2011 50th IEEE Conference on Decision and Control and
European Control Conference (CDC-ECC)
Orlando, FL, USA, December 12-15, 2011

On the Interdependence of Reliability and Security in Networked Control Systems

Saurabh Amin, Galina A. Schwartz, S. Shankar Sastry

Abstract— **This paper studies player incentives to invest in network reliability and security. We consider heterogeneous networked control system (NCS) – also called players – facing a class of problems involving discrete interdependent risks. We formulate the problem of security choices of the individual NCS as a non-cooperative two-stage game, in which players make they security and control decisions, respectively. We characterize equilibria of the game, thus determining the individually 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. From our results, security and reliability decisions are tightly coupled, and should be considered jointly to improve efficiency.**

I. Introduction

Networked Control Systems (NCS) are increasingly deployed to facilitate monitoring and control of critical infrastructures. The information technology (IT) modernization of NCS permists to achieve higher reliability and lower costs. Yet, recent incidents suggest significant issues with NCS security. In this paper, we approach the problem of security of NCS from a game-theoretic perspective. We focus on the problem of NCS (player) incentives to invest in the improvement of network reliability and security. In our setting, player costs are affected by other player's security choices. Thus, players impose externalities on each other, which result in a gap between the individually and socially optimal security decisions.

Network induced vulnerabilities arise in NCS due to four factors. First, due to wider deployment of off-the-shelf IT devices, NCS inherit the vulnerabilities of these devices, and thus are subject to correlated software and hardware failures. Second, the proprietary network protocols, which are traditional for control systems, are being upgraded to open design protocols, making it easier for attackers to learn about NCS operations. Third, sensor-control data is being made accessible to authorized remote users via corporate networks and Internet. This makes NCS subject to insider attacks. Fourth, the existence of organized cybercrime groups enhances attacker capabilities to conduct intrusions into NCS. Indeed, many nation states view cyberwarfare as the future of armed conflict. The most serious attacks are the ones in which attackers tailor their strategies to damage multiple NCS components. The risks of such rare (but extremely disruptive) events are similar to risks of terrorist attacks, and it is well established that private mitigation of such risks fails [1]. While the first factor primarily raises reliability concerns, the latter three factors mainly raise security concerns.

The approach in this paper compliments the existing and growing literature on efficient security strategies for critical networked systems (see for e.g., [2], [3], [4], [5] and the references therein). The closest models to ours are the application of security interdependencies to Internet security such as [6], where the authors apply [1], and present an analytical model, which permits them to study the deployment of security features in the sub-nets with different topologies.

We build on earlier works [7], [8] which stress two different interdependencies: [8] focuses mostly on interdependence of insecurity and unreliability driven risks, and [7] focuses on the interdependence of security driven failures, which depend on security choices of all system operators, because all systems are exposed to network induced risks. Our earlier paper [7] studied interdependent security (IDS) in the case of identical players. To account for network insecurity, [7] introduced an interdependence term to the Bernoulli failure model of packet losses. This interdependence term, which reflects security driven failures, is affected by the security choices of other players. Our modeling of security interdependencies builds on the interdependent security models of [1], [9].

In this paper, we allow *heterogeneous* systems, which vary by their costs of security. We make two distinct contributions. First, generalize the setting of [7] to heterogeneous systems with nonidentical security costs. Second, we advocate that security and reliability of NCS are tightly coupled, and thus decisions about them should be considered jointly. By imposing penalties on the players who fail to invest in security, we can induce socially optimal player choices.

This paper is organized as follows: In Section II, we formulate the game between interdependent NCSt. In Sections III and IV, we present the analysis of the game of 2 and m players respectively. Concluding remarks are drawn in Section V.

II. Problem Setup

A. The Game

We consider a two-stage game of m heterogeneous players, which are denoted by $\mathbf{P}1, \mathbf{P}2, \ldots, \mathbf{P}\mathrm{m}$. Each player is modeled as a NCS. In the first stage, each $\mathbf{P}i$ $(i \in \boldsymbol{M})$ chooses to make a security investment ($\mathcal{S}$) or not ($\mathcal{N}$). Here

This work was supported in part by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), BT, Cisco, DoCoMo USA Labs, EADS, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, TCS, Telecom Italia, and United Technologies.

The authors are with the University of California at Berkeley, CA, USA

{saurabh,schwartz,sastry}@eecs.berkeley.edu

$\boldsymbol{M}$ denotes the index set $\{1,\dots,\mathrm{m}\}$. Let $\mathcal{V}^i$ denote the security choice of $\mathbf{P}i$, i.e.,

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

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

$$\mathcal{V} \coloneqq \{\mathcal{V}^1,\dots,\mathcal{V}^{\mathrm{m}}\}.$$

The $\mathbf{P}i$'s first stage cost is given by

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

where $\mathcal{I}^i$ is the indicator function:

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

and $\ell^i > 0$ is the security investment incurred by $\mathbf{P}i$ only if he has chosen $\mathcal{S}$, i.e., $\mathcal{V}^i = \mathcal{S}$.

The plant of $\mathbf{P}i$ is modeled as the discrete-time stochastic linear system:

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

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 $\mathbf{P}i$ 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. Also, 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 γ_t^i (resp. ν_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. In our model, the failure probabilities $\tilde{\gamma}^i$ and $\tilde{\nu}^i$ depend on the $\mathbf{P}i$'s own security choice $\mathcal{V}^i$ and on the other players' security choices $\{\mathcal{V}^j, j \neq i\}$, i.e.,

$$\mathsf{P}[\gamma_t^i = 0 \mid \mathcal{V}] = \tilde{\gamma}^i(\mathcal{V}), \quad \mathsf{P}[\nu_t^i = 0 \mid \mathcal{V}] = \tilde{\nu}^i(\mathcal{V}), \quad t \in \mathbb{N}_0,$$

where the failure probabilities $\tilde{\gamma}_i(\mathcal{V})$ and $\tilde{\nu}_i(\mathcal{V})$ for $\mathbf{P}i$ are introduced below by (9) and (10) for the case of $\mathrm{m} = 2$ and $\mathrm{m} > 2$ players, respectively. The player security choices are irreversible and observable by all the players.

In the second stage, each $\mathbf{P}i$ ($i \in \boldsymbol{M}$) chooses a control input sequence $\mathcal{U}^i \coloneqq \{u_t^i,\, t \in \mathbb{N}_0\}$ 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. The class of control policies considered here consist of the sequence of functions $\mu_0^i, \mu_1^i, \dots$ such that each μ_t^i maps ζ_t^i into $\mathbb{R}^m$, i.e.,

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

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

$$\mathcal{U} \coloneqq \{\mathcal{U}^1 \cup \dots \cup \mathcal{U}^{\mathrm{m}}\}.$$

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

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

where $G \geqslant 0$ (resp. $H > 0$) is a known matrix in $\mathbb{R}^{d\times d}$ (resp. $\mathbb{R}^{p\times p}$). The objective of each $\mathbf{P}i$ is to minimize his total cost:

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

where $J_{\mathrm{I}}^i(\mathcal{V})$ (resp. $J_{\mathrm{II}}^i(\mathcal{V},\mathcal{U})$) is given by (1) (resp. (6)).

To summarize, in the first stage, each $\mathbf{P}i$ makes a security choice $\mathcal{V}^i$. In the subgame that starts after the first stage, each $\mathbf{P}i$ chooses the control input sequence $\mathcal{U}^i$ to minimize the average cost (6). In this game, different player security costs ℓ^i (see (1)) introduce *heterogeneities*. The solution concept for the game is subgame perfect Nash equilibrium. Next, we introduce the baseline case of a social planner whose objective is to minimize the aggregate cost of all players:

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

B. Security Interdependence

For a two player game ($\mathrm{m} = 2$), we model the failure probabilities for $\mathbf{P}i$ as follows:

$$\begin{aligned} \tilde{\gamma}^i(\mathcal{V}) &= \mathcal{I}^i\bar{\gamma} + (1-\mathcal{I}^i\bar{\gamma})\alpha(\mathcal{I}^i,\mathcal{I}^{-i}), \\ \tilde{\nu}^i(\mathcal{V}) &= \mathcal{I}^i\bar{\nu} + (1-\mathcal{I}^i\bar{\nu})\alpha(\mathcal{I}^i,\mathcal{I}^{-i}), \end{aligned} \tag{9}$$

where the superscript $-i$ denotes the other player. In (9), the first term reflects the probability of a *reliability* (direct) failure, and the second term reflects the probability of an *security* (indirect) failure. The second term in (9) reflects player interdependence due to being networked and subjected to communication losses. We define the player interdependence term $\alpha : \{0,1\}^2 \to]0,1[$ as follows:

$$0 =: \alpha(0,0) = \alpha(1,0) < \alpha(0,1) \coloneqq \underline{\alpha} \leqslant \alpha(1,1) \coloneqq \bar{\alpha} < 1,$$

where $\bar{\alpha}$ is such that $\bar{\gamma}+(1-\bar{\gamma})\bar{\alpha} < 1$ and $\bar{\nu}+(1-\bar{\nu})\bar{\alpha} < 1$. Thus, we assume that, due to network interdependence, the probability of indirect failure increases when more players insecure. Here $\bar{\gamma}$ (resp. $\bar{\nu}$) is the failure probability of the sensor (resp. control) communication channel (*identical* for both players) when $\alpha(\mathcal{I}^i,\mathcal{I}^{-i}) = 0$, i.e., no interdependence.

We now extend (9) to $\mathrm{m} > 2$ players as follows:

$$\begin{aligned} \tilde{\gamma}^i(\mathcal{V}) &= \mathcal{I}^i\bar{\gamma} + (1-\mathcal{I}^i\bar{\gamma})\beta(\eta^i), \\ \tilde{\nu}^i(\mathcal{V}) &= \mathcal{I}^i\bar{\nu} + (1-\mathcal{I}^i\bar{\nu})\beta(\eta^i), \end{aligned} \tag{10}$$

where $\eta^i := \sum_{j\neq i}\mathcal{I}^j$ denotes the number of players (excluding $\mathbf{P}i$) who have chosen $\mathcal{N}$. As in the two-player case, we assume that the probability of indirect failure (the second term in (10)) increases when more players are insecure. To reflect this, we define the player interdependence term $\beta : \{0,1,\ldots,\mathrm{m}-1\} \longrightarrow]0,1[$ as follows:

$$0 =: \beta(0) < \cdots < \beta\left(\eta^i\right) < \cdots < \beta(\mathrm{m}-1) := \bar{\beta} < 1, \tag{11}$$

where $\bar{\gamma} + (1-\bar{\gamma})\bar{\beta} < 1$, and $\bar{\nu} + (1-\bar{\nu})\bar{\beta} < 1$. In contrast to (9), the interdependence for $\mathbf{P}i$ as defined in (10) does not depend his own choice of security investment. This interdependence term is a measure of insecurity to $\mathbf{P}i$'s NCS given that η other players choose $\mathcal{N}$.

C. Second Stage LQG Problem

For any fixed security choices $\mathcal{V}$, the problem of minimizing $\mathbf{P}i$'s expected second stage cost $J^i_{\text{II}}(\mathcal{V},\mathcal{U}^i)$ over $u^i_t = \mu^i_t(\zeta^i_t)$ becomes an infinite horizon LQG problem defined by (3)–(6). Following [10], we assume that (A,B) and $(A,Q^{1/2})$ are controllable, (A,C) and $(A,G^{1/2})$ are observable, and $\mathbf{P}i$'s maximum failure probabilities are below "certain" thresholds, i.e., for (9):

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

where $\tilde{\gamma}_c$ (resp. $\tilde{\nu}_c$) depends on A, C, Q, and R (resp. A, B, G, and H); similarly for (10). In general, the minimum second stage cost cannot be analytically expressed; however, Theorem 5.6 of [10] 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:

$$\begin{aligned} J^{i*}_{\text{II}}(\mathcal{V}) := \min_{\mathcal{U}^i \ni u^i_t = \mu^i_t(\zeta^i_t)} J^i_{\text{II}}(\mathcal{V},\mathcal{U}) = \operatorname{tr}(S^i(\mathcal{V})Q) \\ + \tilde{\gamma}^i(\mathcal{V}) \operatorname{tr}\left((A^\top S^i(\mathcal{V})A + G - S^i(\mathcal{V}))P^i(\mathcal{V})\right), \end{aligned} \tag{12}$$

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

$$\begin{aligned} S^i(\mathcal{V}) =& A^\top S^i(\mathcal{V})A + G - (1-\tilde{\nu}^i(\mathcal{V})) \\ & \times A^\top S^i(\mathcal{V})B(B^\top S^i(\mathcal{V})B + H)^{-1}B^\top S^i(\mathcal{V})A, \\ P^i(\mathcal{V}) =& \tilde{\gamma}^i(\mathcal{V})AP^i(\mathcal{V})A^\top + Q. \end{aligned} \tag{13}$$

The following lemma provides that $J^{i*}_{\text{II}}(\mathcal{V})$ decreases in failure probabilities:

Lemma 1: Let $\tilde{\gamma}^i(\mathcal{V}^1) < \tilde{\gamma}^i(\mathcal{V}^2)$ and $\tilde{\nu}^i(\mathcal{V}^1) < \tilde{\nu}^i(\mathcal{V}^2)$. Then, $J^{i*}_{\text{II}}(\mathcal{V}^1) < J^{i*}_{\text{II}}(\mathcal{V}^2)$.

Proof: From (13) S^i and P^i, are increasing with $\tilde{\nu}^i$ and $\tilde{\gamma}^i$ respectively. The proof follows from (12). ∎

From (9) and (10), when $\mathbf{P}i$ invests in security, the probability of direct failure is reduced to 0. However, our results easily extend to cases when $\mathbf{P}i$'s investment in security reduces this probability to a non-zero value.

III. 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 $\mathbf{P}i$'s minimum expected cost in the second stage $J^{i*}_{\text{II}}(\mathcal{V})$ is given by (12)–(13). For notational convenience, we will henceforth omit the player index i from $J^{i*}_{\text{II}}(\mathcal{V})$. Following (7), the player objectives for the second stage subgame are presented in Fig. 1(top). Following (8), the social planner objectives are presented in Fig. 1(bottom). To derive optimal player actions in the first stage, we will distinguish the following two cases:

$$J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\}) \leqslant J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}) - J^*_{\text{II}}(\{\mathcal{S},\mathcal{S}\}), \tag{14}$$

$$J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}) - J^*_{\text{II}}(\{\mathcal{S},\mathcal{S}\}) \leqslant J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\}). \tag{15}$$

If (14) holds and a player invests in security, other player gain from investing in security *increases*. However, if (15) holds, each player decision to secure *decreases* the other player gain from investing in security. We now present equilibria for different ℓ^i, and compare with social optima.

A. Increasing incentives

Let (14) hold, and let us define

$$\begin{aligned} \underline{\ell}_1 &:= J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\}), \\ \bar{\ell}_1 &:= J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}) - J^*_{\text{II}}(\{\mathcal{S},\mathcal{S}\}). \end{aligned}$$

From Fig. 1(top), we infer that if $\ell^i < \underline{\ell}_1$ (resp. $\ell^i > \bar{\ell}_1$), the symmetric Nash equilibrium $\{\mathcal{S},\mathcal{S}\}$ (resp. $\{\mathcal{N},\mathcal{N}\}$) is unique. 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. If $\underline{\ell}_1 \leqslant \ell^i \leqslant \bar{\ell}_1$, both $\{\mathcal{S},\mathcal{S}\}$ and $\{\mathcal{N},\mathcal{N}\}$ are individually optimal. However, if $\ell^1 < \underline{\ell}_1$ & $\ell^2 > \bar{\ell}_1$ (resp. $\ell^1 > \bar{\ell}_1$ & $\ell^2 < \underline{\ell}_1$), we infer that asymmetric strategy $\{\mathcal{S},\mathcal{N}\}$ (resp. $\{\mathcal{N},\mathcal{S}\}$) is an equilibrium. Let

$$\begin{aligned} \underline{\ell}^{\text{SO}}_1 &:= 2J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\}) - J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}), \\ \bar{\ell}^{\text{SO}}_1 &:= J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}) + J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\}) - 2J^*_{\text{II}}(\{\mathcal{S},\mathcal{S}\}). \end{aligned} \tag{16}$$

From Fig. 1(bottom), if $\ell^i < \bar{\ell}^{\text{SO}}_1$ (resp.$\ell^i > \bar{\ell}^{\text{SO}}_1$), the socially optimum choices are $\{\mathcal{S},\mathcal{S}\}$ (resp. $\{\mathcal{N},\mathcal{N}\}$). If $\ell^1 \leqslant \underline{\ell}^{\text{SO}}_1$ & $\ell^2 \geqslant \bar{\ell}^{\text{SO}}_1$ (resp. $\ell^2 \leqslant \underline{\ell}^{\text{SO}}_1$ & $\ell^1 \geqslant \bar{\ell}^{\text{SO}}_1$), socially optimum choices are $\{\mathcal{S},\mathcal{N}\}$ (resp. $\{\mathcal{N},\mathcal{S}\}$). Fig. 2 summarizes pure strategy equilibria for different ℓ when $\underline{\ell}^{\text{SO}}_1 < \bar{\ell}_1$.

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

$$\begin{aligned} &\theta^i_1\left[J^*_{\text{II}}(\{\mathcal{S},\mathcal{S}\}) + \ell^{-i}\right] + (1-\theta^i_1)\left[J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\}) + \ell^{-i}\right] \\ &\quad = \theta^i_1 J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}) + (1-\theta^i_1)J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\}). \end{aligned}$$

Simplifying the above equation, we obtain

$$\theta^i_1 = \frac{\ell^{-i} - \underline{\ell}_1}{\bar{\ell}_1 - \underline{\ell}_1}, \text{ for } \ell^{-i} \in (\underline{\ell}_1, \bar{\ell}_1).$$

		P2 $\mathcal{S}$	**P2** $\mathcal{N}$
P1	$\mathcal{S}$	$J^*_{\text{II}}(\{\mathcal{S},\mathcal{S}\})+\ell^1,\ J^*_{\text{II}}(\{\mathcal{S},\mathcal{S}\})+\ell^2$	$J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\})+\ell^1,\ J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\})$
	$\mathcal{N}$	$J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}),\ J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\})+\ell^2$	$J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\}),\ J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\})$

	$\mathcal{S}$	$\mathcal{N}$
$\mathcal{S}$	$2J^*_{\text{II}}(\{\mathcal{S},\mathcal{S}\}))+\ell^1+\ell^2$	$J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\})+J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\})+\ell^1$
$\mathcal{N}$	$J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\})+J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\})+\ell^2$	$2J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\})$

Fig. 1. Objectives: 2−player game (top) & social planner (bottom).

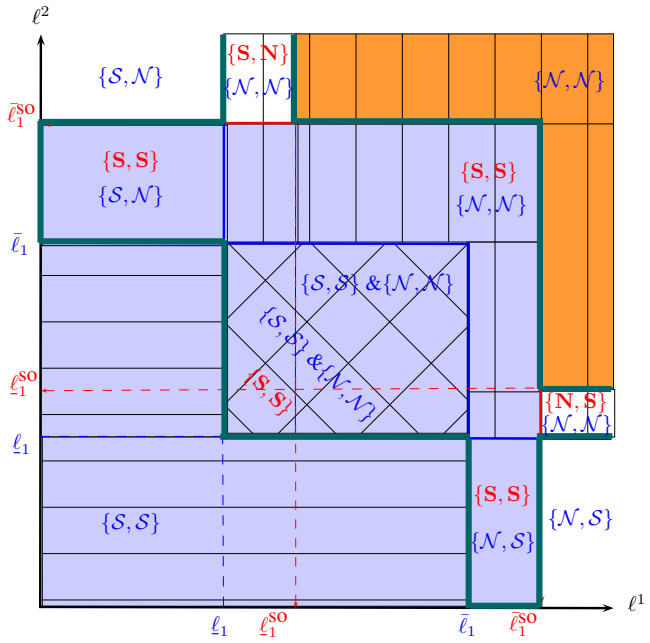

Fig. 2. Equilibria & social optima for the case of increasing incentives.

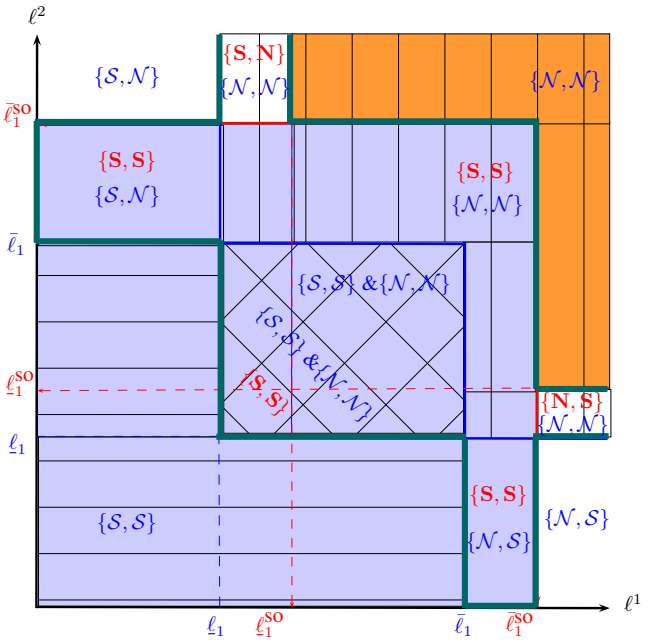

Fig. 3. Equilibria & social optima for the case of decreasing incentives.

B. Decreasing incentives

Let (15) hold, and let us define

$$\underline{\ell}_2 \coloneqq J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}) - J^*_{\text{II}}(\{\mathcal{S},\mathcal{S}\}),$$
$$\bar{\ell}_2 \coloneqq J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\}).$$

Using Fig. 1(top), we infer that if $\ell^i < \underline{\ell}_2$ (resp. $\ell^i > \bar{\ell}_2$) then $\{\mathcal{S},\mathcal{S}\}$ (resp. $\{\mathcal{N},\mathcal{N}\}$) is unique Nash equilibrium. If $\ell^1 \leqslant \bar{\ell}_2$ & $\ell^2 \geqslant \underline{\ell}_2$ (resp. $\ell^2 \leqslant \bar{\ell}_2$ & $\ell^1 \geqslant \underline{\ell}_2$), $\{\mathcal{S},\mathcal{N}\}$ (resp. $\{\mathcal{N},\mathcal{S}\}$) is an equilibrium. Thus, if $\underline{\ell}_2 \leqslant \ell^i \leqslant \bar{\ell}_2$, both $\{\mathcal{S},\mathcal{N}\}$ and $\{\mathcal{N},\mathcal{S}\}$ are individually optimal. From Fig. 1(bottom), if $\ell < \underline{\ell}_2^{\text{SO}}$ (resp.$\ell > \bar{\ell}_2^{\text{SO}}$), the socially optimum choices are $\{\mathcal{S},\mathcal{S}\}$ (resp. $\{\mathcal{N},\mathcal{N}\}$) with

$$\begin{aligned}\underline{\ell}_2^{\text{SO}} &\coloneqq J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}) + J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\}) - 2J^{i*}_{\text{II}}(\{\mathcal{S},\mathcal{S}\}),\\ \bar{\ell}_2^{\text{SO}} &\coloneqq 2J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\}) - J^*_{\text{II}}(\{\mathcal{S},\mathcal{N}\}) - J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}).\end{aligned} \tag{17}$$

Note that $\underline{\ell}_2^{\text{SO}}$ can be either above or below $\bar{\ell}_2$. If $\underline{\ell}_2^{\text{SO}} \leqslant \ell^i \leqslant \bar{\ell}_2^{\text{SO}}$, both $\{\mathcal{S},\mathcal{N}\}$ and $\{\mathcal{N},\mathcal{S}\}$ are socially optimum choices. Fig. 3 summarizes the pure strategy equilibria for different ℓ^i when $\bar{\ell}_2 > \underline{\ell}_2^{\text{SO}}$. Finally, a mixed strategy equilibrium exists for ℓ^{-i} in the range $\underline{\ell}_2 \leqslant \ell^{-i} \leqslant \bar{\ell}_2$ where $\mathbf{P}i$ invests in security with probability:

$$\theta_2^i = \frac{\bar{\ell}_2 - \ell^{-i}}{\bar{\ell}_2 - \underline{\ell}_2}, \text{ for } \ell^{-i} \in (\underline{\ell}_2, \bar{\ell}_2).$$

C. Penalties for insecure players

In both increasing and decreasing incentive cases for the 2−player games of Sections III-A and III-B, the individual and socially optimal security choices differ for a range of security costs. From Figs. 2 and 3, we observe that players tend to under-invest in security relative to the social planner. This reflects the presence of negative externalities. We suggest an instrument (penalty) to alter individually optimal security choices and make them coincide with the socially optimum ones. Let $\mathscr{F}$ denote the penalty imposed on the players who do not invest in security. In the game with penalties, when $\mathbf{P}i$ chooses $\mathcal{S}$ (resp. $\mathcal{N}$), the cost of $\mathbf{P}-i$ when he chooses $\mathcal{N}$ is $J^*_{\text{II}}(\{\mathcal{N},\mathcal{S}\}) + \mathscr{F}$ (resp. $J^*_{\text{II}}(\{\mathcal{N},\mathcal{N}\}) + \mathscr{F}$). We now show that a range of penalties can be computed such that the individually optimum choices in the game with penalties coincide with the social optimum ones.

With (14) imposed, the individual and socially optimal choices coincide if the penalties $\mathscr{F}_1$ for the corresponding game satisfy:

$$\underline{\ell}_1^{\mathrm{SO}} + J_{\mathrm{II}}^*(\{\mathcal{S},\mathcal{N}\}) \leqslant \mathscr{F}_1 + J_{\mathrm{II}}^*(\{\mathcal{N},\mathcal{N}\}) \tag{18}$$

and

$$J_{\mathrm{II}}^*(\{\mathcal{N},\mathcal{S}\}) + \mathscr{F}_1 \leqslant J_{\mathrm{II}}^*(\{\mathcal{S},\mathcal{S}\}) + \bar{\ell}_1^{\mathrm{SO}}. \tag{19}$$

From (18) and (19), and using (16), we obtain:

$$\mathscr{F}_1 \in (J_{\mathrm{II}}^*(\{\mathcal{N},\mathcal{N}\}) - J_{\mathrm{II}}^*(\{\mathcal{N},\mathcal{S}\}), J_{\mathrm{II}}^*(\{\mathcal{S},\mathcal{N}\}) - J_{\mathrm{II}}^*(\{\mathcal{S},\mathcal{S}\})).$$

Similarly, with (15) imposed, the individual and socially optimal choices coincide if the penalties $\mathscr{F}_2$ for the corresponding game satisfy:

$$\underline{\ell}_2^{\mathrm{SO}} + J_{\mathrm{II}}^*(\{\mathcal{S},\mathcal{S}\}) \leqslant \mathscr{F}_2 + J_{\mathrm{II}}^*(\{\mathcal{N},\mathcal{S}\}), \tag{20}$$

and

$$J_{\mathrm{II}}^*(\{\mathcal{N},\mathcal{N}\}) + \mathscr{F}_2 \leqslant J_{\mathrm{II}}^*(\{\mathcal{S},\mathcal{N}\}) + \bar{\ell}_2^{\mathrm{SO}}. \tag{21}$$

From (20) and (21), and using (17), we obtain:

$$\mathscr{F}_2 \in (J_{\mathrm{II}}^*(\{\mathcal{S},\mathcal{N}\}) - J_{\mathrm{II}}^*(\{\mathcal{S},\mathcal{S}\}), J_{\mathrm{II}}^*(\{\mathcal{N},\mathcal{N}\}) - J_{\mathrm{II}}^*(\{\mathcal{N},\mathcal{S}\}).$$

IV. Equilibria for m player game

We now consider $\mathrm{m}-$player games ($\mathrm{m} > 2$) where the interdependent failure probabilities are given by (10). The players $\mathbf{P}1, \mathbf{P}2, \ldots, \mathbf{P}\mathrm{m}$ are ordered according to the security investments ℓ^i incurred when $\mathbf{P}i$ chooses $\mathcal{S}$, i.e.,

$$\ell^1 \leqslant \ldots \leqslant \ell^i \leqslant \ldots \leqslant \ell^{\mathrm{m}}.$$

Consider the $\mathbf{P}i$'s security choice of $\mathcal{S}$ or $\mathcal{N}$, and let the security choices of all other players be fixed. Recall that η^i denotes the number of players (excluding $\mathbf{P}i$) who have chosen $\mathcal{N}$. When obvious, we will omit the superscript i. Let η other players be insecure. Without loss of generality, we 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. $\mathcal{N}$), where $i = \mathrm{m} - \eta$. We use the following simplifying notation:

$$\langle \mathcal{S}, \eta \rangle \coloneqq \left\{ \mathcal{V}^1, \ldots, \mathcal{V}^{\mathrm{m}} \middle| \mathcal{V}^i = \mathcal{S}, \sum_{-i} \mathcal{I}^{-i} = \eta \right\},$$

$$\langle \mathcal{N}, \eta \rangle \coloneqq \left\{ \mathcal{V}^1, \ldots, \mathcal{V}^{\mathrm{m}} \middle| \mathcal{V}^i = \mathcal{N}, \sum_{-i} \mathcal{I}^{-i} = \eta \right\}.$$

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

$$\Delta(\eta) \coloneqq J_{\mathrm{II}}^*(\langle \mathcal{N}, \eta \rangle) - J_{\mathrm{II}}^*(\langle \mathcal{S}, \eta \rangle),\ \eta \in \{0, \ldots, \mathrm{m}-1\}. \tag{22}$$

To derive optimal player security choices $\mathcal{V}^i$, we will distinguish the following two cases (which correspond to the increasing and decreasing incentive cases):

$$\Delta(\eta) \leqslant \Delta(\eta - 1), \quad \text{for all } \eta \in \{1, 2, \ldots, \mathrm{m}-1\}, \tag{23}$$

and

$$\Delta(\eta) \geqslant \Delta(\eta - 1), \quad \text{for all } \eta \in \{1, 2, \ldots, \mathrm{m}-1\}. \tag{24}$$

Thus, similar to (14), (23) corresponds to the case when the decision of an extra player to invest in security *increases* other players' gains from investing in security. Also, similar to (15), (24) corresponds to the case when player gain from investing in security *decreases* as more players invest in security.

Example 2: Consider a $3-$player game ($\mathrm{m} = 3$) of scalar NCS (3) with $d = 1$, $B = 1$, $C = 1$, $G = H = 1$, $Q = 1$, $R = 0$. Let $\bar{\gamma} = \bar{\nu} = \bar{p}$, $\beta(0) = 0$, $\beta(1) = \bar{p}/2$, $\beta(2) = \bar{p}$. Then, $\tilde{\gamma}^i = \tilde{\nu}^i =: \tilde{p}^i$. To ensure closed-stability under $|A| > 1$, we have $\bar{p} < 1 - \frac{\sqrt{A^2-1}}{|A|}$. Following (12), the second-stage cost $J_{\mathrm{II}}^{i*}(\mathcal{V})$ is given by:

$$\begin{aligned} J_{\mathrm{II}}^{i*}(\mathcal{V}) =& \frac{\tilde{p}^i(\mathcal{V})}{1 - A^2\tilde{p}^i(\mathcal{V})} \\ &+ (1 - \tilde{p}^i(\mathcal{V}))\frac{A^2 + \sqrt{A^4 + 4(1 - A^2\tilde{p}^i(\mathcal{V}))}}{2(1 - A^2\tilde{p}^i(\mathcal{V}))^2} \end{aligned} \tag{25}$$

In the game with $A = 0.9$ and $\bar{p} = 0.8$ (resp. $A = 1.1$ and $\bar{p} = 0.6$), players have increasing (resp. decreasing) incentives to secure, i.e., (23) (resp. (24)) are satisfied.

To derive the socially optimal security choices, let $J^{*\mathrm{SO}}(\eta)$ denote the social planner cost when $\mathbf{P}(\eta+1), \ldots, \mathbf{P}\mathrm{m}$ are insecure, i.e.,

$$J^{*\mathrm{SO}}(\eta) \coloneqq (\mathrm{m} - \eta)\left[J_{\mathrm{II}}^*(\langle \mathcal{S}, \eta \rangle) + \ell\right] + \eta J_{\mathrm{II}}^*(\langle \mathcal{N}, \eta - 1 \rangle), \tag{26}$$

where $\eta \in \{0, 1, \ldots, \mathrm{m}-1\}$. Then, social optimum is $\{\mathcal{S}, \ldots, \mathcal{S}\}$ if

$$\begin{aligned} \sum_{i=\mathrm{m}-\eta+1}^{\mathrm{m}} \ell^i = \min_{\eta \in \{1,\ldots,\mathrm{m}\}} \{&(\mathrm{m} - \eta) J_{\mathrm{II}}^*(\langle \mathcal{S}, \eta \rangle) \\ &- \mathrm{m} J_{\mathrm{II}}^*(\langle \mathcal{S}, 0 \rangle) + \eta J_{\mathrm{II}}^*(\langle \mathcal{N}, \eta - 1 \rangle)\}, \end{aligned} \tag{27}$$

and $\{\mathcal{N}, \ldots, \mathcal{N}\}$ if

$$\begin{aligned} \sum_{i=\mathrm{m}-\eta+1}^{\mathrm{m}-\eta} \ell^i = \max_{\eta \in \{0,\ldots,\mathrm{m}-1\}} \{&\mathrm{m} J_{\mathrm{II}}^*(\langle \mathcal{N}, \mathrm{m} - 1 \rangle) \\ &- \eta J_{\mathrm{II}}^*(\langle \mathcal{N}, \eta - 1 \rangle) - (\mathrm{m} - \eta) J_{\mathrm{II}}^*(\langle \mathcal{S}, \eta \rangle)\}. \end{aligned} \tag{28}$$

A. Increasing incentives

Analogous to Section III-A, we have the following result:

Theorem 3: In the game with $\mathrm{m} > 2$ players and (23) imposed, a pure strategy equilibrium exists.

Proof: The proof follows from adopting the construction of Section III-A. ∎

Depending on the magnitude of $\ell^i \in \mathbb{R}_+$, $i \in \boldsymbol{M}$, we identify three interesting cases. A pure strategy equilibrium is

$$\begin{aligned} &\{\mathcal{S}, \ldots, \mathcal{S}\} \text{ if } \ell^{\mathrm{m}} < \Delta(\mathrm{m} - 1) \\ &\{\mathcal{N}, \ldots, \mathcal{N}\} \text{ if } \ell^1 > \Delta(0) \\ &\{\mathcal{S}, \ldots, \mathcal{S}\} \text{ or } \{\mathcal{N}, \ldots, \mathcal{N}\} \text{ if } \ell^j \in (\Delta(\mathrm{m} - 1), \Delta(0)). \end{aligned} \tag{29}$$

B. Decreasing incentives

Analogous to Section III-B, we have the following result:

Theorem 4: In the game with $\mathrm{m} > 2$ players and (24) imposed, a pure strategy equilibrium exists.

Proof: The proof follows from adopting the construction of Section III-B. ∎

Depending on the magnitude of $\ell^i \in \mathbb{R}_+$, $i \in \boldsymbol{M}$, we again identify three cases. A pure strategy equilibrium of the form

$$\left\{ \mathcal{V}^1, \ldots, \mathcal{V}^{\mathrm{m}} \middle| \sum_{i=1}^{\mathrm{m}} \mathcal{I}^i = \eta \right\},$$

exists where

$$\eta = \begin{cases} 0 & \text{if } \ell^{\mathrm{m}} \leqslant \Delta(0) \\ \mathrm{m} & \text{if } \ell^1 \geqslant \Delta(\ell - 1) \\ k & \text{if } \ell^j \in (\Delta(k-1), \Delta(k)),\ k \in \{1, \ldots, \mathrm{m}-1\}. \end{cases} \tag{30}$$

Equilibria for other ranges of ℓ^i can also be characterized.

Theorem 3 (resp. Theorem 4) characterizes the pure strategy equilibria for the case of increasing (resp. decreasing) incentives. Comparing the Nash equilibria of the respective games with (27) and (28), we conclude that the individual players tend to under-invest in security (relative to the social optimum).

The special case when $\ell^i \equiv \ell$, i.e., when player security costs are identical is addressed in [7].

V. Discussion and Concluding Remarks

In this paper, we studied the problem of player incentives to invest in the improvement of network reliability and security when each player is an NCS. In the $2-$player game, we characterized the individually and socially optimal security choices. In the $\mathrm{m}-$player, we present interesting results on the characteristics of equilibria. We find that incentive misalignment between individually and socially optimal actions is present when selfish players choose their security levels to safeguard against network induced risks. Similar results has been reported in the area of economics of information security. For example, the classical review [11] by Varian establishes that (i) in non-cooperative equilibria, underinvestment in security occurs, (ii) for public goods, such as security, regulatory impositions (e.g., due care standards) can be used improve social efficiency. In this paper, we demonstrate similar results for interdependent NCS.

The failure probabilities in (9) and (10) are composed of two terms, with the first one reflecting reliability (or direct) failures and the second one – security (or indirect) failures. We assume that players can choose to invest a fixed sum, which permits them to reduce a direct failure to zero. While we refer to such investment as *security investment*, the effect of such investment is two-fold. Firstly, it affects the direct failure probability, and secondly, it affects the indirect failure probability; hence, the cost of NCS operation. This latter effect is indicative of the interdependence of reliability and security. We conclude that the interactions between these effects are essential and warrant considering security and reliability jointly.

References

[1] G. Heal and H. Kunreuther, "Interdependent security: A general model," National Bureau of Economic Research, Inc, NBER Working Papers 10706, Aug. 2004. [Online]. Available: http://ideas.repec.org/p/nbr/nberwo/10706.html

[2] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The value of intrusion detection systems in information technology security architecture," *Info. Sys. Research*, vol. 16, no. 1, pp. 28–46, 2005.

[3] R. Anderson, R. Böhme, R. Clayton, and T. Moore, "Security economics and European policy," in *Proceedings of the Workshop on the Economics of Information Security WEIS*, Hanover, USA, June 2008.

[4] R. Böhme and G. Schwartz, "Modeling cyber-insurance: Towards a unifying framework," in *Proceedings of the Workshop on the Economics of Information Security WEIS*, Harvard University, June 2010.

[5] T. Alpcan and T. Başar, *Network Security: A Decision and Game Theoretic Approach*. Philadelphia: Cambridge University Press, 2011.

[6] M. Lelarge and J. Bolot, "Network externalities and the deployment of security features and protocols in the internet," *SIGMETRICS Perform. Eval. Rev.*, vol. 36, no. 1, pp. 37–48, 2008.

[7] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," ser. TRUST Working Papers, Berkeley, CA, 2010.

[8] P. Honeyman, G. A. Schwartz, and A. V. Assche, "Interdependence of reliability and security," in *Proceedings of the 6th Workshop on Economics of Information Security (WEIS)*, Jun. 2007.

[9] G. Heal and H. Kunreuther, "Interdependent security," *Journal of Risk and Uncertainty*, vol. 26, no. 2–3, pp. 231–249, 2003.

[10] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proceedings of the IEEE*, vol. 95, pp. 163–187, 2007.

[11] H. R. Varian, "System reliability and free riding," in *Economics of Information Security*. Kluwer Academic Publishers, 2004, pp. 1–15.