Game-Theoretic Resilience Analysis of Cyber-Physical Systems

Fei He and Jun Zhuang
State University of
New York at Buffalo

Nageswara S. V. Rao
Oak Ridge
National Laboratory

Chris Y. T. Ma
Advanced Digital
Sciences Center

David K. Y. Yau
Purdue University

Abstract—**We investigate the resilience of cyber physical systems by modeling the interaction between provider and attacker as a simultaneous game that incorporates cyber and physical spaces. Both the provider and attacker aim to maximize their individual utility, which is determined by a trade-off between target revenue and investment cost. The system resilience function is formulated as a power-form product of the survival probabilities of cyber and physical spaces, each with a corresponding correlation coefficient. The contest success functions based on the reinforcement and attack levels are used to estimate the survival probabilities of cyber and physical spaces. We present the provider strategies based on the Nash equilibrium of the game, and analyze the sensitivities with respect to cyber and physical correlation coefficients, target revenues and costs. The results show that these correlation coefficients affect the cyber and physical reinforcement strategies, and also provide new insights into the system resilience.**

I. Introduction

A Cyber-Physical System (CPS) typically represents a close coupling and coordination between its cyber and physical spaces as indicated in several applications, such as critical infrastructures of power systems, network infrastructures, and smart grids; oil and gas distribution; medical-devices; and robotics. In particular, the Supervisory Control and Data Acquisition (SCADA) systems combined with communications networks are expected to increase the efficiency and reliability of energy generation and storage through smart grid technologies. While the information technology and communication layer within a CPS provides the critical computing and communication capabilities, it also poses new challenges to its operation and security. Furthermore, the heterogeneity and interactions between cyber and physical spaces make the modeling of CPS particularly challenging, and indeed might require a new science and technology foundation that is model based, precise and predictable, as pointed out in [7].

Game theory is a relatively new analysis and design tool that is applied in the study of CPS security and reliability, for example, the development of Stackelberg, Markov, and simultaneous games between defender and attacker [1], [2]. The research area of cyber-physical interdependence is still under development; a recent study investigates the cascading failure of an interconnected cyber-physical network by analyzing node failure modes and network topology dynamics [8]. In this paper, we develop a game theory approach to investigate the cyber-physical interdependence and resilience of CPS.

We incorporate cyber and physical correlations into a game formulation, where the provider and attacker have a complete information about each other's strategy and payoff. We use (i) a power-form product of survival probabilities of cyber and physical spaces, each with a corresponding correlation coefficient, to characterize the system resilience, and (ii) contest success functions based on the reinforcement and attack levels to estimate the survival probabilities of cyber and physical spaces. We present the Nash Equilibrium (NE) solutions of the game, and analyze their sensitivities to cyber and physical correlation coefficients, target revenues, and costs. The results show that the correlation coefficients can lead to both monotonic and non-monotonic dependencies between cyber and physical reinforcement and attack efforts. The overall results suggest that the provider can maximize the payoff by utilizing the correlation coefficients and adapting the target revenues, costs and deployment strategies.

We introduce the CPS resilience function in Section II-A. In Section II-B, we evaluate the survival probabilities of cyber and physical spaces using the contest success functions. The utility fucntions of the provider and attacker are formulated in Sections III and IV, respectively. Section V presents NE analysis of the simultaneous game, and Section VI shows a cloud computing infrastructure example and its resilience analysis. Finally, Section VII concludes with implications and future research directions.

II. The system resilience

The survival of a CPS is determined by both cyber and physical spaces, and the failure of either one leads to its breakdown. Furthermore, the degradation of one affects the survival of other, and they jointly determine the *CPS resilience*, namely, the survivability under attacks. The Cobb-Douglas functional form of production [3] formulates the relationship of a single output based on two inputs. We utilize this characterization to formulate the resilience function of CPS in terms of the survival probabilities of cyber and physical spaces (Section II-A). The individual survival probabilities of cyber and physical spaces themselves are estimated by the reinforcement and attack levels using the contest success function [6] in Section II-B. Let $P_c(x_c, y_c)$,

TABLE I. NOTATION THAT IS USED IN THIS PAPER

Notation	Explanation
Parameters:	
$i = c, p$	Cyber and physical space
$\xi_c, \xi_p > 0$	The inherent defense in cyber, and physical space, respectively
$P_c(x_c, x_p, y_c, y_p)$	Cyber survival probability
$P_p(x_c, x_p, y_c, y_p)$	Physical survival probability
$F_{cp}(x_c, x_p, y_c, y_p)$	Cyber-physical system resilience
$g_D \geq 0$	Provider's target revenue
$g_A \geq 0$	Attacker's target revenue
$c_{Dc} \geq 0$	Unit cost of cyber defense
$c_{Dp} \geq 0$	Unit cost of physical defense
$c_{Ac} \geq 0$	Unit cost of cyber attack
$c_{Ap} \geq 0$	Unit cost of physical attack
$a_c > 0$	Cyber-correlation coefficient
$a_p > 0$	Physical-correlation coefficient
Decision variables:	
x_i	Provider's reinforcement in space i
y_i	Attacker's attack in space i
Utilities:	
$U_D(x_c, x_p, y_c, y_p)$	Defender's utility
$U_A(x_c, x_p, y_c, y_p)$	Attacker's utility

$P_p(x_p, y_p)$ denote the survival probabilities of cyber and physical spaces, respectively, where x_c and x_p are the reinforcement levels of cyber and physical spaces, respectively, by the provider; and y_c and y_p are the attack levels of cyber and physical spaces, respectively. Table I shows the notations used in this paper.

A. CPS Resilience Function

We consider the *CPS resilience function* given by

$$F_{cp} = P_c(x_c, y_c)^{a_c} P_p(x_p, y_p)^{a_p} \tag{1}$$

where $a_c, a_p \geq 0$ are cyber and physical *correlation coefficients*, respectively. This CPS resilience function is a measure of its survivability in that it increases with both $P_c(.)$ and $P_p(.)$, and is closely related to CPS survival probability; indeed, under statistical independence the survival probability equals to $F_{cp} = P_c(x_c, y_c) P_p(x_p, y_p)$, where both correlation coefficients are 1. Deviations of cyber and physical correlation coefficients from 1 represent different levels and types of cyber-physical correlations, as discussed in the following. We assume $F_{cp}(x_c, x_p, y_c, y_p)$ is continuously differentiable and $P_p, P_c > 0$. The effect of cyber correlation coefficient shows that $\frac{\partial F_{cp}}{\partial a_c} = F_{cp} \ln P_c < 0$, $\frac{\partial^2 F_{cp}}{\partial {a_c}^2} = {P_c}^{a_c} {P_p}^{a_p} (\ln P_c)^2 > 0$; and similarly, the effect of physical correlation coefficient shows that $\frac{\partial F_{cp}}{\partial a_p} = F_{cp} \ln P_p < 0$, $\frac{\partial^2 F_{cp}}{\partial {a_p}^2} = {P_c}^{a_c} {P_p}^{a_p} (\ln P_p)^2 > 0$. Thus, CPS resilience function is convex and decreasing in cyber and physical correlation coefficients. We now

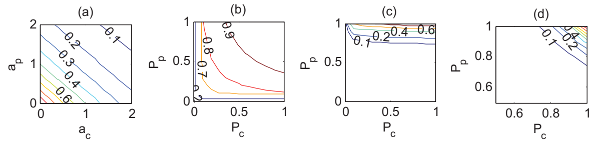


Fig. 1. Isoquants of $F_{cp} = {P_c}^{a_c} {P_p}^{a_p}$, given (a) P_c = 0.5, P_p = 0.5; (b) a_c = 0.1, a_p = 0.1; (c) a_c = 0.2, a_p = 8; (d) a_c = 8, a_p = 8

consider the marginal survivability of cyber space, that is $\frac{\partial F_{cp}}{\partial P_c} = a_c {P_p}^{a_p} {P_c}^{a_c - 1} \geq 0$, and $\frac{\partial^2 F_{cp}}{\partial {P_c}^2} =$

$$a_c(a_c - 1) {P_p}^{a_p} {P_c}^{a_c - 2} \begin{cases} < 0 & \text{if } 0 \leq a_c < 1 \\ = 0 & \text{if } a_c = 1 \\ > 0 & \text{if } a_c > 1 \end{cases} \tag{2}$$

Thus, CPS resilience function increases in P_c and P_p, and the rate of increase can be positive, zero or negative, depending on the value of a_c and a_p. Figures 1(a); (b), (c), and (d) show the isoquants when $\{a_c, a_p\}$, and $\{P_c, P_p\}$ vary, respectively. There is a *complementary effect* between the cyber and physical spaces when a_c and a_p are relatively small, and a *substitution effect* when a_c and a_p are large. When a_c is relatively low and a_p is relatively large, (for example, $a_c = 0.2$ and $a_p = 8$ in Figure 1 (c)), an increase in cyber survival probability, P_c, can effectively increase CPS survivability when P_c is small. When the cyber and physical survival probabilities are equivalently large, although the cyber space is less correlated, increasing P_p leads to a higher F_{cp}. In general, investing in the less correlated space creates a higher F_{cp} when the survival probability of that space is relatively low. However, investing in the more correlated space generates a higher F_{cp} when the survival probabilities of both spaces are relatively high. It implies that, in order to improve the resilience of CPS, we need focus on the individual survival probabilities first, and then on their correlation coefficients. When a_c and a_p are too large, cyber and physical spaces can completely substitute each other (Figure 1 (d)), and the system is almost down since $\lim_{\substack{a_c, a_p \\ \to +\infty}} F_{cp} = 0$. Thus, CPS performs poorly when cyber and physical spaces are highly correlated even if their individual survival probabilities are high.

B. Contest Success Function

The contest success function [5], [6] evaluates the winning probability of each agent (such as provider and attacker) based on the efforts devoted to a contest or conflict. Different forms of contest functions have been applied to applications, such as the ratio and difference forms. We assume that a CPS has inherent cyber and physical-defense levels, denoted by ξ_c and ξ_p, respectively, that counter attacks, and x_c and x_p provide additional reinforcements against the attacks. Then, the survival probability of cyber (physical) space is determined by the percentage of defense effort versus the efforts from both sides in a ratio, or difference form, as shown in Equations (3), and (4), respectively. More details about contest success functions are found in [4], [5].

$$P_c(x_c, y_c) = \frac{\xi_c + x_c}{\xi_c + x_c + y_c},$$
$$P_p(x_p, y_p) = \frac{\xi_p + x_p}{\xi_p + x_p + y_p} \tag{3}$$
$$P_c(x_c, y_c) = \frac{e^{\xi_c} + e^{x_c}}{e^{\xi_c} + e^{x_c} + e^{y_c}},$$
$$P_p(x_p, y_p) = \frac{e^{\xi_p} + e^{x_p}}{e^{\xi_p} + e^{x_p} + e^{y_p}} \tag{4}$$

We use Equation (3) for the model set-up and analysis in Sections III, IV, and V; and Equation (4) for the example illustration in Section VI.

III. Provider Utility Function

We introduce the utility function of the provider first, then develop and analyze the best response from a game-theoretic perspective.

A. The Model

The utility function of the provider is determined by the target revenue and the defense cost [2]. The provider's actual revenue is discounted by the CPS resilience function F_{cp}, which is determined by the defense and attack efforts. So we have the provider's utility $U_D(x_c, x_p, y_c, y_p)$ as follows.

$$U_D = F_{cp}(x_c, x_p, y_c, y_p) g_D - c_{Dc} x_c - c_{Dp} x_p \tag{5}$$

where g_D is the provider's target revenue. c_{Dc}, and c_{Dp} are the unit defense cost in cyber and physical space, respectively.

B. Provider's Best Response

The provider's best response is the defense effort in cyber and physical spaces that she would exert in order to maximize her utility, given certain attack efforts.

Definition 1. *We call the strategy $\{\hat{x}_c, \hat{x}_p\}(y_c, y_p)$ the best response of defender to attacker's attack strategy (y_c, y_p) if*

$$\{\hat{x}_c, \hat{x}_p\}(y_c, y_p) = \arg\max_{x_c \geq 0, x_p \geq 0} U_D(x_c, x_p, y_c, y_p),$$
$$\forall x_c, x_p \in \mathbb{R} \tag{6}$$

In the following, we analyze the provider's best response when the reinforcement and attack efforts (x_c, x_p, y_c, y_p) are continuous and discrete variables, respectively.

1) General Case: When (x_c, x_p, y_c, y_p) are all continuous variables we have the analytical form of best response as follows. $\frac{\partial U_D}{\partial x_c} = \frac{\partial F_{cp}}{\partial x_c} g_D - c_{Dc} = 0$, and $\frac{\partial U_D}{\partial x_p} = \frac{\partial F_{cp}}{\partial x_p} g_D - c_{Dp} = 0$. Considering the functional form as showed in Equation (3), we have the CPS resilience $F_{cp} = \frac{c_{Dc}}{a_c g_D}\left(\frac{(\hat{x}_c+\xi_c)^2}{y_c} + \hat{x}_c + \xi_c\right) = \frac{c_{Dp}}{a_p g_D}\left(\frac{(\hat{x}_p+\xi_p)^2}{y_p} + \hat{x}_p + \xi_p\right)$. The defender's best response implies that a higher system resilience needs a higher unit defense cost, a lower cyber and physical correlation coefficients, a lower target revenue, higher inherent cyber and physical levels, higher cyber and physical reinforcement efforts, and a lower attack effort. We also have $\frac{(\hat{x}_c+\xi_c)(\hat{x}_c+\xi_c+y_c)}{(\hat{x}_p+\xi_p)(\hat{x}_p+\xi_p+y_p)} = \frac{a_c c_{Dp} y_c}{a_p c_{Dc} y_p}$. It indicates that the best response of cyber defense increases in the unit physical defense cost, the inherent physical defense level, the cyber correlation coefficient, the cyber attack level; and decreases in the unit cyber defense cost, the inherent cyber defense level, the physical correlation coefficient, and the physical attack.

2) Discrete Case: Considering the defense and attack efforts as the number of units being reinforced and attacked, we have $x_c, y_c = 0, 1, 2, \cdots, n_c; x_p, y_p = 0, 1, 2, \cdots, n_p$. Figures 2 and 3 show the provider's best response contours $\hat{x}_c(y_c, y_p)$ and $\hat{x}_p(y_c, y_p)$ vary w.r.t. the correlation coefficients a_c and a_p, respectively. We now observe some phenomena that are not obvious in the general case above. The provider's best response effort shrinks to a smaller area with higher gradient when a_c and a_p increases (Figures 2(g) and 3(g)); expands with lower gradient when a_c and a_p decreases (Figures 2(h) and 3(h)). $\hat{x}_c$ decreases when a_c decreases (Figure 2(c)), increases when a_c increases (Figure 2(d)), which has the same trend as the general case discussed in Section III-B1. When a_c increases $\hat{x}_c$ shrinks to a smaller range w.r.t. the cyber attack effort y_p with higher gradient (Figure 2(e)). When a_p increases $\hat{x}_c$

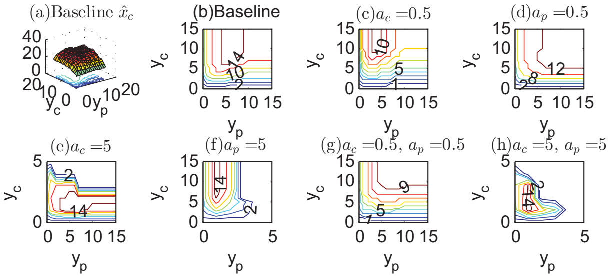


Fig. 2. The provider's best response in cyber space with baseline values: $a_c = 1, a_p = 1, c_{DA} = 0.05, c_{DP} = 0.05, g_D = 5, \xi_c = 0.5, \xi_p = 0.5$

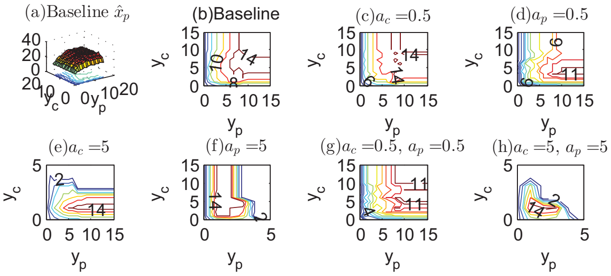


Fig. 3. The provider's best response in physical space with baseline values: $a_c = 1, a_p = 1, c_{DA} = 0.05, c_{DP} = 0.05, g_D = 5, \xi_c = 0.5, \xi_p = 0.5$

shrinks to a smaller range w.r.t. the physical attack effort y_p with higher gradient (Figure 2(f)). So, when the cyber correlation coefficient a_c increases, the best cyber-defense effort increases w.r.t. lower cyber attack, but decreases w.r.t. higher cyber attack. In other words, when the cyber-space is more correlated to the CPS, the defender would exert more cyber-defense effort when the cyber-attack level is relatively low, but would decrease the effort when cyber-attack effort is relatively high.

IV. Attacker Utility Function

The utility function of the attacker is determined by his target revenue, the probability of CPS breakdown, and the attack costs in cyber and physical spaces.

A. The Model

Similar to the utility function of the provider, we have the utility function of the attacker as below.

$$U_A = (1 - F_{cp}(x_c, x_p, y_c, y_p))g_A - c_{Ac}y_c - c_{Ap}y_p \quad (7)$$

where g_A is the the attacker's target revenue. c_{Ac}, and c_{Ap} are the unit attack costs in cyber and physical spaces, respectively.

B. Attacker's Best Response

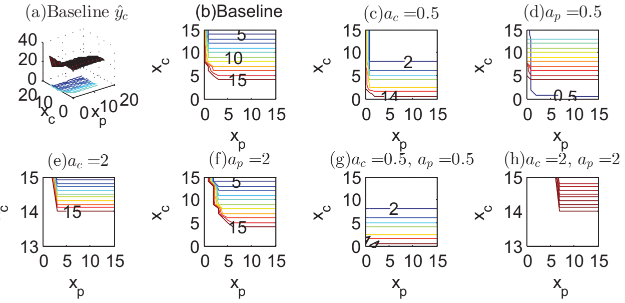
First, we present the concept of attacker's best response, then show the best responses when decision variables are continuous and discrete, respectively.

Definition 2. *We call the strategy $\{\hat{y}_c, \hat{y}_p\}$ the best response of attacker to defender's defense strategy (x_c, x_p) if*

$$\begin{aligned} \{\hat{y}_c, \hat{y}_p\}(x_c, x_p) &= \underset{y_c \geq 0, y_p \geq 0}{\arg\max}\, U_A(x_c, x_p, y_c, y_p), \\ &\forall y_c, y_p \in \mathbb{R} \end{aligned} \quad (8)$$

1) General Case: Based on the attackers utility function, the attackers best response satisfies: $\frac{\partial U_A}{\partial y_c} = -\frac{\partial F_{cp}}{\partial y_c} g_A - c_{Ac} = 0$, and $\frac{\partial U_A}{\partial y_p} = -\frac{\partial F_{cp}}{\partial y_p} g_A - c_{Ap} = 0$. Using the functional form as showed in Equation (3), we have $F_{cp} = \frac{c_{Ac}}{a_c g_A}(\hat{y}_c + x_c + \xi_c) = \frac{c_{Ap}}{a_p g_A}(\hat{y}_p + x_p + \xi_p)$. We also have another form about the attacker's best response. $\frac{\hat{y}_c + x_c + \xi_c}{\hat{y}_p + x_p + \xi_p} = \frac{a_c c_{Ap}}{a_p c_{Ac}}$. It implies that the attacker's best response in cyber space increases in the unit cost of physical-space attack, the cyber correlation coefficient, and the physical-space defense effort; decreases in the unit cost of cyber-space attack, the physical-space correlation coefficient, and the cyber-space defense effort.

2) Discrete Case: Considering the attack and defense efforts as integers, i.e., $x_c, y_c = 0, 1, 2, \cdots, n_c; x_p, y_p = 0, 1, 2, \cdots, n_p$, Figures 4 and 5 show the provider's best response contours $\hat{x}_c$ and $\hat{x}_p$ change w.r.t. the cyber- and physical correlation coefficients a_c and a_p, respectively. We notice that $\hat{y}_c$ decreases when a_c, or a_p decreases, and increases when a_c, or a_p increases. In other words, the best response of cyber-attack increases when the cyber and physical spaces are more correlated.


(a)Baseline $\hat{y}_c$

(b)Baseline

(c)a_c =0.5

(d)a_p =0.5

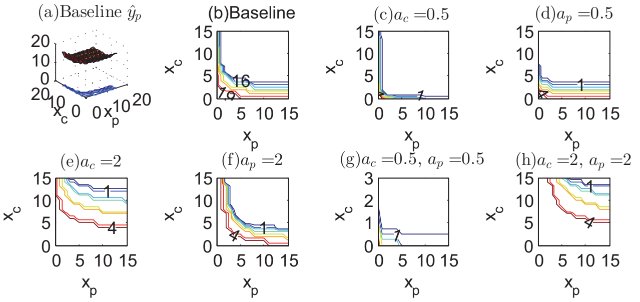
(e)a_c =2

(f)a_p =2

(g)a_c =0.5, a_p =0.5

(h)a_c =2, a_p =2

Fig. 4. The attacker's best response in cyber space with baseline values: $c_{Ac} = 0.1, c_{Ap} = 0.1, a_c = 1, a_p = 1, g_A = 2, \xi_c = 0.5, \xi_p = 0.5$


(a)Baseline $\hat{y}_p$

(b)Baseline

(c)a_c =0.5

(d)a_p =0.5

(e)a_c =2

(f)a_p =2

(g)a_c =0.5, a_p =0.5

(h)a_c =2, a_p =2

Fig. 5. The attacker's best response in physical space with baseline values: $c_{Ac} = 0.1, c_{Ap} = 0.1, a_c = 1, a_p = 1, g_A = 2, \xi_c = 0.5, \xi_p = 0.5$

V. NE of Simultaneous Game

In this section, we consider a simultaneous game in which the provider and the attacker move at the same time. The provider and the attacker decide on defense and attack efforts in cyber and physical spaces, respectively. Notice that $\frac{\partial^2 U_D}{\partial {x_c}^2} < 0$, and $\frac{\partial^2 U_D}{\partial {x_p}^2} < 0$, when $a_c < 1 + \frac{2(x_c + \xi_c)}{y_c}$, and $a_p < 1 + \frac{2(x_p + \xi_p)}{y_p}$, $\frac{\partial^2 U_A}{\partial {y_c}^2} < 0$, and $\frac{\partial^2 U_A}{\partial {y_p}^2} < 0$, which ensure the existence of optimal solution to Equations (6) and (8).

Definition 3. *We call a collection of strategy $(x_c^*, x_p^*, y_c^*, y_p^*)$ a pure Nash equilibrium, or "equilibrium", if and only if both Equations (9) and (10) are satisfied:*

$$U_D(x_c^*, x_p^*, y_c^*, y_p^*) \geq U_D(x_c, x_p, y_c^*, y_p^*), \quad \forall x_c, y_c \quad (9)$$

$$U_A(x_c^*, x_p^*, y_c^*, y_p^*) \geq U_A(x_c^*, x_p^*, y_c, y_p), \quad \forall y_c, y_c \quad (10)$$

A. General Case

Based on the provider's and attacker's best responses (Equations (6) and (8)), we have $\{{x_c}^*, {x_p}^*, {y_c}^*, {z_p}^*\}$ as follows.

$$x_c{}^* \;=\; \frac{F_{cp} a_c g_A g_D - \xi_c c_{Dc} g_A - \xi_c c_{Ac} g_D}{g_D c_{Ac} + g_A c_{Dc}} \quad (11)$$

$$x_p{}^* \;=\; \frac{F_{cp} a_p g_A g_D - \xi_p c_{Dp} g_A - \xi_p c_{Ap} g_D}{g_D c_{Ap} + g_A c_{Dp}} \quad (12)$$

$$y_c{}^* \;=\; \frac{c_{Dc} F_{cp} a_c g_A{}^2}{c_{Ac}(g_D c_{Ac} + g_A c_{Dc})} \quad (13)$$

$$y_p{}^* \;=\; \frac{c_{Dp} F_{cp} a_p g_A{}^2}{c_{Ap}(g_D c_{Ap} + g_A c_{Dp})} \quad (14)$$

where $F_{cp} = \left(\frac{g_D c_{Ac}}{g_D c_{Ac} + g_A c_{Dc}}\right)^{a_c} \left(\frac{g_D c_{Ap}}{g_D c_{Ap} + g_A c_{Dp}}\right)^{a_p}$

Based on the above analytical solution, the CPS resilience F_{cp} increases in the provider's target revenue g_D, the unit attack costs in cyber space c_{Ac}, and physical spaces c_{Ap}; decreases in the cyber correlation coefficient a_c, and physical correlation coefficient a_p, the attacker's target revenue g_A, the unit defense cost in cyber space c_{Dc}, and physical space c_{Dp}. Regarding the cyber reinforcement, $x_c{}^*$ increases in c_{Ap} and g_D; and decreases in c_{Dc}, c_{Dp} and ξ_c. The relations between $x_c{}^*$ and other parameters, such as a_c, a_p, c_{Ac}, g_A, ξ_p, are not monotonic and can be very complicated. For example, consider the effects of c_{Ac} on $x_c{}^*$. When the unit cost of cyber attack increases, the attacker would either keep or withdraw cyber-attack, which depends on the defender's physical reinforcement $x_p{}^*$, the unit costs of physical defense and attack, and the cyber, physical correlation coefficients. The attacker would decrease the level or even withdraw cyber attack if he can fully destroy the physical space by increasing physical attack, considering his target revenue, the unit cyber attack cost, and the cyber and physical correlation coefficients. Otherwise, the attacker would keep attacking the cyber space. The cyber reinforcement, $x_c{}^*$, first increases then decreases in the cyber correlation coefficient, a_c. This is because, considering the discounted target revenue, the provider's utility increases in the system resilience, F_{cp}. While F_{cp} increases in x_c, decreases in a_c, the provider's payoff increases in x_c, and decreases in a_c. With increasing a_c, increasing x_c can counter the negative effect of a_c and generate more revenue. However, when x_c is large, the cost term, which is a linear function of x_c, has a negative effect to his payoff. So $x_c{}^*$ first increases then decreases in a_c.

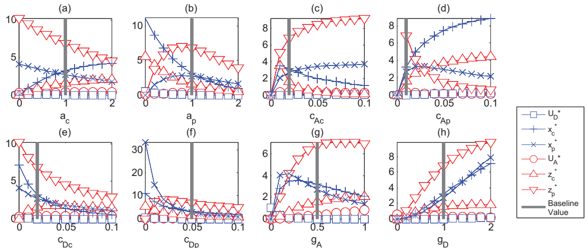


Fig. 6. Sensitivity analysis of NE (continuous decision variables) in a simultaneous game given the baseline values $c_{A_c} = 0.02, c_{A_p} = 0.01, g_A = 0.5, a_c = 1, a_p = 1, g_D = 1, c_{Dc} = 0.02, c_{Dp} = 0.05$

B. Discrete Case

When the decision variables are allowed to take discrete values only, we don't have the closed-form solution, and hence numerically solve the game model. Figure 7 shows the NE pure strategies when defense and attack efforts are integers, for example the number of targets being reinforced and attacked. We observe that the defense efforts in cyber, and physical spaces first increase then decrease in the cyber and physical correlation coefficients. We notice that the existence of NE pure strategy is not guaranteed for the discrete case. For example, given certain target revenues and cyber and physical correlation coefficients, the provider and attacker would have to adjust the costs in cyber and physical spaces and otherwise they won't reach an equilibrium.

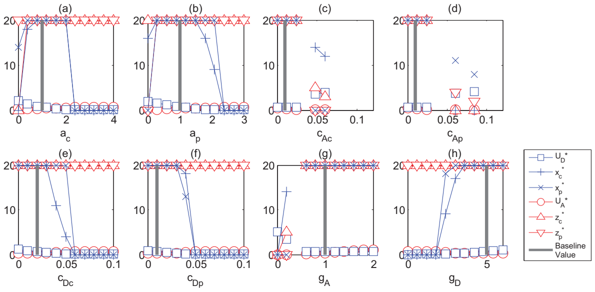


Fig. 7. Sensitivity analysis of NE (discrete decision variables) in a simultaneous game given the baseline values $c_{A_c} = 0.01, c_{A_p} = 0.01, g_A = 1, a_c = 1, a_p = 1, g_D = 5, c_{Dc} = 0.02, c_{Dp} = 0.01, \xi_c = 1, \xi_p = 1$

VI. Cloud-Computing Example

In this section, we examine the resilience of a cloud computing infrastructure that is subject to cyber attacks on servers and routers, and physical attacks on fiber routes and cooling and power systems. The cloud computing infrastructure is composed of 100 servers distributed at five physical sites. The reinforcement and attack efforts are the number of servers being reinforced and attacked. A successful physical attack, such as the disruption of fibers or gateway routers, makes all servers unavailable in the cyber space. Given the predetermined parameters $a_c, a_p, c_{Ac}, c_{Ap}, v, c_{Dc}, c_{Dp}$, and V, the defensive reinforcement and the provider's utility at NE are obtained based on Equations (9) and (10). We compare the provider's utility and the system resilience at NE, for different deployment scenarios, cyber and physical correlation coefficients. Table VI shows the defense and attack efforts at each physical site, the provider's utilities, and the system resilience under three deployment scenarios, namely, (50, 30, 10, 5, 5), (40, 40, 10, 10, 10), and (20, 20, 20, 20, 20). The difference-form contest function (Equation (4)) is used here.

The system resilience $F_{cp}{}^*$, and the provider's utility $U_D{}^*$ both increase as the correlation coefficients a_c and a_p decrease for a given deployment scenario. Uneven

TABLE II. THE ILLUSTRATION OF THE CLOUD COMPUTING INFRASTRUCTURE WITH DIFFERENT DEPLOYMENTS

Deployment Scenarios	${x_c}^*$	${x_p}^*$	${z_c}^*$	${z_p}^*$	${U_D}^*$	${F_{cp}}^*$
$a_c = 1, a_p = 2, c_{Ac} = 0.1, c_{Ap} = 0.1, v = 10, c_{Dc} = 0.5, c_{Dp} = 0.5, V = 50$						
(50, 30, 10, 5, 5)	(0, 0, 10, 5, 5)	(0, 1, 1, 1, 1)	(0, 0, 10, 5, 5)	(0, 0, 1, 1, 1)	35.96	15.34%
(40, 30, 10, 10, 10)	(0, 0, 10, 10, 10)	(0, 1, 1, 1, 1)	(0, 0, 10, 10, 10)	(0, 0, 1, 1, 1)	34.96	15.34%
(20, 20, 20, 20, 20)	(3, 3, 3, 3, 3)	(1, 1, 1, 1, 1)	(3, 3, 3, 3, 3)	(1, 1, 1, 1, 1)	29.25	12.5%
$a_c = 1, a_p = 1, c_{Ac} = 0.1, c_{Ap} = 0.1, v = 10, c_{Dc} = 0.5, c_{Dp} = 0.5, V = 50$						
(50, 30, 10, 5, 5)	(0, 2, 10, 5, 5)	(0, 1, 1, 1, 1)	(0, 2, 10, 5, 5)	(0, 1, 1, 1, 1)	59.90	25%
(40, 30, 10, 10, 10)	(7, 2, 10, 10, 10)	(1, 1, 1, 1, 1)	(7, 2, 10, 10, 10)	(1, 1, 1, 1, 1)	58.10	25%
(20, 20, 20, 20, 20)	(20, 20, 20, 20, 20)	(1, 1, 1, 1, 1)	(20, 20, 20, 20, 20)	(1, 1, 1, 1, 1)	52	25%
$a_c = 0.5, a_p = 0.5, c_{Ac} = 0.1, c_{Ap} = 0.1, v = 10, c_{Dc} = 0.5, c_{Dp} = 0.5, V = 50$						
(50, 30, 10, 5, 5)	(7, 30, 10, 5, 5)	(0, 1, 1, 1, 1)	(8, 3, 10, 5, 5)	(1, 1, 1, 1, 1)	107.35	45.38%
(40, 30, 10, 10, 10)	(40, 30, 10, 10, 10)	(1, 1, 1, 1, 1)	(40, 30, 10, 10, 10)	(1, 1, 1, 1, 1)	114.5	50%
(20, 20, 20, 20, 20)	(20, 20, 20, 20, 20)	(1, 1, 1, 1, 1)	(20, 20, 20, 20, 20)	(1, 1, 1, 1, 1)	114.5	50%

allocation of servers at physical sites (50, 30, 10, 5, 5) may lead to a higher payoff to the provider when the CPS is statistically independent ($a_c = 1$ and $a_p = 1$) or has higher correlation coefficients. But, an even deployment (20, 20, 20, 20, 20) leads to a higher payoff when the CPS has relatively low correlation coefficients. Thus, it is important for the provider to adapt the deployment strategy to the correlation coefficients in order to maximize the payoff.

VII. CONCLUSION

In this paper, we propose a game theory approach to explore the correlations between cyber and physical spaces in CPS. We investigate the system resilience in terms of the cyber and physical correlation coefficients, the reinforcement and attack levels and costs, the defender's and attacker's target revenues. We find that investing on the less correlated space leads to a higher system resilience when the survival probability of that space is relatively low. However, investing on the more correlated space generates a higher system resilience when the survival probabilities of both spaces are relatively high. The cyber and physical correlation coefficients can generate both monotonic and non-monotonic dependencies between the cyber and physical reinforcement and attack efforts, which in turn depend on the relationships between provider's and attacker's target revenues and costs in cyber and physical spaces. In the cloud-computing example, the cyber and physical correlation coefficients can significantly affect the CPS resilience. The provider can obtain a higher payoff by adapting the deployment strategy to the cyber and physical correlation coefficients. Overall, by accounting for the complex interdependence within CPS, our preliminary results provide insights into improving the resilience of CPS.

In the future, we plan to develop more advanced models by considering the budget limits, and use data from practical systems to validate models. We are also interested in investigating real-life CPS applications that present more complex and realistic cyber-physical interdependence.

ACKNOWLEDGMENT

This work is funded by the Mathematics of Complex, Distributed, Interconnected Systems Program, Office of Advanced Computing Research, U.S. Department of Energy, and is performed in part at Oak Ridge National Laboratory managed by UT-Battelle, LLC for U.S. Department of Energy under Contract No. DE-AC05-00OR22725. This research is also partially supported by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under award number 2010-ST-061-RE0001.

REFERENCES

[1] He, F. and Zhuang, J. Modeling 'contracts' between a terrorist group and a government in a sequential game. *Journal of the Operational Research Society*, 63: 790-809, 2012.

[2] He, F., Zhuang, J., and Rao, N. S. V. Game-theoretic analysis of attack and defense in cyber-physical network infrastructures. *Proceedings of the Industrial and Systems Engineering Research Conference*, Orlando, FL, May, 2012.

[3] Houthakker, H. S. The Pareto distribution and the Cobb-Douglas production function in activity analysis. *The Review of Economic Studies*, 23(1), 27-31, 1955.

[4] Hwang, S. H. Contest success functions: Theory and evidence. *Working Paper, University of Massachusetts, Department of Economics*.

[5] Rai, B. K., and Sarin, R. Generalized contest success functions. *Economic Theory*, 40(1): 139-149, 2009.

[6] Skaperdas, S. Contest success functions. Economic Theory, 7(2), 283-290, 1996.

[7] Sztipanovits, J. and Koutsoukos, X. and Karsai, G. and Kottenstette, N. and Antsaklis, P. and Gupta, V. and Goodwine, B. and Baras, J. and Wang, S. (2012) Toward a Science of Cyber-Physical System Integration. *Proceedings of the IEEE*, 100(1): 29-44, 2012.

[8] Yagan, O., Qian, D., Zhang, J., and Cochran, D. Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness. *Parallel and Distributed Systems, IEEE Transactions on*, 23(9), 1708-1720.