Hindawi
Security and Communication Networks
Volume 2017, Article ID 9017039, 19 pages
https://doi.org/10.1155/2017/9017039

Research Article

Stackelberg Interdependent Security Game in Distributed and Hierarchical Cyber-Physical Systems

Jiajun Shen[1,2] and Dongqin Feng[1,2]

[1]*State Key Laboratory of Industrial Control Technology, Department of Control Science and Engineering, Zhejiang University, Hangzhou, Zhejiang 310000, China*
[2]*Institute of Cyber-Systems and Control, Zhejiang, China*

Correspondence should be addressed to Dongqin Feng; dongqinfeng@zju.edu.cn

Received 2 March 2017; Revised 22 May 2017; Accepted 12 June 2017; Published 22 August 2017

Academic Editor: Angelos Antonopoulos

With the integration of physical plant and network, cyber-physical systems (CPSs) are increasingly vulnerable due to their distributed and hierarchical framework. Stackelberg interdependent security game (SISG) is proposed for characterizing the interdependent security in CPSs, that is, the interactions between individual CPSs, which are selfish but nonmalicious with the payoff function being formulated from a cross-layer perspective. The pure-strategy equilibria for two-player symmetric SISG are firstly analyzed with the strategy gap between individual and social optimum being characterized, which is known as negative externalities. Then, the results are further extended to the asymmetric and m-player SISG. At last, a numerical case of practical experiment platform is analyzed for determining the comprehensively optimal security configuration for administrator.

1. Introduction

Cyber-physical systems (CPSs), where modern computing, communication, and control technologies are deeply integrated, have been widely applied in various infrastructures including smart grid, reliable medical devices, and process control [1]. Although CPS can yield enormous benefits for us, its distributed and hierarchical framework (as shown in Figure 1) leads to the exposure of a series of vulnerabilities, which can be directly exploited by external attacker or, in most scenarios, by the compromised neighbors. The corresponding accidents have been reported in various outlets [2–7] and interdependent security of CPS therefore needs urgently to be studied for preventing people's life and property together with national security from being threatened. In this paper, we approach the interdependent security of CPS from a game-theoretic perspective since game theory has already been a mature tool for characterizing the interactions of strategic players.

1.1. Former Studies. According to the former studies, we conclude two branches of recent research concerning interdependent security, that is, internally and externally interdependent security.

In most research, the internally interdependent security is also expressed as cross-layer security, cascading security, or resilient control which is mainly focused on making a tradeoff between cyber cost and physical control performance.

In the literatures for cross-layer security of CPS, researchers have proposed several control theoretic approaches [8–12].

Liu et al. [8] show how an attacker can manipulate the state estimation while avoiding bad-data alarms in the control center. Two security indices are further defined in [9] for quantifying the degree of difficulty of carrying out a successful stealth attack against particular measurements. In [10], by encrypting a certain number of measurement devices, a state estimator is protected from unobserved attacks. In [11], stealthy false-data attacks against the state estimators in power systems are studied. From the perspective of compromise in filter gain or controller gain, Elbsat and Yaz [12] firstly use finite time state-feedback stabilization for discrete-time nonlinear systems with conic-type nonlinearities, bounded feedback control gain perturbations, and additive disturbances.

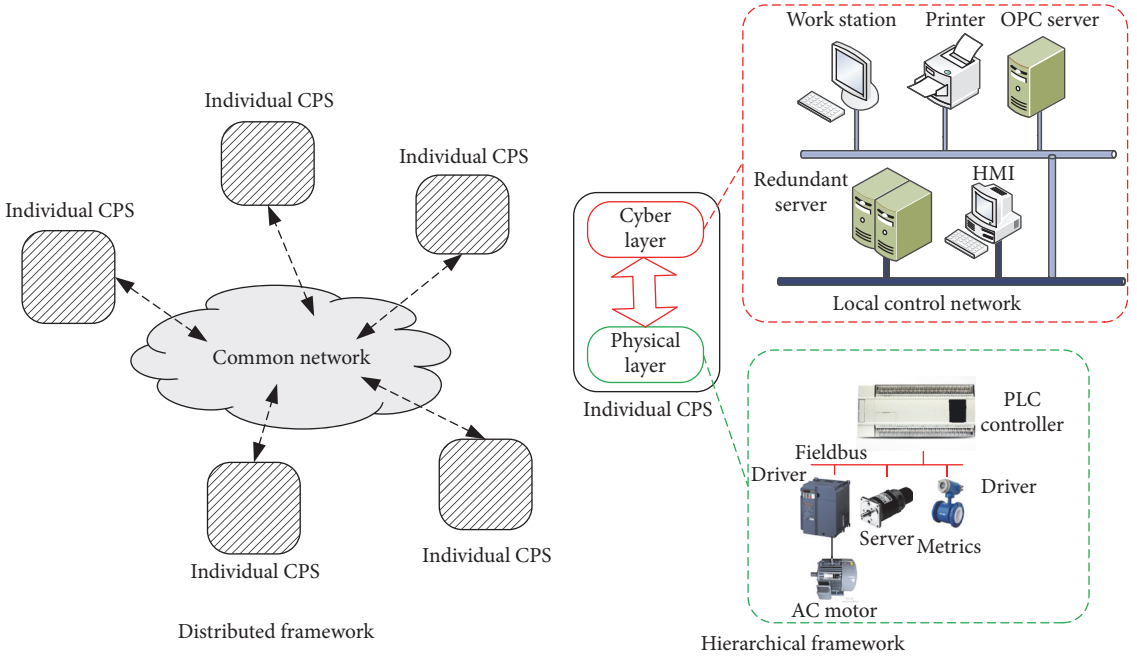

Figure 1: Distributed and hierarchical framework of CPS.

As for cascading security and resilient control, in [13, 14], the authors consider the cyber-physical system consisted of mutually interdependent physical-resource and computational-resource networks, which is basically in accordance with the concept of cross-layer framework. The issue of cascading failure occurring in such system is then investigated with a threshold of the proportion of faulty nodes being obtained for the collapse of system.

Yuan et al. [15] use a unified game approach for resilient control of networked control system (NCS) under Denial-of-Service (DoS) attack. The packet dropout caused by attacker is considered in cyber layer, while, in physical layer, optimal control strategies with multitasking and central tasking structure are developed using game theory. In [16], resilient stabilization of a Multihop Control Network (MCN) is considered as a codesign problem of controller and communication protocol. In physical layer, a MIMO LTI system is considered, and the necessary and sufficient conditions that invalidate controllability and observability are characterized. In cyber layer, how to detect and isolate the compromised nodes is discussed.

Nevertheless, as for external interdependence security of CPS, it is worth mentioning that there is surprisingly little work on this topic. To the best of our knowledge, the most related works to ours are [17–19].

In [17], the interdependent security of identical networked control systems is studied. The problem of how to make security investment for each individual system operator is formulated as a two-stage noncooperative game, in the first stage of which a security investment should be decided to make or not, while, in the second stage, an LQG problem is then resolved for minimizing the average operational cost.

In [18], the authors present an analytical model based on the Kunreuther and Heal game-theoretic model of the interdependent security problem, in order to study the deployment of security features and protocols in the subnets with different network topologies. In [19], the Kunreuther and Heal game-theoretic model of the interdependent security problem is extended by applying empirically based social network, while theft of knowledge is considered as the major threat due to its impact on both economic and national security.

1.2. Contributions. Nevertheless, the static game proposed in [17] is against the practical scenario that once security choices are made, they are observable to all the players connected by the common network. In addition, the amount of defense resources implemented on each individual is ignored since all the individuals are assumed to be identical, and the corresponding action space of each individual merely includes two choices, "invest" or "not invest." Furthermore, in [18, 19], the researchers only discuss the security investment of cyber layer without taking any physical effect into account.

It is noted that there exist the papers and projects containing approaches of taking both cyber and physical aspects into consideration based on the methodology other than game theory, such as switch system-based research [20–22] and state estimation-based research [8, 9]. However, in these researches, the nature of rational cyber attackers and physical uncertainties is ignored. It is hard to capture the rational, intelligent, and uncertain dynamics of the distributed and hierarchical CPSs without game-theoretic methodology. Due to space limitations, we choose to go no further on detailed discussion. The researches [17–19] are analyzed since they are all studied from a game-theoretic perspective which is in accordance with the methodology of our paper.

The main contributions of this paper include the following.

(1) According to the practical scenario, a Stackelberg interdependent security game (SISG) is proposed for better capturing the interactions between individual CPSs sharing common network. Unlike the simultaneous moves in static game proposed in [17], the players would act in order.

(2) When formulating payoff function, we consider the internally interdependent security by taking factors of both cyber layer and physical layer into consideration. More specifically, in physical layer, an H-∞ optimal control problem is considered and control performance index γ^* is dependent on time-delay parameters which are determined by the cyber interactions. The security issues in cyber layer and optimal control problems in physical layer are then intertwined.

(3) The pure-strategy equilibria are analyzed for two-player symmetric SISG with the conditions under which these equilibria can take place being determined. Meanwhile, our results show that the individually optimal choices differ from socially optimal ones, which prove the existence of strategy gap and negative externalities. It indicates that the individual players tend to underinvest in security (relative to the social planner) due to the negative externalities introduced by common network.

(4) The result of two-player symmetric SISG is further extended to asymmetric and m-player SISG. Specifically, we discuss the circumstance that the players are nonidentical, which we name as asymmetric SISG for distinguishing from the case that individuals are equipped with same defense resources and action space.

(5) A numerical case study of practical experiment platform is given, which indicates a possible way of solving interdependent security issues in practical engineering projects. It will help administrator make a comprehensively optimal configuration in distributed environment.

1.3. Organization. The rest of this paper is organized as follows. In Section 2, SISG is introduced with cross-layer payoff function being defined. Moreover, the security interdependence reflected in payoff function is explained as well. In Sections 3 and 4, the pure-strategy equilibria for two-player symmetric SISG are firstly analyzed and the results are extended to asymmetric and m-player SISG. The condition under which these equilibria can take place is given, and meanwhile both individual and social optima are explored with the gap of which is being clearly distinguished. A numerical case of practical experiment platform is analyzed in Section 5. Section 6 concludes this paper and introduces our future interests. The proofs of Theorems 3, 4, and 5 are supplied in Appendices A, B, and C, respectively.

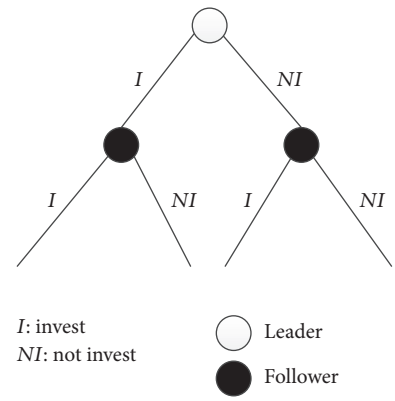

Figure 2: Extensive form representation of two-player symmetric SISG.

2. Problem Setting

2.1. Stackelberg Interdependent Security Game. Firstly, the definition of interdependent security game is given as follows.

Definition 1 (interdependent security game). In an interdependent security game, the players are selfish but nonmalicious and are able to choose whether to invest in security or remain unprotected. Each player's goal is to minimize his own risk, which depends on the investments of some or every other players who also aim to minimize their own costs.

We firstly consider the situation that all the players (individual CPSs) are identical and the corresponding Stackelberg interdependent security game (SISG) is therefore called symmetric SISG. The extensive form representation of two-player and m-player symmetric SISG is as shown in Figures 2 and 3, respectively.

In two-player symmetric SISG as described in Figure 2, leader chooses to invest or not invest in security at first, and then follower makes an optimal response for minimizing his own payoff. In m-player SISG as described in Figure 3, the players other than P_i, who are assumed to act simultaneously, are regarded as leader. $\psi_L(\xi)$ denotes the strategy of leader with ξ representing the number of insecure individuals, that is, the players who do not make a security investment. Furthermore, m is the total number of players. After the strategy of P_{-i}, $\psi_L(\xi)$, being determined, the follower, P_i, chooses an optimal strategy for minimizing his own payoff. Based on Figures 2 and 3, it would be easy to extend the symmetric SISG to the situation that the amount of defense investment choices of all the players is more than two.

It is noted that, in the symmetric SISG given by Figures 2 and 3, all of the players (individual CPSs) are supposed to be identical. The action space defined for each CPS is the same and includes "invest" or "not invest" with the different defense resources implemented on each CPS being ignored. In practical security scenarios such as Stuxnet worm [2], Flame virus [4], and Water Plant Breach [5], the rational attackers are always familiar with the fingerprint characteristic of CPS, which indicates that they are capable of accurately parsing the command message and find the target

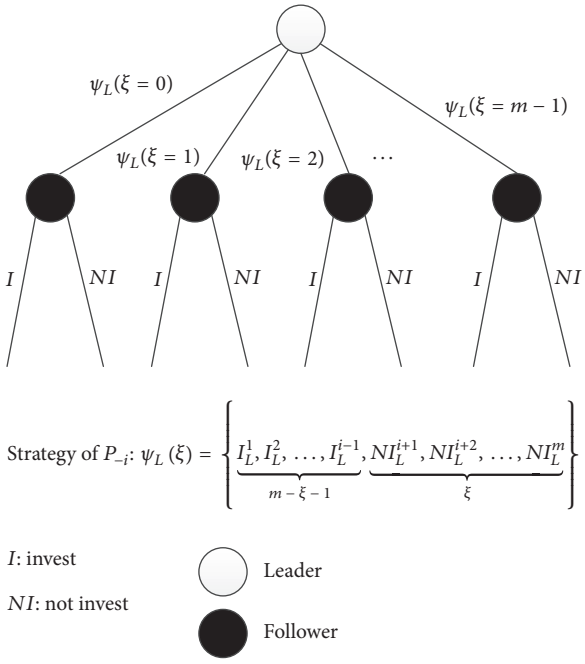

Figure 3: Extensive form representation of m-player symmetric SISG.

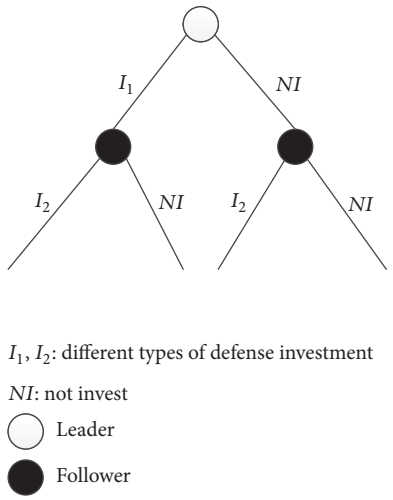

Figure 4: Extensive form representation of two-player asymmetric SISG.

devices even in the complicated hierarchical and distributed framework. Naturally, it is supposed that different attack strategy would be implemented for different target devices and thus each CPS is faced with different types of cyber attacks. Under this circumstance, the players (individual CPSs) of SISG should be considered as nonidentical.

The extensive form representations of asymmetric SISG for two-player and m-player are given in Figures 4 and 5, respectively, where different types of defense investment are considered for each player. In Figure 4, I_1 and I_2 represent different types of defense investment of each player. In Figure 5, $I_{1,L}^j$ ($j \neq i$) indicates that the defense investment implemented by the jth leader is I_1.

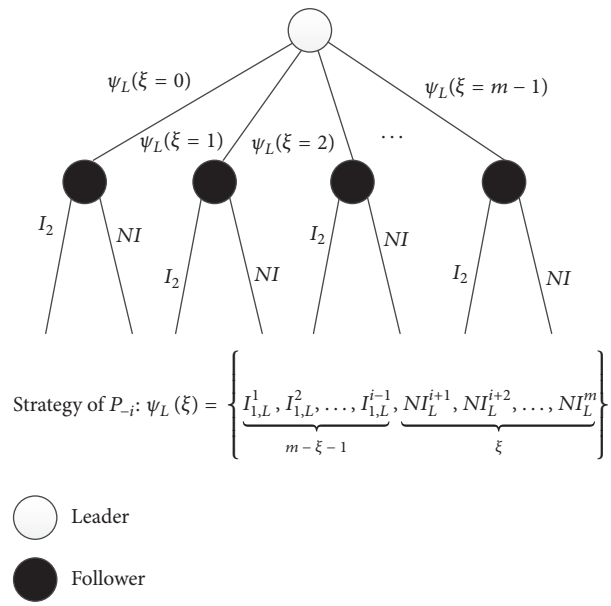

Figure 5: Extensive form representation of m-player asymmetric SISG.

Based on Figures 4 and 5, it is easy to extend the situations to more complicated ones, such as the situation that amount of defense investment choices of each player is more than two.

2.2. Cross-Layer Payoff Function. For better characterizing the SISG, we formulate payoff function from a cross-layer perspective, that is, taking factors of both cyber layer and physical layer into consideration.

Each individual CPS is viewed as a player P_i ($i \in M$), where M is the set of all players. Each player aims to minimize his own overall payoff for maintaining a relatively higher security level and better control performance.

In cyber layer, P_i is able to decide whether to invest in security or not and SI^i is denoted as the security choice made by P_i,

$$SI^i := \begin{cases} 1, & P_i \text{ invests in security,} \\ 0, & P_i \text{ does not invest in security.} \end{cases} \tag{1}$$

The security choices made by all players can therefore be denoted as $SI := \{SI^1, \ldots, SI^i, \ldots, SI^m\}$, and thus the cyber layer cost of P_i is given by

$$J_C^i\left(SI^i\right) := SI^i \cdot l, \quad i \in M. \tag{2}$$

The physical plant of each individual CPS is described by discrete-time model, which is assumed to be in the form as follows:

$$\begin{aligned} x_{k+1} &= Ax_k + B_2 u_{c,k} + B_1 \omega_k, \\ z_k &= Dx_k, \end{aligned} \tag{3}$$

where $x_k \in \mathbb{R}^n$ is the system state, $u_{c,k} \in \mathbb{R}^m$ is the control input, $z_k \in \mathbb{R}^r$ is the controlled output, $\omega_k \in \mathbb{R}^q$ is the

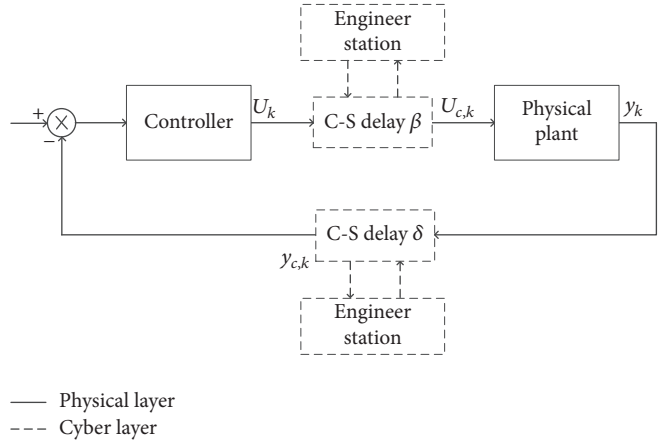

Figure 6: Structure of CPS with C-A and S-C delays.

disturbance input belonging to $l_2[0,\infty)$, A, B_1, B_2, and D are known real matrices with appropriate dimensions.

The randomly varying communication delays are described by

$$\begin{aligned} y_k &= Cx_k, \\ y_{c,k} &= (1-\delta)\, y_k + \delta y_{k-1}, \\ u_k &= K\hat{x}_k, \\ u_{c,k} &= (1-\beta)\, u_k + \beta u_{k-1}, \end{aligned} \tag{4}$$

where $y_{c,k} \in \mathbb{R}^p$ is the measured output and $y_k \in \mathbb{R}^p$ is the actual output. $u_k \in \mathbb{R}^m$ is the control signal generated by the controller and $u_{c,k}$ is the signal received by the actuator. δ and β are both communication delays.

In practical engineering scenario, such as controlling the PWM inverter for an uninterrupted power system (UPS) through network, the output AC voltage data measured by sensor and then collected by PLC corresponds to $y_{c,k}$, while the actual output AC voltage corresponds to y_k. u_k is the control command for the PWM inverter, while $u_{c,k}$ is the control signal received by the PWM inverter. δ (resp., β) can be interpreted as the communication delay on sensor-to-controller (resp., controller-to-actuator) channel as shown in Figure 6.

The stochastic variable is considered as Bernoulli distributed white sequence with

$$\begin{aligned} \overline{\delta} &= \Pr\{\delta = 1\} = E\{\delta\}, \\ \Pr\{\delta = 0\} &= 1 - E\{\delta\} = 1 - \overline{\delta}. \end{aligned} \tag{5}$$

According to (4), it is noted that when $\delta = 1$ (resp., $\delta = 0$), $y_{c,k} = y_{k-1}$ (resp., $y_{c,k} = y_k$) indicates that the last sensor command is not received (or received) by the controller at k, and when $\beta = 1$ (resp., $\beta = 0$), $u_{c,k} = u_{k-1}$ (resp., $u_{c,k} = u_k$) indicates that the last control command is not received (or received) by the actuator at k. The influence that time-delay attacker exerts on system control can therefore be embodied by packet losses happened in the last step.

More specifically, taking typical time-delay attack, DoS attacks, into consideration, we can view both $\overline{\delta}$ and $\overline{\beta}$ as intensity-of-attack (IoA) on S-C and C-A communication channel, respectively. According to Xu et al. [23], DoS attacks can degrade the channel quality which leads to the packet losses and thus lowers package delivery rate (PDR). The corresponding $H\infty$-optimal control problem under DoS attacks should be able to address the issue of packet losses which is also common in traditional network control system (NCS) [24, 25].

Here we use the dynamic observer-based control scheme [26] for the system described by (3):

$$\text{Observer: } \begin{cases} \hat{x}_{k+1} = A\hat{x}_k + B_2 u_{c,k} + L\left(y_{c,k} - \overline{y}_{c,k}\right), \\ \overline{y}_{c,k} = \left(1-\overline{\delta}\right) C\hat{x}_k + \overline{\delta} C\hat{x}_{k-1}, \end{cases} \tag{6}$$

$$\text{Controller: } \begin{cases} u_k = K\hat{x}_k, \\ \overline{u}_{c,k} = \left(1-\overline{\beta}\right) u_k + \overline{\beta} u_{k-1}, \end{cases} \tag{7}$$

where $\hat{x}_k \in \mathbb{R}^n$ is the estimated state, $\overline{y}_{c,k} \in \mathbb{R}^p$ is the observer output, $u_k \in \mathbb{R}^m$ is the control signal generated by the controller, $u_{c,k}$ is the signal received by the actuator, and $L \in \mathbb{R}^{n\times p}$ and $K \in \mathbb{R}^{m\times n}$ are the observer gain and controller gain, respectively. The stochastic variable β, mutually independent of δ, is also a Bernoulli distributed white sequence with expected value $\overline{\beta}$.

The parameters in physical layer, $\overline{\delta}$ and $\overline{\beta}$, are defined as $\overline{\delta}(SI^i, SI^{-i})$ and $\overline{\beta}(SI^i, SI^{-i})$ for depicting the internally interdependent security, since communication delay in physical layer is influenced by the cyber interactions. Once $\overline{\delta}$ and $\overline{\beta}$ are determined, the $H\infty$-optimal controller can then be designed. If the initial condition is zero, the $H\infty$ index γ satisfies inequality (7) and can be obtained through applying Theorem 1 proposed in [26].

$$E\left\{\sum_{k=0}^{\infty}\left\{\|z_k\|^2\right\}\right\} < \gamma^2 \sum_{k=0}^{\infty}\left\{\|w_k\|^2\right\}. \tag{8}$$

Table 1: Strategic form representation of two-player symmetric SISG.

		Follower			
		(I_2, I_2)	(I_2, NI_L)	(NI_L, I_2)	(NI_L, NI_L)
Leader	I_1	$l_1 + J_P^*\{I_1, I_2\}$, $l_2 + J_P^*\{I_1, I_2\}$	$l_1 + J_P^*\{I_1, I_2\}$, $l_2 + J_P^*\{I_1, I_2\}$	$l_1 + J_P^*\{I_1, NI_F\}$, $J_P^*\{I_1, NI_F\}$	$l_1 + J_P^*\{I_1, NI_F\}$, $J_P^*\{I_1, NI_F\}$
	NI_L	$J_P^*\{NI_L, I_2\}$, $l_2 + J_P^*\{NI_L, I_2\}$	$J_P^*\{NI_L, NI_F\}$, $J_P^*\{NI_L, NI_F\}$	$J_P^*\{NI_L, I_2\}$, $l_2 + J_P^*\{NI_L, I_2\}$	$J_P^*\{NI_L, NI_F\}$, $J_P^*\{NI_L, NI_F\}$

Table 2: Strategic form representation of m-players symmetric SISG.

		Follower			
		$\left(I_F, \underbrace{NI_F, \ldots, NI_F}_{m-1}\right)$	$\left(I_F, I_F, \underbrace{NI_F, \ldots, NI_F}_{m-2}\right)$	$\cdots$	$\left(\underbrace{I_F, \ldots, I_F}_{m-1}, NI_F\right)$
Leader	$\psi_L(\xi = 0)$	$(m-1)\cdot l + J_P^*\{\psi_L(\xi = 0), I_F\}$, $l + J_P^*\{\psi_L(\xi = 0), I_F\}$	$(m-1)\cdot l + J_P^*\{\psi_L(\xi = 0), I_F\}$, $l + J_P^*\{\psi_L(\xi = 0), I_F\}$	$\cdots$	$(m-1)\cdot l + J_P^*\{\psi_L(\xi = 0), I_F\}$, $l + J_P^*\{\psi_L(\xi = 0), I_F\}$
	$\psi_L(\xi = 1)$	$(m-2)\cdot l + J_P^*\{\psi_L(\xi = 1), NI_F\}$, $J_P^*\{\psi_L(\xi = 1), NI_F\}$	$(m-2)\cdot l + J_P^*\{\psi_L(\xi = 1), I_F\}$, $l + J_P^*\{\psi_L(\xi = 1), I_F\}$	$\cdots$	$(m-2)\cdot l + J_P^*\{\psi_L(\xi = 1), I_F\}$, $l + J_P^*\{\psi_L(\xi = 1), I_F\}$
	$\psi_L(\xi = 2)$	$(m-3)\cdot l + J_P^*\{\psi_L(\xi = 2), NI_F\}$, $J_P^*\{\psi_L(\xi = 2), NI_F\}$	$(m-3)\cdot l + J_P^*\{\psi_L(\xi = 2), NI_F\}$, $J_P^*\{\psi_L(\xi = 2), NI_F\}$	$\cdots$	$(m-3)\cdot l + J_P^*\{\psi_L(\xi = 2), I_F\}$, $l + J_P^*\{\psi_L(\xi = 2), I_F\}$
	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
	$\psi_L(\xi = m-1)$	$0\cdot l + J_P^*\{\psi_L(\xi = m-1), NI_F\}$, $J_P^*\{\psi_L(\xi = m-1), NI_F\}$	$0\cdot l + J_P^*\{\psi_L(\xi = m-1), NI_F\}$, $J_P^*\{\psi_L(\xi = m-1), NI_F\}$	$\cdots$	$0\cdot l + J_P^*\{\psi_L(\xi = m-1), I_F\}$, $l + J_P^*\{\psi_L(\xi = m-1), I_F\}$

The physical layer cost in this paper is denoted as $J_P = \gamma^*$ which is the minimum of $H\infty$ index γ that satisfies inequality (8). It is noted that the aim of designing an $H\infty$-optimal controller is to minimize the closed-loop impact of a perturbation. For the attenuation rate of controlled output z_k under the impact of disturbance input w_k, $H\infty$ optimal index, γ^*, represents and quantifies the control performance of physical plant. The lower the value of γ^* is, the better the control performance physical plant is. In addition, for reflecting the influence of cyber security investment, we further refine the expression of J_P by

$$\begin{aligned} J_P^i\left\{SI^{-i}, SI^i\right\} &= \gamma^*\left\{SI^{-i}, SI^i\right\} \\ &= \gamma^*\left(\overline{\delta}\left\{SI^{-i}, SI^i\right\}, \overline{\beta}\left\{SI^{-i}, SI^i\right\}\right). \end{aligned} \tag{9}$$

The cyber layer cost depends on the security choice made by players. Since SI^i denotes the security choice made by player P_i, the cyber layer cost of P_i can therefore be given as $J_C^i(SI^i) = SI^i \cdot l$, where l represents the cost of cyber countermeasure adopted and therefore quantifies the cyber security investment. For example, if the cyber layer is equipped with SCADA or IDS, l can be further interpreted as the computing resource occupancy ratio of a specific packet filtering policy. When P_i chooses to invest in security, the cyber layer cost would be l; otherwise it would be 0.

The overall payoff function of each individual player can therefore be obtained as (10). The security issues in cyber layer and optimal control problems in physical layer are intertwined, and the payoff of each individual is therefore formulated from a more comprehensive and accurate perspective.

$$J_O^i\left\{SI^{-i}, SI^i\right\} = J_C^i\left\{SI^i\right\} + J_P^i\left\{SI^{-i}, SI^i\right\}. \tag{10}$$

We then show how to build payoff matrix for SISG. Take the two-player and m-player symmetric SISG introduced in Figures 2 and 3 as instance, the strategic form representation of which is given as shown in Tables 1 and 2, respectively.

In Table 1, subscripts L and F indicate the leader and follower; for example, I_F denotes that follower chooses to invest in security. In addition, since follower has two information sets and two available actions, four pure strategies for follower including (I_F, I_F), (I_F, NI_F), (NI_F, I_F), and (NI_F, NI_F) can be implemented. (I_F, I_F) indicates the response strategy that no matter what action leader takes, he will always choose to invest in security. In addition, the upper (resp., lower) one is the payoff function of leader (resp., follower), that is, J^{L*} (resp., J^{F*}).

In Table 2, m pure strategies for follower are listed. In addition, it is noted that although there actually exists 2^m pure strategies, implementing pure strategy $(I_F, I_F, \underbrace{NI_F, \ldots, NI_F}_{m-2})$ has the same result with that of applying $(I_F, NI_F, I_F, \underbrace{NI_F, \ldots, NI_F}_{m-3})$. For the convenience of denotation and analysis, only m situations are listed. It is easy for us to extend the result to asymmetric situation according to Tables 1 and 2.

2.3. Security Interdependence. Let each individual CPS be subjected to time-delay attacks (such as DoS, DDoS). The

communication delays $\overline{\delta}^i$ and $\overline{\beta}^i$ for P_i are then modeled as follows:

$$\begin{aligned}\overline{\delta}^i\left(SI^i, SI^{-i}\right) &= \left(1 - SI^i\right)\cdot\overline{\delta} + \alpha\left(n\left(P_{-i} \mid SI^{-i} = 0\right)\right)\\ &\quad\cdot\overline{\delta},\\ \overline{\beta}^i\left(SI^i, SI^{-i}\right) &= \underbrace{\left(1 - SI^i\right)\cdot\overline{\beta}}_{\text{direct delays}}\\ &\quad+\underbrace{\alpha\left(n\left(P_{-i} \mid SI^{-i} = 0\right)\right)\cdot\overline{\beta}}_{\text{indirect delays}},\end{aligned} \tag{11}$$

where $n(P_{-i} \mid SI^{-i} = 0)$ indicates the number of players (excluding P_i) who do not invest in security. α is the discount parameter and is assumed as a strictly increasing function with maximum and minimum being set as $\alpha\ (n = m - 1)$ and $\alpha\ (n = 0)$, where m is the total number of players. Thus, α reflects the indirect influence that insecure individual CPS has on P_i via common network.

In (11), the first term reflects the direct delays caused by P_i's decision on security investment, while the second one indicates the indirect delays from common network, which are caused by other insecure individuals.

Remark 2. Two reasonable explanations as follows indicate the soundness of (11) with respect to $\overline{\delta}^i$ and $\overline{\beta}^i$.

(1) If P_i makes a security investment against time-delay attack, part of delays can then be eliminated due to the unwillingness of rational attacker. However, it still cannot avoid the delays from common communication network caused by other individuals under attack, which corresponds to our definition in (11) that when $SI^i = 1$, both $\overline{\delta}^i$ and $\overline{\beta}^i$ merely depend on the number of other insecure individuals.

(2) If one individual CPS invests in security, the overall security level of distributed CPS will therefore increase, which indicates that, with a higher number of secure individual CPSs, rational attackers will be less willing to implement time-delay attack, and then the expected value of stochastic delays will be relatively lower with both better security levels in cyber layer and control performance being obtained by each individual CPS. This is also reflected by (11), since for P_i, when $SI^i = 1$, both $\overline{\delta}^i$ and $\overline{\beta}^i$ will decrease, and meanwhile for P_{-i}, α reduces with the decrement of the number of insecure individuals, $n(P_{-i} \mid SI^{-i} = 0)$.

3. Pure-Strategy Equilibria Analysis for Two-Player SISG

As the SISG we describe is game of complete information, pure-strategy equilibria always exist, and the pure-strategy equilibria for both two-player symmetric and asymmetric SISG are analyzed in this section, while that of m-player SISG will also be discussed for both symmetric and asymmetric situation in the next section.

Table 3: Social payoff for two-player symmetric SISG.

Strategy pair	Overall payoff
$\{I_L, I_F\}$	$J^{\text{Social}*}\{I_L, I_F\} = 2\cdot(J_P^*\{I_L, I_F\} + l)$
$\{NI_L, I_F\}$	$J^{\text{Social}*}\{NI_L, I_F\} = 2\cdot J_P^*\{NI_L, I_F\} + l$
$\{I_L, NI_F\}$	$J^{\text{Social}*}\{I_L, NI_F\} = 2\cdot J_P^*\{I_L, NI_F\} + l$
$\{NI_L, NI_F\}$	$J^{\text{Social}*}\{NI_L, NI_F\} = 2\cdot J_P^*\{NI_L, NI_F\}$

3.1. Pure-Strategy Equilibria for Two-Player Symmetric SISG

Theorem 3. *In two-player symmetric SISG, pure-strategy subgame perfect Nash equilibria (SPNE) will always exist and are symmetric. Depending on different value of* $l \in \mathbb{R}_+$,

(1) *when* $J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} \leq J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}$, *the SPNE is*

$$\begin{aligned}&\{NI_L, NI_F\}, \quad \text{if } l > l^1_{\max}\\ &\{NI_L, I_F\}, \quad \text{if } l^1_{\min} < l \leqslant l^1_{\max}\\ &\{I_L, I_F\} \text{ or } \{NI_L, I_F\} \quad \text{if } l = l^1_{\min}\\ &\{I_L, I_F\}, \quad \text{if } l < l^1_{\min},\end{aligned} \tag{12}$$

(2) *when* $J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} > J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}$, *the SPNE is*

$$\begin{aligned}&\{NI_L, NI_F\} \quad \text{if } l > l^2_{\max}\\ &\{I_L, I_F\} \quad \text{if } l \leqslant l^2_{\max},\end{aligned} \tag{13}$$

where $l^1_{\max} = J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}$, $l^1_{\min} = J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\}$, *and* $l^2_{\max} = J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\}$.

In addition, we further explore the preference of administrator (social planner) seeking for social optimum, that is, minimizing overall payoff of the distributed CPSs. Since three SPNE are possibly reached, we derive social payoff under each strategy pair, as shown in Table 3.

Since $J^{\text{Social}*}\{NI_L, I_F\}$ is equal to $J^{\text{Social}*}\{I_L, NI_F\}$, we firstly derive three critical points, $l_1 = 2\cdot(J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\})$, $l_2 = 2\cdot(J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\})$, and $l_3 = J_P^*\{NI_L, NI_F\} - J_P^*\{I_L, I_F\}$, at which we have $J^{S*}\{I_L, I_F\} = J^{S*}\{NI_L, I_F\}$, $J^{S*}\{NI_L, I_F\} = J^{S*}\{NI_L, NI_F\}$, and $J^{S*}\{I_L, I_F\} = J^{S*}\{NI_L, NI_F\}$. According to Theorem 3, two situations for social optimum are discussed.

(1) When $J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} < J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}$ is satisfied, we have $l_1 < l_3 < l_2$, and the socially optimum choices are as shown in Table 4. The relationship between socially and individually optimal choices is directly reflected in Figure 7, through which the strategic gap is clearly distinguished. It is noted that, in Figure 7(a), $l_1' = l_1 > l^1_{\max}$, while, in Figure 7(b), $l_1'' = l_1 < l^1_{\max}$.

(2) When $J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} > J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}$ is satisfied, we have $l_2 < l_3 < l_1$, and socially, individually optimal choices and their relationship are also as shown in Table 4 and Figure 7. It is noted that, in Figure 7(c), $l_2' = l_2 > l^2_{\max}$, while, in Figure 7(d), $l_2'' = l_2 < l^2_{\max}$.

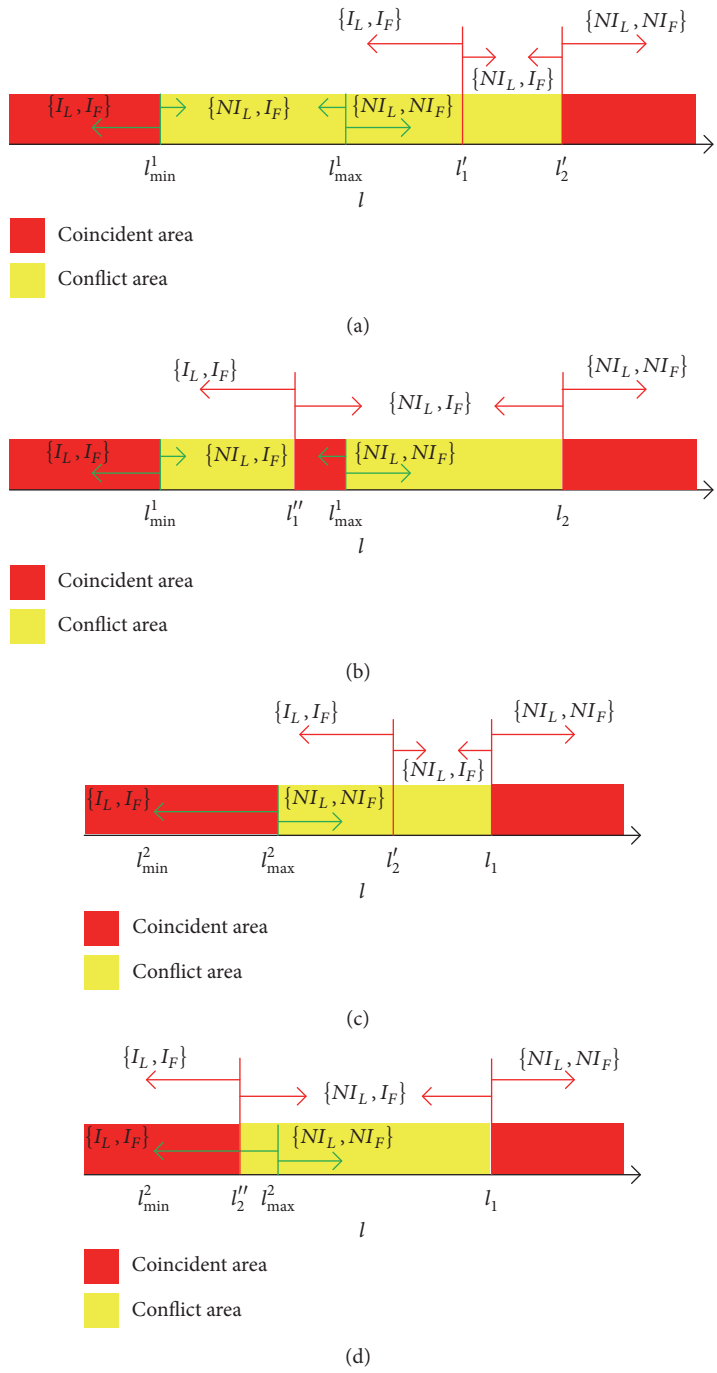

Figure 7: The relationship between socially and individually optimal choices in two-player symmetric SISG.

Table 4: Socially optimal choices for different magnitude of l.

Magnitude of l	Socially optimum choice
$l \geqslant \max[l_1, l_2] > l_3 > \min[l_1, l_2]$	$\{NI_L, NI_F\}$
$\max[l_1, l_2] > l \geqslant l_3 > \min[l_1, l_2]$	$\{NI_L, I_F\}$
$\max[l_1, l_2] > l_3 > l \geqslant \min[l_1, l_2]$	$\{NI_L, I_F\}$
$\max[l_1, l_2] > l_3 > \min[l_1, l_2] > l$	$\{I_L, I_F\}$

3.2. Pure-Strategy Equilibria for Two-Player Asymmetric SISG. We then further analyze the pure-strategy equilibria for two-player asymmetric SISG as given in Figure 4. Similar with building game matrix for two-player symmetric SISG, the strategic form representation of two-player asymmetric SISG is given in Table 5 where I_1 and I_2 are different types of security investment, the cost of which is l_1 and l_2, respectively.

Table 5: Strategic form representation of two-player asymmetric SISG.

		Follower			
		(I_2, I_2)	(I_2, NI_L)	(NI_L, I_2)	(NI_L, NI_L)
Leader	I_1	$l_1 + J_P^*\{I_1, I_2\}$, $l_2 + J_P^*\{I_1, I_2\}$	$l_1 + J_P^*\{I_1, I_2\}$, $l_2 + J_P^*\{I_1, I_2\}$	$l_1 + J_P^*\{I_1, NI_F\}$, $J_P^*\{I_1, NI_F\}$	$l_1 + J_P^*\{I_1, NI_F\}$, $J_P^*\{I_1, NI_F\}$
	NI_L	$J_P^*\{NI_L, I_2\}$, $l_2 + J_P^*\{NI_L, I_2\}$	$J_P^*\{NI_L, NI_F\}$, $J_P^*\{NI_L, NI_F\}$	$J_P^*\{NI_L, I_2\}$, $l_2 + J_P^*\{NI_L, I_2\}$	$J_P^*\{NI_L, NI_F\}$, $J_P^*\{NI_L, NI_F\}$

The following theorem concerning equilibria of two-player asymmetric SISG is put forward for obtaining the individually optimal choice, which is given in the form of the solution of SPNE.

Theorem 4. *In two-player asymmetric SISG, pure-strategy subgame perfect Nash equilibria (SPNE) will always exist. Depending on different value of* $l_1, l_2 \in \mathbb{R}_+$,

(1) *when* $J_P^*\{I_1, NI_F\} - J_P^*\{I_1, I_2\} \leq J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_2\}$, *the SPNE is*

$$\begin{aligned}
&\{NI_L, NI_F\} \quad if \begin{cases} l_2 > B \\ l_1 > E \end{cases} \\
&\{I_1, NI_F\} \quad if \begin{cases} l_2 > B \\ l_1 \leq E \end{cases} \quad or \begin{cases} A < l_2 \leq B \\ l_1 \leq C \end{cases} \\
&\{NI_L, I_2\} \quad if \begin{cases} A < l_2 \leq B \\ l_1 > C \end{cases} \quad or \begin{cases} l_2 \leq A \\ l_1 > D \end{cases} \\
&\{I_1, I_2\} \quad if \begin{cases} l_2 \leq A \\ l_1 \leq D \end{cases} \quad or \begin{cases} l_2 \leq A \\ l_1 > D, \end{cases}
\end{aligned} \tag{14}$$

(2) *when* $J_P^*\{I_1, NI_F\} - J_P^*\{I_1, I_2\} > J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_2\}$, *the SPNE is*

$$\begin{aligned}
&\{NI_L, NI_F\} \quad if \begin{cases} l_2 > A \\ l_1 > E \end{cases} \quad or \begin{cases} B < l_2 \leq A \\ l_1 > F \end{cases} \\
&\{I_1, NI_F\} \quad if \begin{cases} l_2 > A \\ l_1 \leq E \end{cases} \\
&\{NI_L, I_2\} \quad if \begin{cases} l_2 \leq B \\ l_1 > D \end{cases} \\
&\{I_1, I_2\} \quad if \begin{cases} B < l_2 \leq A \\ l_1 < F \end{cases} \quad or \begin{cases} l_2 \leq B \\ l_1 \leq D, \end{cases}
\end{aligned} \tag{15}$$

where $A = J_P^*\{I_1, NI_F\} - J_P^*\{I_1, I_2\}$, $B = J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_2\}$, $C = J_P^*\{NI_L, I_2\} - J_P^*\{I_1, NI_F\}$, $D = J_P^*\{NI_L, I_2\} - J_P^*\{I_1, I_2\}$, $E = J_P^*\{NI_L, NI_F\} - J_P^*\{I_1, NI_F\}$, *and* $F = J_P^*\{NI_L, NI_F\} - J_P^*\{I_1, I_2\}$.

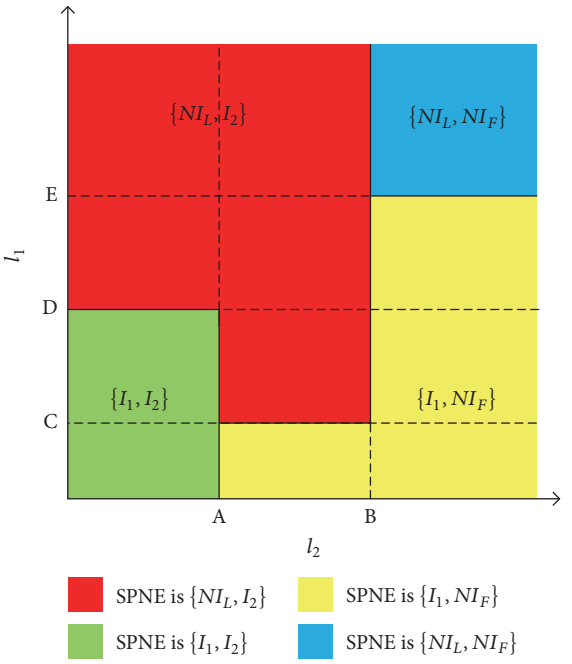

Figure 8: The SPNE of two-player asymmetric SISG when $A \leq B$.

The conclusions made in Theorem 4 can be vividly reflected in the form of two-dimension figures as shown in Figures 8 and 9 where we can clearly distinguish the different SPNE with corresponding conditions.

The optimal choices for social planner in two-player asymmetric SISG are further explored. We derive social payoff under each strategy pair, as shown in Table 6.

According to Theorem 4, two situations are discussed.

(1) When $J_P^*\{I_1, NI_F\} - J_P^*\{I_1, I_2\} \leq J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_2\}$ is satisfied, the socially optimum choices are as shown in Table 7. The relationship between socially and individually optimal choices is directly reflected in Figure 10 where the coincident strategy area is highlighted by red blocks and the rest area denotes the strategy gap between individual and social players.

(2) When $J_P^*\{I_1, NI_F\} - J_P^*\{I_1, I_2\} > J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_2\}$ is satisfied, the socially optimum choices are as shown in Table 8. The relationship between socially and individually optimal choices is directly reflected in Figure 11 where the coincident strategy area is highlighted by red blocks and the rest area denotes the strategy gap between individual and social players.

Table 6: Social payoff for two-player asymmetric SISG.

Magnitude of l	Socially optimum choice
$\{I_1, I_2\}$	$J^{\text{Social}*}\{I_1, I_2\} = l_1 + l_2 + 2 \cdot J_P^*\{I_1, I_2\}$
$\{NI_L, I_2\}$	$J^{\text{Social}*}\{NI_L, I_F\} = l_2 + 2 \cdot J_P^*\{NI_L, I_2\}$
$\{I_1, NI_F\}$	$J^{\text{Social}*}\{I_1, NI_F\} = l_1 + 2 \cdot J_P^*\{I_1, NI_F\}$
$\{NI_L, NI_F\}$	$J^{\text{Social}*}\{NI_L, NI_F\} = 2 \cdot J_P^*\{NI_L, NI_F\}$

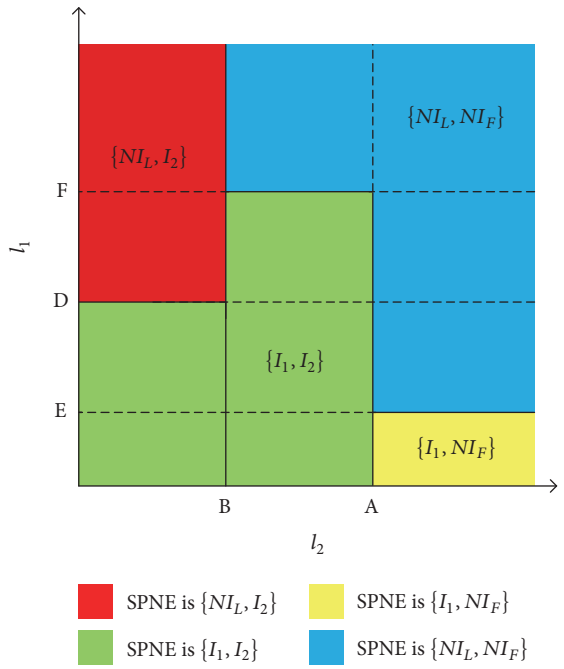

Figure 9: The SPNE of two-player asymmetric SISG when $A > B$.

4. Pure-Strategy Equilibria Analysis for m-Player SISG

In this section, we show how to extend the theorems concerning pure-strategy equilibria to the situation of m-player SISG. Firstly, in the m-player ($m > 2$) symmetric SISG, the SPNE is proved to exist with the corresponding analytical solutions being obtained. Moreover, the socially optimal choices are discussed, and at last the relationship between socially and individually optimal choices is studied with the strategy gap being characterized. According to Figure 5, the theorem concerning m-player symmetric SISG can be easily extended to the asymmetric.

Thus, we consider m-player ($m > 2$) symmetric SISG that all the players excluding P_i act simultaneously, and then according to the strategy chosen by P_{-i}, P_i decides his own optimal strategy.

ξ is used for denoting the number of insecure players excluding P_i, while $\psi_L(\xi) = \{\underbrace{I_L^1, I_L^2, \ldots, I_L^{i-1}}_{m-\xi-1}, \underbrace{NI_L^{i+1}, NI_L^{i+2}, \ldots, NI_L^m}_{\xi}\}$ characterizes the strategy of P_{-i}.

Theorem 5. *In m-player ($m > 2$) SISG, a pure-strategy subgame perfect Nash equilibrium (SPNE) will always exists. Depending on different value of $l \in \mathbb{R}_+$,*

Table 7: Socially optimal choices in two-player asymmetric SISG_1.

Magnitude of l_1	Magnitude of l_2	Socially optimum choice
$l_1 > 2E$	$l_2 > 2B$	$\{NI_L, NI_F\}$
$l_1 \le 2E$		$\{I_1, NI_F\}$
$l_1 > l_2 + 2C$	$2A < l_2 \le 2B$	$\{NI_L, I_2\}$
$l_1 \le l_2 + 2C$		$\{I_1, NI_F\}$
$l_1 > 2D$	$l_2 \le 2A$	$\{NI_L, I_2\}$
$l_1 \le 2D$		$\{I_1, I_2\}$

Table 8: Socially optimal choices in two-player asymmetric SISG_2.

Magnitude of l_1	Magnitude of l_2	Socially optimum choice
$l_1 > 2E$	$l_2 > 2A$	$\{NI_L, NI_F\}$
$l_1 \le 2E$		$\{I_1, NI_F\}$
$l_1 > 2F - l_2$	$2B < l_2 \le 2A$	$\{NI_L, NI_F\}$
$l_1 \le 2F - l_2$		$\{I_1, I_2\}$
$l_1 > 2D$	$l_2 \le 2B$	$\{NI_L, I_2\}$
$l_1 \le 2D$		$\{I_1, I_2\}$

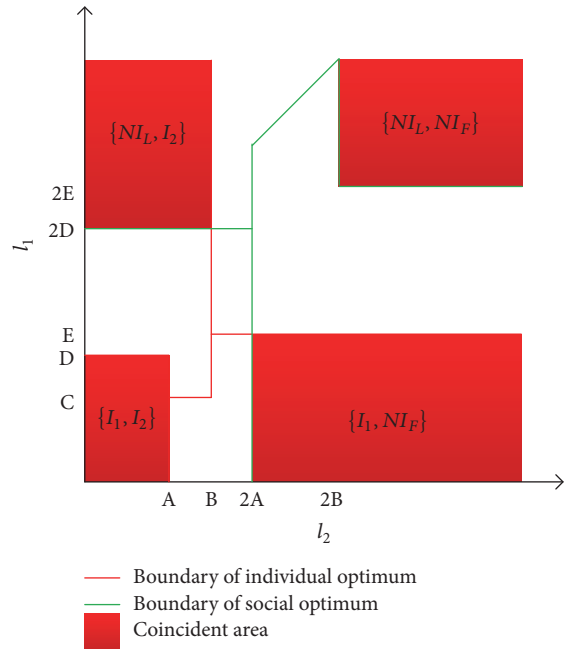

Figure 10: The relationship between socially and individually optimal choices in two-player asymmetric SISG_1.

(1) *when* $\Delta(0) > \Delta(1) > \Delta(2) > \cdots > \Delta(m-2) > \Delta(m-1)$, *the SPNE is*

$$\begin{aligned} &\{\psi_L(\xi = m-1), NI_F\} && \text{if } l \geqslant \Delta(0) \text{ or } \Delta(0) > l > \varpi_1 \\ &\{\psi_L(\xi = m-1), NI_F\} \text{ or } \{\psi_L(\xi = 0), I_F\} && \text{if } l = \varpi_1 \\ &\{\psi_L(\xi = 0), I_F\} && \text{if } l \leqslant \Delta(m-1) \text{ or } \varpi_1 > l > \Delta(m-1), \end{aligned} \tag{16}$$

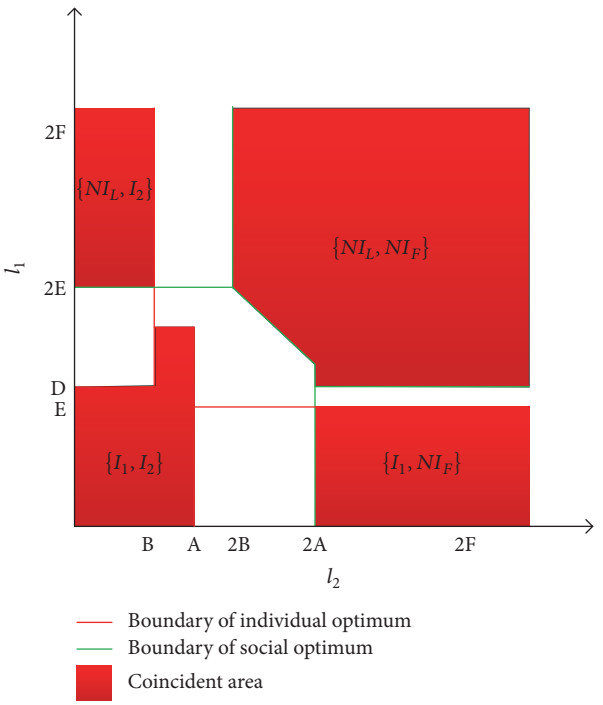

FIGURE 11: The relationship between socially and individually optimal choices in two-player asymmetric SISG_2.

(2) *when* $\Delta(0) < \Delta(1) < \Delta(2) < \cdots < \Delta(m-2) < \Delta(m-1)$, *the SPNE is*

$$\begin{cases} \{\psi_L(\xi = 0), I_F\} & \text{if } l \leqslant \Delta(0) \\ \{\psi_L(\xi = \alpha - 1), NI_F\} & \text{if } \Delta(\alpha - 1) < l < \varpi_2(\alpha) \\ \{\psi_L(\xi = \alpha - 1), NI_F\} \text{ or } \{\psi_L(\xi = \alpha), I_F\} & \text{if } l = \varpi_2(\alpha) \\ \{\psi_L(\xi = \alpha), I_F\} & \text{if } \varpi_2(\alpha) < l < \Delta(\alpha) \\ \{\psi_L(\xi = m - 1), NI_F\} & \text{if } l \geqslant \Delta(m - 1), \end{cases} \tag{17}$$

where $\Delta(\xi) = J_P^*\{\psi_L(\xi), NI_F\} - J_P^*\{\psi_L(\xi), I_F\}$, $\xi \in [0, m-1]$, $\varpi_1 = (J_P^*\{\psi_L(\xi = m-1), NI_F\} - J_P^*\{\psi_L(\xi = 0), I_F\})/(m-1)$, *and* $\varpi_2(\alpha) = J_P^*\{\psi_L(\xi = \alpha), I_F\} - J_P^*\{\psi_L(\xi = \alpha - 1), NI_F\}$, $\alpha \in [1, m-1]$.

We then further discuss the socially optimal choices for m-player symmetric SISG. The payoff function of administrator is denoted in (18). Analogous to the analysis of individually optimal choice, two situations are considered.

$$J^{\text{Social}}(\eta) = \begin{cases} \eta \cdot l + J_P^*\{\psi_L(\xi = m - \eta), I_F\}, & \eta \in [1, m] \\ 0 \cdot l + J_P^*\{\psi_L(\xi = m - 1), NI_F\}, & \eta = 0, \end{cases} \tag{18}$$

where η is the total number of players making investment in security.

Situation 1. One has $\Delta(0) > \Delta(1) > \cdots > \Delta(i) > \cdots > \Delta(m-1)$.

Case 1. One has $l \geqslant \Delta(0) > \Delta(1) > \cdots > \Delta(i) > \cdots > \Delta(m-1)$, $i \in [0, m-1]$.

In accordance with inequality (19), $J^{\text{Social}}(0)$ is the minimum of social cost, and thus $J_P^*\{\psi_L(\xi = m-1), NI_F\}$ is the optimal choice for administrator if $l \geqslant \Delta(0)$.

$$\begin{aligned} & J^{\text{Social}}(\eta') - J^{\text{Social}}(\eta' - 1) \\ & = l + J_P^*(\psi_L(\xi = m - \eta'), I_F) \\ & \quad - J_P^*(\psi_L(\xi = m - \eta' + 1), I_F) \\ & > \Delta(m - \eta') + J_P^*(\psi_L(\xi = m - \eta'), I_F) \\ & \quad - J_P^*(\psi_L(\xi = m - \eta' + 1), I_F) = 0, \\ & J^{\text{Social}}(1) - J^{\text{Social}}(0) \\ & = l + J_P^*(\psi_L(\xi = m - 1), I_F) \\ & \quad - J_P^*(\psi_L(\xi = m - 1), NI_F) \\ & > \Delta(m - 1) + J_P^*(\psi_L(\xi = m - 1), I_F) \\ & \quad - J_P^*(\psi_L(\xi = m - 1), NI_F) = 0. \end{aligned} \tag{19}$$

Case 2. One has $\Delta(0) > \Delta(1) > \cdots > \Delta(\alpha - 1) > l > \Delta(\alpha) > \cdots > \Delta(m-1)$, $\alpha \in [1, m-1]$.

In Case 2, $J^{\text{Social}}(\eta)$ is an increasing (resp., decreasing) function when $1 \leqslant \eta \leqslant m - 1 - \alpha$ (resp., $m \geqslant \eta \geqslant m - \alpha$) with the minimum being determined as $J^{\text{Social}}(1)$ (resp., $J^{\text{Social}}(m)$). By comparing the value of $J^{\text{Social}}(0)$, $J^{\text{Social}}(1)$, and $J^{\text{Social}}(m)$ under different magnitude of l, the socially minimal cost is derived as follows:

$$\min\left[J^{\text{Social}}(0), J^{\text{Social}}(1), J^{\text{Social}}(m)\right] = \begin{cases} J^{\text{Social}}(0), & l \geqslant \varpi_3 \\ J^{\text{Social}}(m), & \varpi_4 \leqslant l < \varpi_3 \\ J^{\text{Social}}(m), & l < \varpi_4, \end{cases} \tag{20}$$

where $\varpi_3 = (J_P^*(\psi_L(\xi = m-1), NI_F) - J_P^*(\psi_L(\xi = 0), I_F))/m$ and $\varpi_4 = (J_P^*(\psi_L(\xi = m-1), I_F) - J_P^*(\psi_L(\xi = 0), I_F))/(m-1)$.

Case 3. One has $\Delta(0) > \Delta(1) > \cdots > \Delta(i) > \cdots > \Delta(m-1) \geqslant l$, $i \in [0, m-1]$.

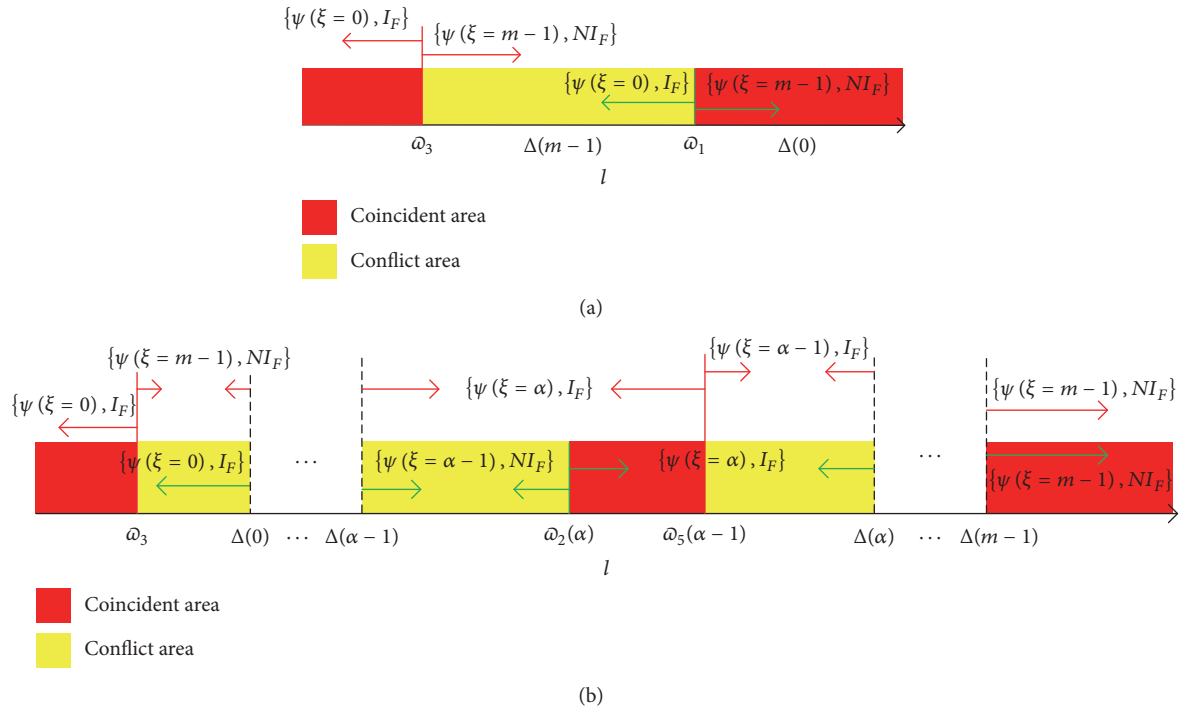

FIGURE 12: The relationship between socially and individually optimal choices in m-player SISG.

According to inequality (21), $J^{\text{Social}}(0)$ (resp., $J^{\text{Social}}(m)$) is the minimal cost when $l > \varpi_3$ (resp., $l < \varpi_3$). When $l = \varpi_3$, both $J^{\text{Social}}(0)$ and $J^{\text{Social}}(m)$ are socially minimal cost.

$$\begin{aligned} &J^{\text{Social}}\left(\eta'\right) - J^{\text{Social}}\left(\eta' - 1\right) \\ &\quad = l + J_P^*\left(\psi_L\left(\xi = m - \eta'\right), I_F\right) \\ &\qquad - J_P^*\left(\psi_L\left(\xi = m - \eta' + 1\right), I_F\right) \\ &\quad < \Delta\left(m - \eta'\right) + J_P^*\left(\psi_L\left(\xi = m - \eta'\right), I_F\right) \\ &\qquad - J_P^*\left(\psi_L\left(\xi = m - \eta' + 1\right), I_F\right) = 0, \\ &J^{\text{Social}}(m) - J^{\text{Social}}(0) = l - \varpi_3. \end{aligned} \tag{21}$$

Situation 2. One has $\Delta(0) < \Delta(1) < \Delta(2) < \cdots < \Delta(m-2) < \Delta(m-1)$.

Case 1. One has $l \leqslant \Delta(0) < \Delta(1) < \cdots < \Delta(i) < \cdots < \Delta(m-2) < \Delta(m-1)$, $i \in [0, m-1]$.

Similar to Case 3 of Situation 1, $J^{\text{Social}}(0)$ (resp., $J^{\text{Social}}(m)$) is the minimal cost when $\Delta(0) \geqslant l > \varpi_3$ (resp., $l < \varpi_3$). When $l = \varpi_3$, both $J^{\text{Social}}(0)$ and $J^{\text{Social}}(m)$ are socially minimal cost.

Case 2. One has $\Delta(0) < \Delta(1) < \cdots < \Delta(\alpha-1) < l < \Delta(\alpha) < \cdots < \Delta(m-1)$, $\alpha \in [1, m-1]$.

In Case 2, $J^{\text{Social}}(\eta)$ is an increasing (resp., decreasing) function when $m - \alpha \leqslant \eta \leqslant m$ (resp., $m - \alpha - 1 \geqslant \eta \geqslant 1$) with the minimum being determined as $J^{\text{Social}}(m-\alpha)$ (resp., $J^{\text{Social}}(m-\alpha-1)$). According to (22), $J^{\text{Social}}(m-\alpha)$ (resp., $J^{\text{Social}}(m-\alpha-1)$) is the minimum when $l > \varpi_5(\alpha)$ (resp., $l < \varpi_5(\alpha)$). When $l = \varpi_5(\alpha)$, both $J^{\text{Social}}(m-\alpha)$ and $J^{\text{Social}}(m-\alpha-1)$ are socially minimal cost.

$$\begin{aligned} &J^{\text{Social}}(m-\alpha) - J^{\text{Social}}(m-\alpha-1) > 0 \Longrightarrow \\ &l + J_P^*\left(\psi_L(\xi = \alpha), I_F\right) - J_P^*\left(\psi_L(\xi = \alpha+1), I_F\right) > 0 \Longrightarrow \\ &l > J_P^*\left(\psi_L(\xi = \alpha+1), I_F\right) - J_P^*\left(\psi_L(\xi = \alpha), I_F\right) \\ &\quad = \varpi_5(\alpha). \end{aligned} \tag{22}$$

Case 3. One has $\Delta(0) < \Delta(1) < \cdots < \Delta(i) < \cdots < \Delta(m-2) < \Delta(m-1) \leqslant l$, $i \in [0, m-1]$.

According to inequality (19), $J^{\text{Social}}(0)$ is the socially minimal cost when $l > \Delta(m-1)$. Both $J^{\text{Social}}(0)$ and $J^{\text{Social}}(1)$ are the minimum of cost when $l = \Delta(m-1)$.

The relationship between socially and individually optimal choices in m-player SISG is characterized in Figure 12, where Figure 12(a) is for Situation 1, while Figure 12(b) is for Situation 2.

In the conflict area as denoted in Figures 7, 10, 11, and 12, we can clearly distinguish that the individually optimal choices differ from socially optimal ones, and the tendency of individual player's underinvestment reflects the existence of negative externalities and is in accordance with the strategy gap between individual and social players proposed in [27].

5. Numerical Case Studies

In this section, we refer to the simulation example given in [28, 29] and then build our experimental platform for numerical case studies. The distributed and hierarchical

Table 9: Executing time of encryption and length of command of plaintext.

Time (ms)\length (B)	144	272	400	528	656	784	912	1040
AES	7.48	67.21	127.18	187.24	246.88	306.46	366.37	432.94
DES Encryption	14.72	85.59	151.22	225.12	299.94	475.34	549.98	620.94

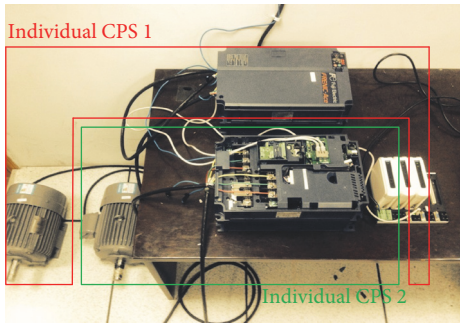

Figure 13: Distributed and hierarchical framework of our experiment platform.

framework of our experiment platform is as shown in Figure 13, and more details of plant devices are further provided in Figure 14. In both Figures 13 and 14, two individual CPSs consisted of engineer station as cyber component and inverter together with motor as physical component can be clearly distinguished.

The object of administrator in chief engineer station is to choose a coincident and optimal defense strategy (configuration of security countermeasures) for individual player and social planner under external attacks. The man-in-the-middle (MIM) attack is considered, and meanwhile encryption algorithms including AES and DES are regarded as security countermeasures.

Due to its high threats and low possibility of being detected, MIM attack against time synchronization is considered. Once the vulnerability of time synchronization protocol is exploited by MIM attacker, the main-clock device will be completely spoofed while the slave-clock devices will be fully manipulated. The attacker is capable of mastering the real-time clock of slave-clock devices by sending bogus command messages without being detected by main-clock device. In our case, when CPS is compromised by MIM attacker, all the devices will then be synchronized by attacker with S-C delay, δ, and C-A delay, β, being manipulated. For more details about man-in-the-middle (MIM) attack against time synchronization, the reader can refer to [30].

The experiment is carried out according to the following procedures.

Step 1 (determination of security configuration). The security configuration is determined by chief engineer station acting as a social planner, according to which each individual CPS is equipped with a certain security countermeasure, AES or DES.

Step 2 (introduction of MIM attack). MIM attack launched by external host computers is introduced into CPSs via common network. The victimized devices will be cheated to receive synchronization command messages with false timestamps and then lose the synchronization to other devices in the same network. The delays in physical plant are therefore produced due to the out-of-synchronization.

Step 3 (realization of $H\infty$-optimal control under MIM attack and quantification of cyber cost). PLC together with individual engineer station equipped with security countermeasure will deal with the control problems under MIM attack by sending control command messages to plant devices, inverter, and motor. In addition, the individual engineer station is realized as an embedded platform (ATM91SAM9XE512QU, MCU 32 bits, 180 Mhz) for proceeding encryption process and quantifying the cost of security countermeasure in cyber layer. It is noted that we refer to [31–33] for realizing $H\infty$-optimal control through PLC and meanwhile the feedback macrocycle time of motors in physical plant is set to be 5 seconds.

We quantify the value of l for each defense strategy based on the test data for executing time of encrypting/decrypting sensor or control command of plaintext as shown in Table 9, since the longer time that MCU spends on encryption, the more computational resources of defender will be occupied and thus the more cost defender should pay.

The mapping function for $T_{\text{AES}}/T_{\text{DES}}$ and $l_{\text{AES}}/l_{\text{DES}}$ is defined as $l_{\text{AES/DES}} = \eta \cdot (T_{\text{AES/DES}}/(T_{\text{AES/DES}} + T_{\text{DES/AES}}))$, where η is the weighing parameter and given as 0.1 in our case. In addition, we consider the situation that the length of both sensor and control command is configured as 1040 and thus l_{AES} and l_{DES} are obtained as 0.0411 and 0.0589, respectively.

Step 4 (quantification of physical cost). The data of output AC voltage returned from inverter is used for quantifying the performance of controlled plant.

Step 5 (repeated experiments with different security configuration). Different security configuration is implemented by chief engineer station and the corresponding overall cost in physical layer and cyber layer can be obtained similarly through Steps 1–4.

Since the feedback macrocycle time of physical signal is 5 seconds and meanwhile the maximum of encryption executing time in the closed-loop communication channel is 1.24 seconds, there is enough time left for individuals security decision-making and processing $H\infty$-optimal control algorithm. Additionally, the bandwidth in our case is 1 Gbps and thus the delays on communication channel are microsecond level or even nanosecond level. As a consequence, the feasibility and performance of proposed algorithm are ensured.

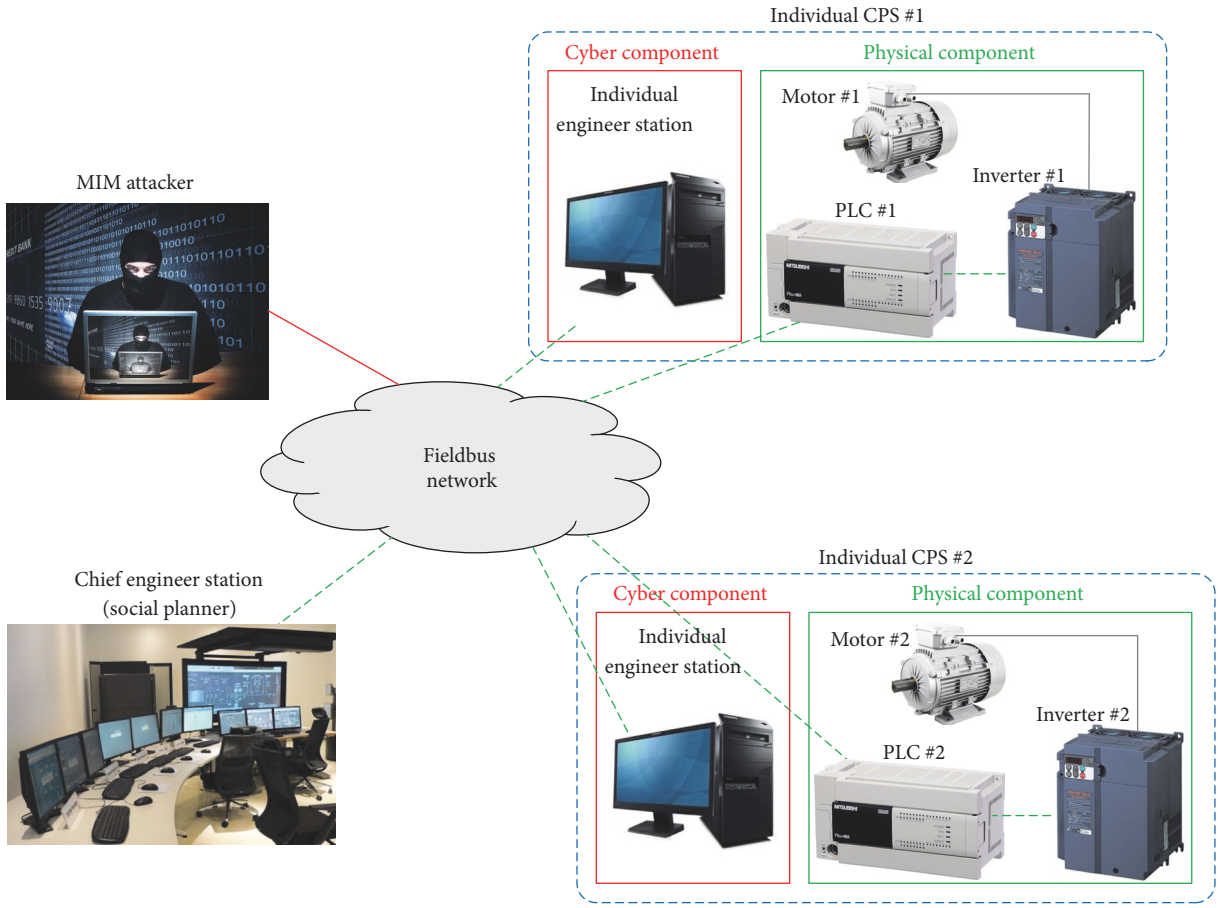

Figure 14: The plant device of experiment platform.

The discrete-time model at half-load operating point can be found in [28, 29]:

$$A = \begin{bmatrix} 0.9226 & -0.6330 & 0 \\ 1.0 & 0 & 0 \\ 0 & 1.0 & 0 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 0.5 \\ 0 \\ 0.2 \end{bmatrix} \tag{23}$$

$$B_2 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

$$D = \begin{bmatrix} 0.1 & 0 & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 23.738 & 20.287 & 0 \end{bmatrix}.$$

As being manipulated by MIM attacker, S-C delay and C-A delay of CPS equipped with either AES or DES are given by the same matrix and the corresponding cost in physical layer J_P^* under different cyber strategy pairs is obtained as follows:

Table 10: Individually optimal choices for experiment platform.

Magnitude of l	Individually optimum choice
$l > l_{\max}^2 = 0.0413$	$\{NI_L, NI_F\}$
$l \le l_{\max}^2 = 0.0413$	$\{I_L, I_F\}$

$$\overline{\delta} = \overline{\beta} = \begin{matrix} \\ I_L \\ NI_L \end{matrix} \begin{matrix} \begin{matrix} I_F & NI_F \end{matrix} \\ \begin{bmatrix} 0.01 & 0.04 \\ 0.04 & 0.06 \end{bmatrix} \end{matrix},$$

$$J_P^* = \gamma^* = \begin{matrix} \\ I_L \\ NI_L \end{matrix} \begin{matrix} \begin{matrix} I_F & NI_F \end{matrix} \\ \begin{bmatrix} 0.0994 & 0.1407 \\ 0.1407 & 0.1691 \end{bmatrix} \end{matrix}. \tag{24}$$

We will then have $J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} = 0.0413 > J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\} = 0.0284$. According to Theorem 3, when $J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} > J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}$ and $l > l_{\max}^2$ (resp., $l \le l_{\max}^2$) are satisfied, the SPNE would be $\{NI_L, NI_F\}$ (resp., $\{I_L, I_F\}$) as listed in Table 10.

Furthermore, in accordance with the analysis in Section 3.2, the socially optimal choices for different magnitude of l are obtained in Table 11 with l_1, l_2, and l_3 being computed as 0.0826, 0.0568, and 0.0697, respectively. Additionally, the

Table 11: Socially optimal choices in experiment platform.

Magnitude of l	Socially optimum choice
$l \geq 0.0826$	$\{NI_L, NI_F\}$
$0.0697 \leq l < 0.0826$	$\{NI_L, I_F\}$
$0.0568 \leq l < 0.0697$	$\{NI_L, I_F\}$
$l < 0.0568$	$\{I_L, I_F\}$

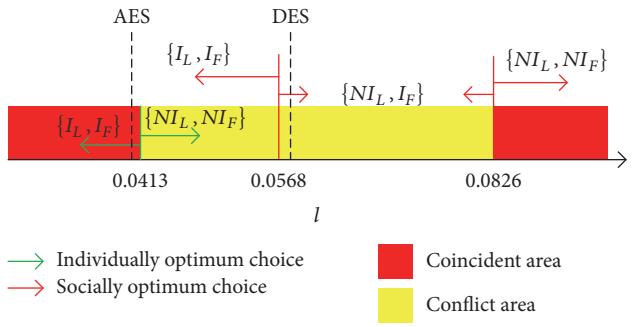

Figure 15: The socially and individually optimum choices in experiment platform.

magnitude of l for each encryption algorithm (l_A for AES, l_D for DES) is quantified based on the test of occupying rate of the hardware resource, with l_A and l_D being determined as 0.0391 and 0.061, respectively.

The relationship between socially and individually optimal choices can then be depicted in Figure 15, where we can clearly distinguish the coincident and conflict area and meanwhile recognize the fact that, by setting the security configuration of applying AES on each individual CPS, the social planner can achieve both individual and social optimum. As a consequence, in this case, the security configuration of both individuals being equipped with AES is optimal.

It is easy to extend our example to m-player situation following the theorem we propose in Section 4, and there would be 2^{m-1} boundaries in Figure 15 for distinguishing the gap between individually and socially optimal choices under different value of l.

6. Concluding Remarks

In this article, we explore the interdependent security of CPS with distributed and hierarchical framework. SISG is proposed for characterizing the interactions between individual CPSs, which are selfish but nonmalicious, and meanwhile the payoff function is formulated from a cross-layer perspective. The pure-strategy equilibria for two-player symmetric SISG are firstly analyzed with the strategy gap between individual and social optimum being distinguished. The result is further extended to asymmetric and m-player SISG. At last, a numerical case study is analyzed by applying the proposed theorems in order to obtain the comprehensively optimal security decision for administrator.

As future work, we are interested in investigating the game with incomplete information due to the fact that the information on common network might not be fully trustable and cannot accurately reflect the actual security choices of other players either. Since we have already discussed the different cyber cost function, another interesting extension of our work would be to consider the CPSs of different physical plants where more types of control model (such as time-delay system, stochastic system) would be taken into account. In addition, when applying the proposed theorems in solving the practical security decision-making problems in m-player scenarios, the state space explosion problem caused by the geometric increase of payoff matrix dimension will complicate the analysis and corresponding results, and it would be further discussed in our following work.

Appendix

A. Proof of Theorem 3

In the second stage of SISG described in Figure 2, there contains two subgames, and meanwhile the follower has four pure strategies, (I_F, I_F), (I_F, NI_F), (NI_F, I_F), and (NI_F, NI_F). According to payoff function given in Table 1, following four inequalities and two equations can be derived for determining the optimal strategy for individual player.

$$J_P^*\{I_L, I_F\} + l > J_P^*\{I_L, NI_F\} \quad (A.1)$$

$$J_P^*\{I_L, I_F\} + l = J_P^*\{I_L, NI_F\} \quad (A.2)$$

$$J_P^*\{I_L, I_F\} + l < J_P^*\{I_L, NI_F\} \quad (A.3)$$

$$J_P^*\{NI_L, I_F\} + l > J_P^*\{NI_L, NI_F\} \quad (A.4)$$

$$J_P^*\{NI_L, I_F\} + l = J_P^*\{NI_L, NI_F\} \quad (A.5)$$

$$J_P^*\{NI_L, I_F\} + l < J_P^*\{NI_L, NI_F\}. \quad (A.6)$$

We then discuss existence of SPNE in the following situations.

Situation 1. When inequalities (A.1) and (A.4) are satisfied, optimal strategy for the follower would be (NI_F, NI_F), which is denoted as red branch in Figure 16(a); that is, in both subgames 1 and 2, not investing in security would be the optimal choice for follower. For leader, two possible gaming paths, $\{I_L, NI_F\}$ and $\{NI_L, NI_F\}$, can then be procured, in which the payoff of leader is $J_P^*\{I_L, NI_F\} + l$ and $J_P^*\{NI_L, NI_F\}$, respectively. Since inequality (A.4) is satisfied and $J_P^*\{I_L, NI_F\}$ is equal to $J_P^*\{NI_L, I_F\}$, we will have

$$J_P^*\{NI_L, NI_F\} < J_P^*\{I_L, NI_F\} + l. \quad (A.7)$$

Hence, $\{NI_L, NI_F\}$ is proved to be the optimal path (as denoted in Figure 16(b)) and also SPNE in Situation 1, if inequality (A.7) is satisfied. Then inequality (A.8) is obtained.

$$l > \max\left[J_P^*\{I_L, NI_F\} - J_P^*\{I_L, I_F\}, J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}\right]. \quad (A.8)$$

Situation 2. When inequalities (A.1) and (A.6) are satisfied, optimal strategy for the follower would be (NI_F, I_F). Analogous to the analysis of Situation 1, two possible gaming paths

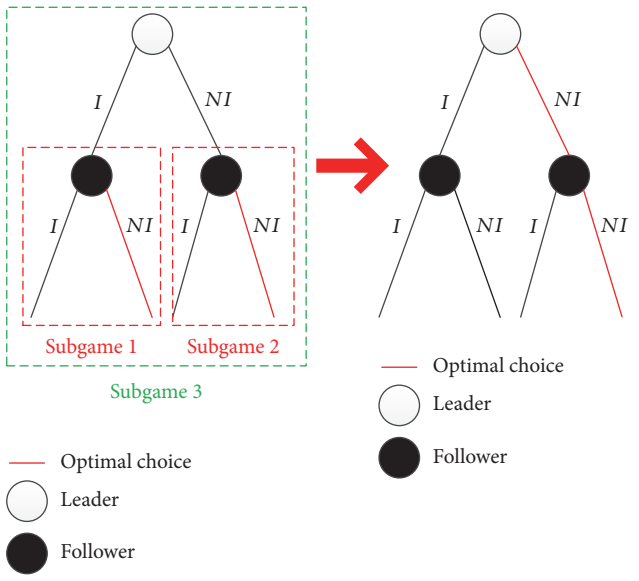

Figure 16: Situation 1 of two-player symmetric SISG equilibria analysis.

for leader are $\{I_L, NI_F\}$ and $\{NI_L, I_F\}$, in which the payoff of leader is $J_P^*\{I_L, NI_F\} + l$ and $J_P^*\{NI_L, I_F\}$. Since $J_P^*\{I_L, NI_F\}$ is equal to $J_P^*\{NI_L, I_F\}$, we will have

$$J_P^*\{NI_L, I_F\} < J_P^*\{I_L, NI_F\} + l. \tag{A.9}$$

Hence, $\{NI_L, I_F\}$ is proved to be the optimal path and also SPNE in Situation 2, if inequality (A.10) is satisfied.

$$\begin{aligned} &J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} \\ &\quad < J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\} \\ &J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} < l \\ &\quad < J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}. \end{aligned} \tag{A.10}$$

Situation 3. When inequalities (A.3) and (A.4) are satisfied, optimal strategy for the follower would be (I_F, NI_F). Analogous to the analysis of Situation 1, two possible gaming paths for leader are $\{I_L, I_F\}$ and $\{NI_L, NI_F\}$, in which the payoff of leader is $J_P^*\{I_L, I_F\} + l$ and $J_P^*\{NI_L, NI_F\}$. According to $J_P^*\{NI_L, NI_F\} > J_P^*\{NI_L, I_F\} > J_P^*\{I_L, I_F\}$ and inequalities (A.3) and (A.4), we will have

$$J_P^*\{I_L, I_F\} + l < J_P^*\{NI_L, NI_F\}. \tag{A.11}$$

Hence, $\{I_L, I_F\}$ is proved to be the optimal path and also SPNE in Situation 3, if inequality (A.12) is satisfied.

$$\begin{aligned} &J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} \\ &\quad > J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\} \\ &J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\} \leqslant l \\ &\quad < J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\}. \end{aligned} \tag{A.12}$$

Situation 4. When inequalities (A.3) and (A.6) are satisfied, optimal strategy for the follower would be (I_F, I_F). Analogous to the analysis of Situation 1, two possible gaming paths for leader are $\{I_L, I_F\}$ and $\{NI_L, I_F\}$, in which the payoff of leader is $J_P^*\{I_L, I_F\}+l$ and $J_P^*\{NI_L, I_F\}$. According to inequalities (A.3) and (A.4), we then have

$$J_P^*\{I_L, I_F\} + l < J_P^*\{NI_L, I_F\}. \tag{A.13}$$

Hence, $\{I_L, I_F\}$ is proved to be the optimal path and also SPNE in Situation 4, if inequality (A.14) is satisfied.

$$\begin{aligned} l < \min &\left[J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\}, J_P^*\{NI_L, NI_F\}\right. \\ &\left. - J_P^*\{NI_L, I_F\}\right]. \end{aligned} \tag{A.14}$$

Situation 5. When (A.2) or (A.5) is satisfied, two cases are discussed.

Case 1 ($J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} < J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}$). In this case, when (A.2) is satisfied, we have $l = l_{\max}^1 = J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}$. For follower, both (NI_F, I_F) and (NI_F, NI_F) are optimal pure strategies since $J^{F*}\{I_L, NI_F\} < J^{F*}\{I_L, I_F\}$ and $J^{F*}\{NI_L, NI_F\} = J^{F*}\{NI_L, I_F\}$ are satisfied. Furthermore, for leader, $J^{L*}\{NI_L, I_F\} < J^{L*}\{NI_L, NI_F\} = J^{L*}\{I_L, NI_F\}$ is satisfied. $\{NI_L, I_F\}$ is therefore obtained as SPNE.

When (A.5) is satisfied, we have $l = l_{\min} = J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\}$. For follower, both (I_F, I_F) and (NI_F, I_F) are optimal pure strategies. Furthermore, for leader, $J^{L*}\{I_L, I_F\} = J^{L*}\{NI_L, I_F\} < J^{L*}\{I_L, NI_F\}$ is satisfied. $\{I_L, I_F\}$ and $\{NI_L, I_F\}$ are then obtained as SPNE.

Case 2 ($J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\} > J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}$). In this case, when (A.2) is satisfied, we have $l = l_{\max}^2 = J_P^*\{NI_L, I_F\} - J_P^*\{I_L, I_F\}$. For follower, both (I_F, NI_F) and (NI_F, NI_F) are optimal pure strategies, while, for leader, $J^{L*}\{I_L, I_F\} < J^{L*}\{I_L, NI_F\}$ and $J^{L*}\{I_L, I_F\} < J^{L*}\{NI_L, NI_F\}$ are both satisfied. Thus, $\{I_L, I_F\}$ is obtained as SPNE.

When (A.5) is satisfied, we have $l = l_{\min} = J_P^*\{NI_L, NI_F\} - J_P^*\{NI_L, I_F\}$. For follower, both (I_F, I_F) and (I_F, NI_F) are optimal pure strategies, while, for leader, $J^{L*}\{I_L, I_F\} < J^{L*}\{NI_L, I_F\} < J^{L*}\{NI_L, NI_F\}$ is satisfied. Thus, $\{I_L, I_F\}$ is obtained as SPNE.

B. Proof of Theorem 4

Similar to the proof line of symmetric SISG, different situations will be discussed separately based on inequalities (B.1), (B.3), (B.4), and (B.6) and equations (B.2) and (B.5) in order to determine the SPNE.

$$l_2 + J_P^*\{I_1, I_2\} > J_P^*\{I_1, NI_F\} \tag{B.1}$$

$$l_2 + J_P^*\{I_1, I_2\} = J_P^*\{I_1, NI_F\} \tag{B.2}$$

$$l_2 + J_P^*\{I_1, I_2\} < J_P^*\{I_1, NI_F\} \tag{B.3}$$

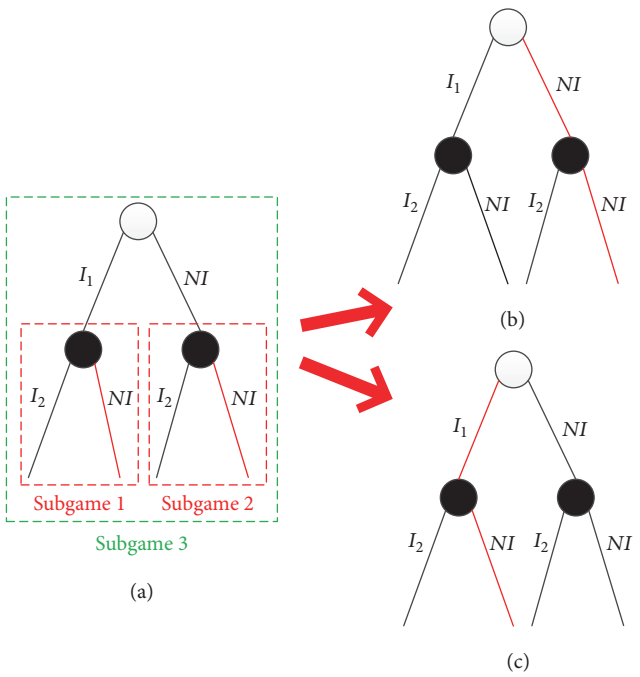

FIGURE 17: Situation 1 of two-player asymmetric SISG equilibria analysis.

$$l_2 + J_P^*\{NI_L, I_2\} > J_P^*\{NI_L, NI_F\} \tag{B.4}$$

$$l_2 + J_P^*\{NI_L, I_2\} = J_P^*\{NI_L, NI_F\} \tag{B.5}$$

$$l_2 + J_P^*\{NI_L, I_2\} < J_P^*\{NI_L, NI_F\}. \tag{B.6}$$

Situation 1. When inequalities (B.1) and (B.4) are satisfied, optimal strategy for the follower would be (NI_F, NI_F), which is denoted as red branch in Figure 17; that is, in both subgames 1 and 2, not investing in security would be the optimal choice for follower. As for leader, two possible gaming paths, $\{I_1, NI_F\}$ and $\{NI_L, NI_F\}$, can then be procured, in which the payoff of leader is $l_1 + J_P^*\{I_1, NI_F\}$ and $J_P^*\{NI_L, NI_F\}$, respectively. The value of l_1 determines the optimal choice and leader. When $l_1 > J_P^*\{NI_L, NI_F\} - J_P^*\{I_1, NI_F\} = E$ (resp., $l_1 \le E$), the optimal path for leader would be NI (resp., I_1), and thus the SPNE will be obtained as $\{NI_L, NI_F\}$ (resp., $\{I_1, NI_F\}$), which is as shown in Figure 17(b) (resp., Figure 17(c)).

The result can be extended to the situation that inequalities (B.1) and (B.6), inequalities (B.3) and (B.4), and (B.3) and (B.6) are satisfied.

Then we discuss the boundary of game, that is, when (B.2) or (B.3) is satisfied.

Situation 2. When (B.2) is satisfied, $l_2 = J_P^*\{I_1, NI_F\} - J_P^*\{I_1, I_2\} = A$ and the following two cases will be considered.

Case 1 ($A > B$). In this case, there exist three possible optimal paths for leader, $\{I_1, I_2\}$, $\{I_1, NI_F\}$, and $\{NI_L, NI_F\}$, the leader's cost of which is $l_1 + J_P^*\{I_1, I_2\}$, $l_1 + J_P^*\{I_1, NI_F\}$, and $J_P^*\{NI_L, NI_F\}$, respectively. Since $l_1 + J_P^*\{I_1, NI_F\} > l_1 + J_P^*\{I_1, I_2\}$, two optimal paths for leader are left and depend on the value of l_1. When $l_1 > J_P^*\{NI_L, NI_F\} - J_P^*\{I_1, I_2\} = F$ ($l_1 \le F$), the optimal choice for leader would be NI (resp., I_1) with the SPNE being obtained as $\{NI_L, NI_F\}$ (resp., $\{I_1, I_2\}$).

Case 2 ($A \le B$). In this case, there exist three possible optimal paths for leader, $\{I_1, I_2\}$, $\{I_1, NI_F\}$, and $\{NI_L, I_2\}$, the leader's cost of which is $l_1 + J_P^*\{I_1, I_2\}$, $l_1 + J_P^*\{I_1, NI_F\}$, and $J_P^*\{NI_L, I_2\}$, respectively. Since $l_1 + J_P^*\{I_1, NI_F\} > l_1 + J_P^*\{I_1, I_2\}$, two optimal paths for leader are left and depend on the value of l_1. When $l_1 > J_P^*\{NI_L, I_2\} - J_P^*\{I_1, I_2\} = D$ ($l_1 \le D$), the optimal choice for leader would be NI (resp., I_1) with the SPNE being obtained as $\{NI_L, I_2\}$ (resp., $\{I_1, I_2\}$).

Similarly, the result can be readily extended to the situation that (B.5) is satisfied.

$$\begin{aligned}
&J^{L*}(\xi = \alpha - 1, NI_F) - J^{L*}(\xi = \alpha, NI_F) = l \\
&\quad + J_P^*(\psi_L(\xi = \alpha - 1), NI_F) \\
&\quad - J_P^*(\psi_L(\xi = \alpha), NI_F) > \Delta(\alpha) \\
&\quad + J_P^*(\psi_L(\xi = \alpha - 1), NI_F) \\
&\quad - J_P^*(\psi_L(\xi = \alpha), NI_F) = 0
\end{aligned} \tag{B.7}$$

$$\begin{aligned}
&J^{L*}(\xi = \alpha - 1, I_F) - J^{L*}(\xi = \alpha, I_F) = l \\
&\quad + J_P^*(\psi_L(\xi = \alpha - 1), I_F) - J_P^*(\psi_L(\xi = \alpha), I_F) \\
&\quad < \Delta(\alpha - 2) + J_P^*(\psi_L(\xi = \alpha - 1), I_F) \\
&\quad - J_P^*(\psi_L(\xi = \alpha), I_F) = 0
\end{aligned} \tag{B.8}$$

$$\begin{aligned}
&J^{L*}\{\xi = 0, I_F\} - J^{L*}\{\xi = m - 1, NI_F\} > 0 \Longrightarrow \\
&(m-1) \cdot l + J_P^*(\psi_L(\xi = 0), I_F) \\
&\quad - J_P^*(\psi_L(\xi = m - 1), NI_F) > 0 \Longrightarrow \\
&l > \frac{J_P^*(\psi_L(\xi = m - 1), NI_F) - J_P^*(\psi_L(\xi = 0), I_F)}{m - 1} \\
&\quad = \varpi_1.
\end{aligned} \tag{B.9}$$

C. Proof of Theorem 5

In the second stage of m-player SISG, m subgames are included, and meanwhile m pure strategies as listed in Table 2 are available for follower. We then extend the equilibria analysis for two-player (in Section 3) to m-player. Two situations are discussed for obtaining the pure-strategy SPNE in m-player SISG.

It is noted that the overall payoff of leader $J^{L*}(\xi = i, NI_F)$ (resp., $J^{L*}(\xi = i, I_F)$) is derived as $(m - 1 - i) \cdot l + J_P^*\{\psi_L(\xi = i), NI_F\}$ (resp., $(m - 1 - i) \cdot l + J_P^*\{\psi_L(\xi = i), I_F\}$).

Situation 1. One has $\Delta(0) > \Delta(1) > \cdots > \Delta(i) > \cdots > \Delta(m - 1)$.

Case 1. When $l \geqslant \Delta(0) > \Delta(1) > \cdots > \Delta(i) > \cdots > \Delta(m-1)$, $i \in [0, m-1]$, the optimal choice for follower in each subgame would be NI_F.

In accordance with inequality (B.7), we have $J^{L*}(\xi = \alpha - 1, NI_F) > J^{L*}(\xi = \alpha, NI_F)$, $\alpha \in [1, m-1]$, with SPNE being determined as $\{\psi_L(\xi = m-1), NI_F\}$.

Case 2. When $\Delta(0) > \Delta(1) > \cdots \Delta(\alpha - 1) > l > \Delta(\alpha) > \cdots > \Delta(m-1)$, $\alpha \in [1, m-1]$, the optimal choice for follower would be $(\underbrace{I_F, \ldots, I_F}_{\alpha}, \underbrace{NI_F, \ldots, NI_F}_{m-\alpha-1})$.

According to inequality (B.7) (resp., (B.8)), $J^{L*}(\xi = m-1, NI_F)$ (resp., $J^{L*}(\xi = 0, I_F)$) is the minimum of cost among all the gaming paths that follower chooses NI_F (resp., I_F). Furthermore, from inequality (B.9), the SPNE is determined as $\{\psi_L(\xi = m-1), NI_F\}$ when $l > \varpi_1$, and $\{\psi_L(\xi = 0), I_F\}$ when $l < \varpi_1$. It is noted that if $l = \varpi_1$, we will have $J^{L*}(\xi = 0, I_F) = J^{L*}(\xi = m-1, NI_F)$, and both $\{\xi = 0, I_F\}$ and $\{\xi = m-1, NI_F\}$ are SPNE.

Case 3. When $\Delta(0) > \Delta(1) > \cdots > \Delta(i) > \cdots > \Delta(m-1) \geqslant l$, $i \in [0, m-1]$, the optimal choice for follower in each subgame would be I_F. According to inequality (B.8), we have $J^{L*}(\xi = \alpha - 1, I_F) < J^{L*}(\xi = \alpha, I_F)$, $\alpha \in [1, m-1]$, with SPNE being determined as $\{\psi_L(\xi = 0), I_F\}$.

Situation 2. One has $\Delta(0) < \Delta(1) < \Delta(2) < \cdots < \Delta(m-2) < \Delta(m-1)$.

Case 1. When $l \leqslant \Delta(0) < \Delta(1) < \cdots < \Delta(i) < \cdots < \Delta(m-2) < \Delta(m-1)$, $i \in [0, m-1]$, the optimal choice for follower in each subgame would be I_F.

In accordance with inequality (C.1), we have $J^{L*}(\xi = \alpha - 1, NI_F) < J^{L*}(\xi = \alpha, NI_F)$, $\alpha \in [1, m-1]$, with SPNE being determined as $\{\psi_L(\xi = 0), I_F\}$.

$$\begin{aligned} &J^{L*}(\xi = \alpha - 1, I_F) - J^{L*}(\xi = \alpha, I_F) \\ &\quad = l + J_P^*(\psi_L(\xi = \alpha - 1), I_F) - J_P^*(\psi_L(\xi = \alpha), I_F) \\ &\quad < \Delta(\alpha - 1) + J_P^*(\psi_L(\xi = \alpha - 1), I_F) \\ &\qquad - J_P^*(\psi_L(\xi = \alpha), I_F) = 0. \end{aligned} \tag{C.1}$$

Case 2. When $\Delta(0) < \Delta(1) < \cdots < \Delta(\alpha - 1) < l < \Delta(\alpha) < \cdots < \Delta(m-1)$, $\alpha \in [1, m-1]$, the optimal choice for follower would be $(\underbrace{I_F, \ldots, I_F}_{m-\alpha-1}, \underbrace{NI_F, \ldots, NI_F}_{\alpha})$.

According to inequality (C.1) (resp., (C.2)), $J^{L*}(\xi = \alpha, I_F)$ (resp., $J^{L*}(\xi = \alpha - 1, NI_F)$) is the minimum of cost among all the gaming paths that follower chooses I_F (resp., NI_F). Furthermore, from inequality (C.3), the SPNE is determined as $\{\psi_L(\xi = \alpha), I_F\}$ when $l > \varpi_2(\alpha)$ and $\{\psi_L(\xi = \alpha - 1), NI_F\}$ when $l < \varpi_2(\alpha)$. It is noted that if $l = \varpi_2(\alpha)$, both $\{\psi_L(\xi = \alpha), I_F\}$ and $\{\psi_L(\xi = \alpha - 1), NI_F\}$ are SPNE.

$$\begin{aligned} &J^{L*}(\xi = \alpha - 1, NI_F) - J^{L*}(\xi = \alpha, NI_F) \\ &\quad = l + J_P^*(\psi_L(\xi = \alpha - 1), NI_F) \\ &\qquad - J_P^*(\psi_L(\xi = \alpha), NI_F) \\ &\quad > \Delta(\alpha) + J_P^*(\psi_L(\xi = \alpha - 1), NI_F) \\ &\qquad - J_P^*(\psi_L(\xi = \alpha), NI_F) = 0 \end{aligned} \tag{C.2}$$

$$\begin{aligned} &J^{L*}(\xi = \alpha - 1, NI_F) - J^{L*}(\xi = \alpha, I_F) > 0 \Longrightarrow \\ &l + J_P^*(\psi_L(\xi = \alpha - 1), NI_F) - J_P^*(\psi_L(\xi = \alpha), I_F) \\ &\quad > 0 \Longrightarrow \\ &l > J_P^*(\psi_L(\xi = \alpha), I_F) - J_P^*(\psi_L(\xi = \alpha - 1), NI_F) \\ &\quad = \varpi_2(\alpha). \end{aligned} \tag{C.3}$$

Case 3. When $\Delta(0) < \Delta(1) < \cdots < \Delta(i) < \cdots < \Delta(m-2) < \Delta(m-1) \leqslant l$, $i \in [0, m-1]$, the optimal choice for follower in each subgame would be NI_F. According to inequality (C.2), we have $J^{L*}(\xi = \alpha, NI_F) < J^{L*}(\xi = \alpha - 1, NI_F)$, $\alpha \in [1, m-1]$, with SPNE being determined as $\{\psi_L(\xi = m-1), NI_F\}$.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Science Fund for Creative Research Groups of NSFC (Grant no. 61621002).

References

[1] E. A. Lee, "Cyber physical systems: design challenges," in *Proceedings of the 11th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC '08)*, pp. 363–369, May 2008.

[2] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *Proceedings of the IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*, vol. 60, pp. 4490–4494, IEEE, Melbourne, VIC, Australia, 2011.

[3] T. Sakamoto and A. Chiba, "Experimental security analysis of a modern automobile," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 41, no. 3, pp. 447–462, 2010.

[4] S. Checkoway, D. Mccoy, B. Kantor et al., "Comprehensive experimental analyses of automotive attack surfaces," *Usenix Security Symposium*, vol. 1, article 43.

[5] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in *Critical Infrastructure Protection*, Springer, 2007.

[6] U.S Department of Energy, 21 Steps to Improve Cyber Security of SCADA Networks. [2015-06-07]. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps-SCADA.pdf.

[7] Consultiong Group and CPNI, Good Practice Guide Process Control and SCADA Security PA. [2015-06-07] http://www.cpni.gov.uk/documents/publications/2008/2008031-gpg_scada_security_good_practice.pdf.

[8] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information System Security*, vol. 14, no. 1, pp. 21–32, 2009.

[9] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proceedings of the First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweden.

[10] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc

state estimation," in *Proceedings of the First Workshop on Secure Control Systems Cpsweek*.

[11] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proceedings of the IEEE International Conference on Smart Grid Communications*, vol. 54, pp. 214–219, IEEE, 2010.

[12] M. N. Elbsat and E. E. Yaz, "Robust and resilient finite-time bounded control of discrete-time uncertain nonlinear systems," *Automatica*, vol. 49, no. 7, pp. 2292–2296, 2013.

[13] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Characterization of cascading failures in interdependent cyber-physical systems," *IEEE Transactions on Computers*, vol. 64, no. 8, pp. 2158–2168, 2015.

[14] H. Musso, U. V. Gizycki, U. I. Zhorszky, and D. Bormann, "Small cluster in cyber physical systems: network topology, interdependence and cascading failures," *IEEE Transactions on Parallel Distributed Systems*, vol. 26, no. 8, 2015.

[15] Y. Yuan, H. Yuan, L. Guo, and H. Yang, "Resilient control of networked control system under dos attacks: a unified game approach," *IEEE Transactions on Industrial Informatics*, 2016.

[16] A. D'Innocenzo, F. Smarra, and M. D. Di Benedetto, "Resilient stabilization of Multi-Hop Control Networks subject to malicious attacks," *Automatica*, vol. 71, pp. 1–9, 2016.

[17] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186–192, 2013.

[18] M. Lelarge and J. Bolot, "Network externalities and the deployment of security features and protocols in the internet," *ACM Sigmetrics Performance Evaluation Review*, vol. 36, no. 1, pp. 37–48, 2008.

[19] F. Hare and J. Goldstein, "The interdependent security problem in the defense industrial base: an agent-based model on a social network," *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3-4, pp. 128–139, 2010.

[20] J. Jin, A. Green, and N. Gans, "A stable switched-system approach to obstacle avoidance for mobile robots in SE(2)," in *Proceedings of the 2014 IEEE/RSJ International Conference on Intelligent Robots and Systems, IROS 2014*, pp. 1533–1539, September 2014.

[21] Y. Yuan, F. Sun, and Q. Zhu, "Resilient control in the presence of DoS attack: Switched system approach," *International Journal of Control, Automation and Systems*, vol. 13, no. 6, pp. 1423–1435, 2015.

[22] B. Hamid, S. Gürgens, C. Jouvray, and N. Desnos, "Enforcing S&D pattern design in RCES with modeling and formal approaches," in *Model Driven Engineering Languages and Systems*, Springer, Berlin, Germany, 2011.

[23] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '05)*, pp. 46–57, Chicago, Ill, USA, May 2005.

[24] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 3023–3028, 2015.

[25] A. Abate, S. Amin, M. Prandini, J. Lygeros, and S. Sastry, "Computational approaches to reachability analysis of stochastic hybrid systems," in *Proceedings of the International Conference on Hybrid Systems: Computation and Control*, vol. 4416, pp. 4–17, Springer, 2007.

[26] Q. Zhu and T. Başar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 46–65, 2015.

[27] T. Alpcan and T. Básar, *Network Security: A Decision and Game-Theoretic Approach*, Cambridge University Press, 2010.

[28] F. Yang, Z. Wang, Y. S. Hung, and M. Gani, "H∞ control for networked systems with random communication delays," *IEEE Transactions on Automatic Control*, vol. 51, no. 3, pp. 511–518, 2006.

[29] X.-Y. Li and S.-L. Sun, "H∞ control for networked systems with random delays and packet dropouts," *International Journal of Control, Automation and Systems*, vol. 10, no. 5, pp. 1023–1031, 2012.

[30] J. Shen and D. Feng, "Vulnerability analysis of clock synchronization protocol using stochastic petri net," in *Proceedings of the IEEE International Conference on High PERFORMANCE Computing and Communications*, pp. 615–620, IEEE, 2014.

[31] S. F. Chew, S. Wang, and M. A. Lawley, "Robust supervisory control for product routings with multiple unreliable resources," *IEEE Transactions on Automation Science and Engineering*, vol. 6, no. 1, pp. 195–200, 2009.

[32] B. Riera, R. Benlorhfar, D. Annebicque, F. Gellot, and B. Vigario, "Robust control filter for manufacturing systems: application to PLC training," in *Proceedings of the 18th IFAC World Congress*, pp. 14265–14270, September 2011.

[33] M. Knotek, F. Zezulka, Z. Simeu-Abazi, and Z. Bouredji, "Robust control and its implementation in PLC for Multi-hoist surface treatment lines," in *Proceedings of the IEEE International Conference on Industrial Technology*, vol. 2, pp. 887–890, IEEE Xplore, December 2003.