker, our assumption on $\alpha(\eta^{-i})$ in (9) is aligned with a formal model which includes a strategic attacker as an additional player.

### 2.3. Second stage LQG problem

For any fixed security choices $\mathcal{V}$, the problem of minimizing **P***i*'s expected second stage cost $J_{\mathbb{I}}^i(\mathcal{V},\mathcal{U}^i)$ over $u_t^i = \mu_t^i(\zeta_t^i)$ becomes an infinite horizon LQG problem defined by (3)–(6). We assume that $(A, B)$ and $(A, Q^{1/2})$ are controllable, $(A, C)$ and $(A, G^{1/2})$ are observable, and the maximum failure probabilities are below certain thresholds, as derived in Schenato et al. (2007).[4] That is, for (9):

$$\bar{\gamma} + (1-\bar{\gamma})\bar{\alpha} < \tilde{\gamma}_c, \qquad \bar{v} + (1-\bar{v})\bar{\alpha} < \tilde{v}_c,$$

where the threshold probability $\tilde{\gamma}_c$ (resp. $\tilde{v}_c$) depends on $A$, $C$, $Q$, and $R$ (resp. $A$, $B$, $G$, and $H$). In general, the minimum second stage cost cannot be analytically expressed; however, Theorem 5.6 of Schenato et al. (2007) provides analytical expressions for the upper and lower bounds of this cost. To simplify the exposition, we restrict our attention to the case of invertible $C$ and $R = 0$, which allows us to analytically express the minimum cost:

$$\begin{aligned}J_{\mathbb{I}}^{i*}(\mathcal{V}) := \min_{\mathcal{U}^i\ni u_t^i=\mu_t^i(\zeta_t^i)} J_{\mathbb{I}}^i(\mathcal{V},\mathcal{U}) &= \mathrm{tr}(S^i(\mathcal{V})Q)\\ &\quad + \tilde{\gamma}^i(\mathcal{V})\mathrm{tr}\left((A^\top S^i(\mathcal{V})A + G - S^i(\mathcal{V}))P^i(\mathcal{V})\right),\end{aligned} \tag{10}$$

where the matrices $S^i(\mathcal{V})$ and $P^i(\mathcal{V})$ are the respective positive definite solutions of the following equations:

$$\begin{aligned}S^i(\mathcal{V}) &= A^\top S^i(\mathcal{V})A + G - (1-\tilde{v}^i(\mathcal{V}))\\ &\quad \times A^\top S^i(\mathcal{V})B(B^\top S^i(\mathcal{V})B + H)^{-1}B^\top S^i(\mathcal{V})A,\\ P^i(\mathcal{V}) &= \tilde{\gamma}^i(\mathcal{V})AP^i(\mathcal{V})A^\top + Q.\end{aligned} \tag{11}$$

[2] In using the term "network configuration", we mean network topology, link capacities, etc.

[3] Examples of such security measures are intrusion prevention systems, switches with packet inspection, firewalls, etc.

[4] In Schenato et al. (2007) these expressions are given for the arrival probabilities $(1-\tilde{\gamma}_i)$ and $(1-\tilde{v}_i)$, while we work with $\tilde{\gamma}_i$ and $\tilde{v}_i$.

P2

| P1 | $\mathcal{S}$ | $\mathcal{N}$ |
|---|---|---|
| $\mathcal{S}$ | $J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{S}\})+\ell,\ J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{S}\})+\ell$ | $J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\})+\ell,\ J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\})$ |
| $\mathcal{N}$ | $J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\}),\ J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\})+\ell$ | $J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{N}\}),\ J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{N}\})$ |

| | $\mathcal{S}$ | $\mathcal{N}$ |
|---|---|---|
| $\mathcal{S}$ | $2(J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{S}\})+\ell)$ | $J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\})+J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\})+\ell$ |
| $\mathcal{N}$ | $J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\})+J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\})+\ell$ | $2J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{N}\})$ |

**Fig. 2.** Objectives: 2-player game (top) and social planner (bottom).

In a general case, an estimate of minimum cost $J^{i*}_{\mathbb{I}}(\mathcal{V})$ can be obtained via Monte-Carlo simulations. The following lemma shows that $J^{i*}_{\mathbb{I}}(\mathcal{V})$ is strictly increasing in the failure probabilities:

**Lemma 1.** *Let $\tilde{\gamma}^i_1 < \tilde{\gamma}^i_2$ and $\tilde{v}^i_1 < \tilde{v}^i_2$. Then, $J^{i*}_{\mathbb{I},1} < J^{i*}_{\mathbb{I},2}$.*

**Proof.** From (11) we note that $S^i_1 < S^i_2$ and $P^i_1 < P^i_2$. The proof follows from (10). □

**Example 2.** Consider (3) for the scalar setting with $d = 1$, $B = 1$, $C = 1$. Then $Q, R, G, H$ are scalars. For $|A| > 1$, $\tilde{\gamma}_c = \tilde{v}_c = A^{-2}$. From (10)–(11), the minimum cost $J^{i*}_{\mathbb{I}}(\mathcal{V})$ can be expressed as:

$$J^{i*}_{\mathbb{I}}(\mathcal{V}) = QS^i(\mathcal{V}) + \tilde{\gamma}^i(\mathcal{V})P^i(\mathcal{V})T^i(\mathcal{V}) \tag{12}$$

where $S^i(\mathcal{V}) = \frac{(A^2H+G-H)+\sqrt{(A^2H+G-H)^2+4GH(1-A^2\tilde{v}^i(\mathcal{V}))}}{2(1-A^2\tilde{v}^i(\mathcal{V}))}$, $P^i(\mathcal{V}) = \frac{Q}{1-A^2\tilde{\gamma}^i(\mathcal{V})}$, and $T^i(\mathcal{V}) = \big((A^2-1)S^i(\mathcal{V})+G\big)$.

## 3. Equilibria for two player game

Consider a 2-player game, where the interdependent failure probabilities are given by (9). For any fixed security choices $\mathcal{V}$, each **P***i*'s minimum expected cost in the second stage $J^{i*}_{\mathbb{I}}(\mathcal{V})$ is given by (10)–(11). Following (7), the player objectives for the second stage subgame are presented in Fig. 2 (top). Following (8), the social planner objectives are presented in Fig. 2 (bottom).

To derive optimal player actions in the first stage (security choices $\mathcal{V}^i$), we will distinguish the following two cases:

$$J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\}) \leqslant J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\}) - J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{S}\}), \tag{13}$$

$$J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\}) - J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{S}\}) \leqslant J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\}). \tag{14}$$

If (13) holds and a player invests in security, the other player's gain from investing in security *increases*. However, if (14) holds, each player's decision to secure *decreases* the other player's gain from investing in security. In Sections 3.1 and 3.2, we present equilibria for different $\ell$, and compare with social optima.

### 3.1. Increasing incentives

Let (13) hold, and let us define

$$\underline{\ell}_1 := J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\}),$$
$$\bar{\ell}_1 := J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\}) - J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{S}\}).$$

From Fig. 2 (top), we infer that if $\ell < \underline{\ell}_1$ (resp. $\ell > \bar{\ell}_1$), $\{\mathcal{S},\mathcal{S}\}$ (resp. $\{\mathcal{N},\mathcal{N}\}$) is unique Nash equilibrium. Thus, $\underline{\ell}_1$ (resp. $\bar{\ell}_1$) is the cut-off cost below (resp. above) which both players invest (resp. neither player invests) in security. However, if $\underline{\ell}_1 \leqslant \ell \leqslant \bar{\ell}_1$, both $\{\mathcal{S},\mathcal{S}\}$ and $\{\mathcal{N},\mathcal{N}\}$ are individually optimal, i.e., the game has two pure strategy Nash equilibria. From Fig. 2 (bottom), if $\ell \leqslant \ell^{\text{so}}_1$, the socially optimum choices are $\{\mathcal{S},\mathcal{S}\}$ with

$$\ell^{\text{so}}_1 := J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{S}\}). \tag{15}$$

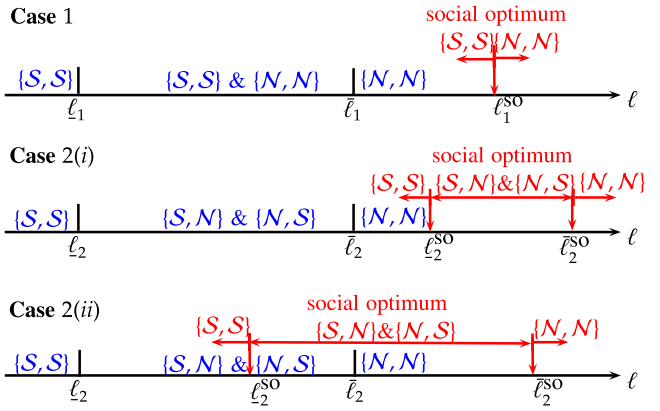


**Fig. 3.** Nash equilibria and social optima for different $\ell$.

For $\ell$ in the range $\bar{\ell}_1 < \ell < \ell^{\text{so}}_1$, individually optimal choices are $\{\mathcal{N},\mathcal{N}\}$, while the socially optimal choices are still $\{\mathcal{S},\mathcal{S}\}$. If $\ell > \ell^{\text{so}}_1$, the individually and socially optimal choices coincide at $\{\mathcal{N},\mathcal{N}\}$. Case 1 of Fig. 3 summarizes pure strategy equilibria for different $\ell$.

For $\ell$ in the range $\underline{\ell}_1 < \ell < \bar{\ell}_1$, a mixed strategy equilibrium exists. Let $\theta^i_1$ (resp. $(1-\theta^i_1)$) denote the mixing probability with which **P***i* chooses $\mathcal{S}$ (resp. $\mathcal{N}$). Then, **P**1's mixing probability $\theta^1_1$ is such that the **P**2's expected costs for both choices $\mathcal{S}$ or $\mathcal{N}$ are equal, i.e.,

$$\theta^1_1\left[J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{S}\})+\ell\right] + (1-\theta^1_1)\left[J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\})+\ell\right]$$
$$= \theta^1_1 J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\}) + (1-\theta^1_1)J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{N}\}).$$

Simplifying the above equation, we obtain

$$\theta^1_1 = \frac{\ell - \underline{\ell}_1}{\bar{\ell}_1 - \underline{\ell}_1}, \quad \text{for } \ell \in (\underline{\ell}_1, \bar{\ell}_1).$$

By writing a similar equation for **P**1, it is easy to check that $\theta^2_1 = \theta^1_1$. Thus, mixed equilibrium is symmetric.

### 3.2. Decreasing incentives

Let (14) hold, and let us define

$$\underline{\ell}_2 := J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\}) - J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{S}\}),$$
$$\bar{\ell}_2 := J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\}).$$

Using Fig. 2 (top), we infer that if $\ell < \underline{\ell}_2$ (resp. $\ell > \bar{\ell}_2$) then $\{\mathcal{S},\mathcal{S}\}$ (resp. $\{\mathcal{N},\mathcal{N}\}$) is unique Nash equilibrium. However, if $\underline{\ell}_2 \leqslant \ell \leqslant \bar{\ell}_2$, both $\{\mathcal{S},\mathcal{N}\}$ and $\{\mathcal{N},\mathcal{S}\}$ are individually optimal. From Fig. 2 (bottom), if $\ell < \underline{\ell}^{\text{so}}_2$ (resp.$\ell > \bar{\ell}^{\text{so}}_2$), the socially optimum choices are $\{\mathcal{S},\mathcal{S}\}$ (resp. $\{\mathcal{N},\mathcal{N}\}$) with

$$\begin{aligned}\underline{\ell}^{\text{so}}_2 &:= J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\}) + J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\}) - 2J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{S}\}),\\ \bar{\ell}^{\text{so}}_2 &:= 2J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\mathbb{I}}(\{\mathcal{S},\mathcal{N}\}) - J^*_{\mathbb{I}}(\{\mathcal{N},\mathcal{S}\}).\end{aligned} \tag{16}$$

Note that $\underline{\ell}^{\text{so}}_2$ can be either above or below $\bar{\ell}_2$. If $\underline{\ell}^{\text{so}}_2 \leqslant \ell \leqslant \bar{\ell}^{\text{so}}_2$, both $\{\mathcal{S},\mathcal{N}\}$ and $\{\mathcal{N},\mathcal{S}\}$ are socially optimum choices. Case 2(i) (resp. Case 2(ii)) of Fig. 3 summarizes the pure strategy equilibria for different $\ell$ when $\bar{\ell}_2 < \underline{\ell}^{\text{so}}_2$ (resp. $\bar{\ell}_2 > \underline{\ell}^{\text{so}}_2$).

Finally, a symmetric mixed strategy equilibrium exists for $\ell$ in the range $\underline{\ell}_2 < \ell < \bar{\ell}_2$ where each player invests in security with probability:

$$\theta^1_2 = \theta^2_2 = \frac{\bar{\ell}_2 - \ell}{\bar{\ell}_2 - \underline{\ell}_2}, \quad \text{for } \ell \in (\underline{\ell}_2, \bar{\ell}_2).$$

We now provide an example system for each case of Fig. 3.

**Example 3.** *Case* 1. Let $A = 0.80, G = Q = H = R = 1$, and $\bar{\gamma} = \bar{\nu} = \underline{\alpha} = \bar{\alpha} = 0.1$. From (12), this system satisfies (13). *Case* 2(i). Let $A = 1.2, G = H = Q = R = 1, \bar{\gamma} = \bar{\nu} = 0.1, \underline{\alpha} = \bar{\alpha} = 0.25$. This system satisfies (14) and $\bar{\ell}_2 < \underline{\ell}_2^{\text{so}}$. *Case* 2(ii). Let $\bar{\gamma} = \bar{\nu} = 0.25$ and all other parameters be as in Case 2(i). This system satisfies (14) and $\bar{\ell}_2 > \underline{\ell}_2^{\text{so}}$.

In both increasing and decreasing incentive cases for the 2-player games of Sections 3.1 and 3.2, the individual and socially optimal security choices differ for a range of security costs. From Fig. 3, we observe that players tend to under-invest in security relative to the social planner. This reflects the presence of negative externalities.

## 4. Equilibria for m player game

We now extend the analysis of Section 3 to m-player games ($\mathrm{m} > 2$), where the interdependent failure probabilities are given by (9). Consider the security choice of $\mathcal{S}$ or $\mathcal{N}$ for $\mathbf{P}i$ (the pivot player), and let the security choices of all other players be fixed. Without loss of generality, let us assume that $\mathbf{P}1, \ldots, \mathbf{P}(i-1)$ (resp. $\mathbf{P}(i+1), \ldots, \mathbf{P}\mathrm{m}$) have chosen $\mathcal{S}$ (resp. $\mathcal{N}$). Let $\mathcal{V}_{\mathcal{S},\eta}$ (resp. $\mathcal{V}_{\mathcal{N},\eta}$) denote the set of player security choices when the pivot player $\mathbf{P}i$ chooses $\mathcal{S}$ (resp. $\mathcal{N}$) and the number of other players who have chosen $\mathcal{N}$ is $\eta$,[5] i.e.,

$$\mathcal{V}_{\mathcal{S},\eta} := \left\{\mathcal{V} | \mathcal{V}^1 = \cdots = \mathcal{V}^i = \mathcal{S}; \mathcal{V}^{i+1} = \cdots = \mathcal{V}^{\mathrm{m}} = \mathcal{N}\right\},$$

$$\mathcal{V}_{\mathcal{N},\eta} := \left\{\mathcal{V} | \mathcal{V}^1 = \cdots = \mathcal{V}^{i-1} = \mathcal{S}; \mathcal{V}^i = \cdots = \mathcal{V}^{\mathrm{m}} = \mathcal{N}\right\},$$

where $i = \mathrm{m} - \eta$.

Let $\Delta(\eta)$ denote the gain of a player from investing in security when $\eta$ other players are insecure, i.e.,

$$\Delta(\eta) := J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{N},\eta}) - J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{S},\eta}), \quad \eta \in \{0, \ldots, \mathrm{m}-1\}. \tag{17}$$

To derive optimal player security choices, we will distinguish the following two cases (which generalize the increasing and decreasing incentive cases for the 2-player games of Sections 3.1 and 3.2):

$$\Delta(\eta) \leqslant \Delta(\eta - 1), \quad \text{for all } \eta \in \{1, 2, \ldots, \mathrm{m}-1\}, \tag{18}$$

and

$$\Delta(\eta) \geqslant \Delta(\eta - 1), \quad \text{for all } \eta \in \{1, 2, \ldots, \mathrm{m}-1\}. \tag{19}$$

Thus, similar to (13), (18) corresponds to the case when the decision of an extra player to invest in security *increases* the other players' gains from investing in security. Also, similar to (14), (19) corresponds to the case when a player's gain from investing in security *decreases* as more players invest in security.

To derive the socially optimal security choices, let $J^{*\text{so}}(\mathrm{n})$ denote the social planner cost when $\mathrm{n} := \sum_{j \in \boldsymbol{M}} \mathcal{I}^j$ players (in total) are insecure, i.e.,

$$J^{*\text{so}}(\mathrm{n}) := (\mathrm{m} - \mathrm{n})\left[J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{S},\mathrm{n}}) + \ell\right] + \mathrm{n} J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{N},\mathrm{n}-1}), \tag{20}$$

where $\mathrm{n} \in \{0, 1, \ldots, \mathrm{m}\}$. Then, social optimum is $\{\mathcal{S}, \ldots, \mathcal{S}\}$ (resp. $\{\mathcal{N}, \ldots, \mathcal{N}\}$) if $\ell < \underline{\ell}^{\text{so,m}}$ (resp. $\ell > \bar{\ell}^{\text{so,m}}$), where

$$\underline{\ell}^{\text{so,m}} = \min_{\mathrm{n} \in \{1, \ldots, \mathrm{m}\}} \left\{ \frac{(\mathrm{m} - \mathrm{n}) J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{S},\mathrm{n}}) - \mathrm{m} J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{S},0})}{\mathrm{n}} + J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{N},\mathrm{n}-1}) \right\},$$

and

$$\bar{\ell}^{\text{so,m}} = \max_{\mathrm{n} \in \{0, \ldots, \mathrm{m}-1\}} \left\{ \frac{\mathrm{m} J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{N},\mathrm{m}-1}) - \mathrm{n} J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{N},\mathrm{n}-1})}{\mathrm{m} - \mathrm{n}} - J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{S},\mathrm{n}}) \right\}.$$

Note that the thresholds $\underline{\ell}^{\text{so,m}}$ and $\bar{\ell}^{\text{so,m}}$ are such that

$$\underline{\ell}^{\text{so,m}} > \Delta(0), \qquad \bar{\ell}^{\text{so,m}} > \Delta(\mathrm{m} - 1). \tag{21}$$

We now characterize the equilibria of the m player game, which includes the determination of optimal player security choices.

[5] We omit the superscript $-i$ from $\eta^{-i} = \sum_{j \neq i} \mathcal{I}^j$ for notational simplicity.

### 4.1. Increasing incentives

Analogous to Section 3.1, we have:

**Theorem 4.** *In the* m *player game (*$\mathrm{m} > 2$*) with (18) imposed, a pure strategy equilibrium exists, and is symmetric. Depending on the magnitude of* $\ell \in \mathbb{R}_+$*, the equilibrium is*

$$\begin{aligned} &\{\mathcal{S}, \ldots, \mathcal{S}\} \quad \text{if } \ell < \ell_1^{\mathrm{m}-1} \\ &\{\mathcal{N}, \ldots, \mathcal{N}\} \quad \text{if } \ell > \ell_1^0 \\ &\{\mathcal{S}, \ldots, \mathcal{S}\} \quad \text{or} \quad \{\mathcal{N}, \ldots, \mathcal{N}\} \quad \text{if } \ell_1^{\mathrm{m}-1} \leqslant \ell \leqslant \ell_1^0, \end{aligned} \tag{22}$$

*where* $\ell_1^{\mathrm{m}-1} := \Delta(\mathrm{m} - 1)$ *and* $\ell_1^0 := \Delta(0)$.

**Proof.** First, with (18) imposed, the existence of symmetric pure strategy Nash equilibrium (22) follows from adopting the construction of Section 3.1. Indeed, if $\ell < \ell_1^{\mathrm{m}-1} \leqslant \Delta(\eta)$ for all $\eta \in \{0, \ldots, \mathrm{m} - 2\}$ (resp. $\ell > \ell_1^0 \geqslant \Delta(\eta)$ for all $\eta \in \{1, \ldots, \mathrm{m} - 1\}$), each $\mathbf{P}i$'s dominant strategy is $\mathcal{S}$ (resp. $\mathcal{N}$). Thus, $\{\mathcal{S}, \ldots, \mathcal{S}\}$ (resp. $\{\mathcal{N}, \ldots, \mathcal{N}\}$) is unique Nash equilibrium. If $\ell \leqslant \ell_1^0$ (resp. $\ell \geqslant \ell_1^{\mathrm{m}-1}$), $\{\mathcal{S}, \ldots, \mathcal{S}\}$ (resp. $\{\mathcal{N}, \ldots, \mathcal{N}\}$) is a Nash equilibrium. Hence, if $\ell$ is in the range $\ell_1^{\mathrm{m}-1} \leqslant \ell \leqslant \ell_1^0$, both $\{\mathcal{S}, \ldots, \mathcal{S}\}$ and $\{\mathcal{N}, \ldots, \mathcal{N}\}$ are equilibria.

Second, we show that no asymmetric equilibrium exists. Assume on the contrary that $\{\mathcal{S}, \ldots, \mathcal{S}, \underbrace{\mathcal{N} \ldots, \mathcal{N}}_{\mathrm{m}_1 \text{ players}}\}$ is an equilibrium, i.e., when $\mathbf{P}1, \ldots, \mathbf{P}(\mathrm{m} - \mathrm{m}_1)$ invest in security and $\mathbf{P}\mathrm{m}_1, \ldots, \mathbf{P}\mathrm{m}$ do not. For $\mathbf{P}(\mathrm{m} - \mathrm{m}_1 + 1)$,

$$\Delta(\mathrm{m}_1 - 1) < \ell, \tag{23}$$

and for $\mathbf{P}(\mathrm{m} - \mathrm{m}_1)$,

$$\ell < \Delta(\mathrm{m}_1). \tag{24}$$

Combining inequalities (23) and (24), we obtain

$$\Delta(\mathrm{m}_1 - 1) < \Delta(\mathrm{m}_1),$$

which contradicts (18) for $\eta = \mathrm{m}_1$. The same contradiction can be shown for any other asymmetric equilibrium. Thus, no asymmetric equilibrium exists. □

From Theorem 4 and noting (21), we conclude that the individual players tend to under-invest in security relative to the social optimum. For $\ell$ in the range $\ell_1^0 < \ell < \underline{\ell}^{\text{so,m}}$, the individually optimal choices are $\{\mathcal{N}, \ldots, \mathcal{N}\}$, while the socially optimal choices are still $\{\mathcal{S}, \ldots, \mathcal{S}\}$.

### 4.2. Decreasing incentives

Analogous to Section 3.2, we have:

**Theorem 5.** *In the game of* m *players with (19) imposed, a pure strategy equilibrium exists. Depending on the magnitude of* $\ell \in \mathbb{R}_+$*, equilibrium is* $\{\mathcal{V}^1, \ldots, \mathcal{V}^{\mathrm{m}} | \mathcal{V}^i \in \{\mathcal{S}, \mathcal{N}\}\}$*, where the number of insecure players is given by*

$$\mathrm{n} = \begin{cases} 0 & \text{if } \ell < \ell_2^0 \\ \mathrm{m} & \text{if } \ell > \ell_2^{\mathrm{m}-1} \\ k & \text{if } \ell_2^{k-1} \leqslant \ell \leqslant \ell_2^k, \quad k \in \{1, \ldots, \mathrm{m}-1\}, \end{cases} \tag{25}$$

*and* $\ell_2^j := \Delta(j),\ j \in \{0, \ldots, \mathrm{m} - 1\}$.

**Proof.** First, with (19) imposed, the existence of equilibrium follows by adopting the construction of Section 3.2. If $\ell < \ell_1^0$ (resp. $\ell > \ell_1^{\mathrm{m}-1}$), all players invest (resp. no player invests) in security, and $\{\mathcal{S}, \ldots, \mathcal{S}\}$ (resp. $\{\mathcal{N}, \ldots, \mathcal{N}\}$) is an equilibrium. However, for any $k \in \{1, \ldots, \mathrm{m} - 1\}$, if $\ell$ is in the range

$$\Delta(k - 1) \leqslant \ell \leqslant \Delta(k),$$

the asymmetric equilibrium $\{\mathcal{S}, \ldots, \mathcal{S}, \underbrace{\mathcal{N} \ldots, \mathcal{N}}_{k \text{ players}}\}$ exists where $(\mathrm{m}-k)$ players choose $\mathcal{S}$ and $k$ players choose $\mathcal{N}$. Thus, the number of insecure players in any equilibrium is given by (25). □

From Theorem 5 and noting (21), we conclude that for $\ell$ in the range $\ell_2^{\mathrm{m}-1} < \ell < \bar{\ell}^{\mathrm{so,m}}$, the individually optimal choices are $\{\mathcal{N}, \ldots, \mathcal{N}\}$, while the socially optimal choices are not $\{\mathcal{N}, \ldots, \mathcal{N}\}$, i.e., at least some security investment is made.

Theorem 4 (resp. Theorem 5) characterizes the pure strategy Nash equilibria for the case of increasing (resp. decreasing) incentives. Since the m player game in both cases is symmetric, a symmetric mixed equilibrium exists and can be computed according to the following proposition:

**Proposition 6.** *In the game of* m *players, an equilibrium mixing probability* $\theta \in (0, 1)$ *is a solution of the equation:*

$$\sum_{j=0}^{\mathrm{m}-1} \binom{\mathrm{m}-1}{j} (\ell - \Delta(j)) \times \theta^{\mathrm{m}-1-j}(1-\theta)^j = 0. \tag{26}$$

**Proof.** Any equilibrium mixing probability $\theta$ is such that any **P***i*'s expected costs for both choices $\mathcal{S}$ or $\mathcal{N}$ are equal. Player expected costs for choosing $\mathcal{S}$ is

$$\begin{aligned}
&\theta^{\mathrm{m}-1}\left(J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{S},0}) + \ell\right) + \binom{\mathrm{m}}{1}\theta^{\mathrm{m}-2}(1-\theta)\left(J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{S},1}) + \ell\right) \\
&\quad + \cdots + \binom{\mathrm{m}}{\mathrm{m}-1}\theta(1-\theta)^{\mathrm{m}-2}\left(J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{S},\mathrm{m}-2}) + \ell\right) \\
&\quad + (1-\theta)^{\mathrm{m}-1}\left(J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{S},\mathrm{m}-1}) + \ell\right).
\end{aligned}$$

Similarly, player expected cost for choosing $\mathcal{N}$ is

$$\begin{aligned}
&\theta^{\mathrm{m}-1}\left(J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{N},0})\right) + \binom{\mathrm{m}}{1}\theta^{\mathrm{m}-2}(1-\theta)\left(J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{N},1})\right) \\
&\quad + \cdots + \binom{\mathrm{m}}{\mathrm{m}-1}\theta(1-\theta)^{\mathrm{m}-2}\left(J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{N},\mathrm{m}-2})\right) \\
&\quad + (1-\theta)^{\mathrm{m}-1}\left(J_{\mathbb{I}}^*(\mathcal{V}_{\mathcal{N},\mathrm{m}-1})\right).
\end{aligned}$$

Equating the above expressions and noting (17), we conclude that mixing probability $\theta \in (0, 1)$ is a solution of (26). □

## 5. Discussion and concluding remarks

In this article, we investigated the incentives to invest in security for players which operate interdependent and identical NCS. We presented a new model of interdependent NCS, where the communication failure probabilities faced by each player are dependent on the security investments of other players. Due to network induced externalities, the individual players tend to under-invest in security (relative to the social planner).

We hope that our findings are relevant for analyzing the risks of DoS attacks on the NCS governing critical infrastructures. It is well accepted that in the near future, a large number of commodity IT solutions will be deployed in critical infrastructures. A wider deployment of smart devices is likely to result in a higher number of players (higher m), a higher degree of interdependence between the players (a higher second term in (9)), and also a higher security cost $\ell$ due to the increased configuration (and overall system) complexity. Thus, we expect that with the NCS becoming increasingly IT-based, the magnitude of negative externalities, and therefore the gap between the individually and socially optimal outcomes only widens.

Security underinvestment in the presence of interdependencies raises the possibility of major breakdowns, which would create losses (due to higher costs) far beyond the NCS losses considered here. Our model does not incorporate these extra losses, which makes our estimates of security investments, including the socially optimal ones, rather conservative.

An interesting extension of our work would be to explicitly model a strategic attacker. Then the question would be to study how the players' security choices are affected by the attacker's objective (e.g., maximizing the average operational costs of all the NCS, or destabilizing a single NCS), and the constraints (e.g., available resources to mount the attack, and information about the network configuration and the NCS parameters).

## Acknowledgments

This work was supported by the Team for Research in Ubiquitous Secure Technology (TRUST), an NSF Science and Technology Center. The first author acknowledges the support of MIT faculty start-up grant. We are grateful to two anonymous reviewers for their valuable feedback, and thank Professors Pravin Varaiya and Demosthenis Teneketzis for useful discussions.

## References

Alpcan, T., & Başar, T. (2011). *Network security: a decision and game theoretic approach*. Philadelphia: Cambridge University Press.

Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2008). Security economics and European policy. In *Proc. of the seventh workshop on the economics of information security. WEIS*. Hanover, NH, USA, June.

Anderson, R., & Fuloria, S. (2009). Security economics and critical national infrastructure. In *Proc. of the eighth workshop on the economics of information security. WEIS*. London, England, June.

Antsaklis, P., & Baillieul, J. (2007). Special issue on technology of networked control systems. *Proceedings of the IEEE*, *95*(1), 5–8.

Bier, V., Oliveros, S., & Samuelson, L. (2007). Choosing what to protect: strategic defensive allocation against an unknown attacker. *Journal of Public Economic Theory*, *9*(4), 563–587.

Böhme, R., & Schwartz, G. A. (2010). Modeling cyber-insurance: towards a unifying framework. In *Proc. of the ninth workshop on the economics of information security. WEIS*. Cambridge, MA, USA, June.

Cárdenas, A. A., Amin, S., & Sastry, S. S. (2008). Research challenges for the security of control systems. In *Proc. of the 3rd USENIX workshop on hot topics in security. HotSec*. San Jose, CA, USA.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, *16*(1), 28–46.

Gupta, V., Dana, A. F., Hespanha, J. P., Murray, R. M., & Hassibi, B. (2009). Data transmission over networks for estimation and control. *IEEE Transactions on Automatic Control*, *54*(8), 1807–1819.

Heal, G., & Kunreuther, H. (2003). Interdependent security. *Journal of Risk and Uncertainty*, *26*(2–3), 231–249.

Heal, G., & Kunreuther, H. (2004). Interdependent security: a general model. NBER Working papers 10706. National Bureau of Economic Research, Inc., August.

Hespanha, J. P., Naghshtabrizi, P., & Xu, Y. (2007). A survey of recent results in networked control systems. *Proceedings of the IEEE*, *95*(1), 138–162.

Hofmann, A. (2007). Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks. *The Geneva Risk and Insurance Review*, *32*(1), 91–111.

Honeyman, P., Schwartz, G. A., & Van Assche, A. (2007). Interdependence of reliability and security. In *Proc. of the 6th workshop on economics of information security. WEIS*. Pittsburgh, PA, USA, June.

Imer, O. C., Yüksel, S., & Başar, T. (2006). Optimal control of LTI systems over unreliable communication links. *Automatica*, *42*(9), 1429–1439.

Langner, R. (2011). Stuxnet: dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, *9*(3), 49–51.

Lelarge, M. (2009). Economics of malware: epidemic risks model, network externalities and incentives. In *Proc. of the 47th annual allerton conference on communication, control, and computing* (pp. 1353–1360). Piscataway, NJ, USA: IEEE Press.

Lelarge, M., & Bolot, J. (2008). Network externalities and the deployment of security features and protocols in the Internet. *SIGMETRICS Performance Evaluation Review*, *36*(1), 37–48.

Miura-Ko, R. A., Yolken, B., Bambos, N., & Mitchell, J. (2008a). Security investment games of interdependent organizations. In *Proc. of the 46th annual allerton conference on communication, control, and computing*. September (pp. 252–260).

Miura-Ko, R. A., Yolken, B., Mitchell, J., & Bambos, N. (2008b). Security decision-making among interdependent organizations. In *Proceedings of the 21st IEEE computer security foundations symposium* (pp. 66–80). Washington, DC, USA: IEEE Computer Society.

Mounzer, J., Alpcan, T., & Bambos, N. (2010). Dynamic control and mitigation of interdependent IT security risks. In *Proc. of the IEEE conference on communication*, ICC. IEEE Communications Society.

Owens, W. A., Dam, K. W., & Lin, H. S. (2009). *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*. Committee on Offensive Information Warfare. National Research Council. Philadelphia.

Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., & Sastry, S. S. (2007). Foundations of control and estimation over lossy networks. *Proceedings of the IEEE*, *95*, 163–187.

Varian, H. R. (2004). System reliability and free riding. In *Economics of information security* (pp. 1–15). Kluwer Academic Publishers.

**Saurabh Amin** is an Assistant Professor in the Department of Civil and Environmental Engineering, Massachusetts Institute of Technology (MIT). His research focuses on the design and implementation of high-confidence network control algorithms for infrastructure systems. He works on robust diagnostics and control problems that involve using networked systems to facilitate the monitoring and control of large-scale critical infrastructures, including transportation, water and energy distribution systems. He also studies the effect of security attacks and random faults on the survivability of networked systems, and designs incentive-compatible control mechanisms to reduce network risks. Dr. Amin received his Ph.D. in systems engineering from the University of California, Berkeley, M.S. in transportation engineering from the University of Texas at Austin, and B.Tech. in civil engineering from the Indian Institute of Technology, Roorkee.

**Galina A. Schwartz** is research economist in the Department of Electrical Engineering and Computer Sciences at the University of California, Berkeley. Dr. Schwartz's primary expertise is game theory and microeconomics. Dr. Schwartz has authored papers in numerous economic and engineering journals. Recently she published on the subjects of network neutrality, cyber risks management and modeling of cyber-insurance markets, and security and privacy of cyber-physical systems. In her earlier research, she has applied contract theory to study the interplay between information, transaction costs, institutions and regulations. Dr. Schwartz has been on the faculty in the Ross School of Business at the University of Michigan, Ann-Arbor, and has taught at Economics Departments at the University of California, Davis and Berkeley. Dr. Schwartz received her M.S. in mathematical physics from Moscow Institute of Engineering Physics (Russia), and Ph.D. in economics from Princeton University in 2000.

**S. Shankar Sastry** received his Ph.D. degree in 1981 from the University of California, Berkeley. He was on the faculty of MIT as Assistant Professor from 1980 to 82 and Harvard University as a chaired Gordon Mc Kay professor in 1994. He is currently the Dean of Engineering at University of California, Berkeley. His areas of personal research are embedded control especially for wireless systems, cybersecurity for embedded systems, critical infrastructure protection, autonomous software for unmanned systems (especially aerial vehicles), computer vision, nonlinear and adaptive control, control of hybrid and embedded systems, and network embedded systems and software. He has supervised over 60 doctoral students and over 50 M.S. students to completion. His students now occupy leadership roles in several places and on the faculties of many major universities. He has coauthored over 450 technical papers and 9 books. Dr. Sastry served on the editorial board of numerous journals, and is currently an Associate Editor of the *IEEE Proceedings*.

Dr. Sastry was elected into the National Academy of Engineering in 2001 and the American Academy of Arts and Sciences (AAAS) in 2004. He also received the President of India Gold Medal in 1977, the IBM Faculty Development award for 1983–1985, the NSF Presidential Young Investigator Award in 1985 and the Eckman Award of the American Automatic Control Council in 1990, the Ragazzini Award for Distinguished Accomplishments in teaching in 2005, an M. A. (honoris causa) from Harvard in 1994, Fellow of the IEEE in 1994, the distinguished Alumnus Award of the Indian Institute of Technology in 1999, and the David Marr prize for the best paper at the International Conference in Computer Vision in 1999, an honorary doctorate from the Royal Swedish Institute of Technology in 2007 and the C.L. Tien Award for Academic Leadership in 2010.