A Game Theoretic Study of Attack and Defense in Cyber-Physical Systems

Chris Y. T. Ma
Advanced Digital Sciences Center
Illinois at Singapore

Nageswara S. V. Rao
Oak Ridge National Laboratory

David K. Y. Yau
Purdue University

Abstract

Cyber-physical systems encompass a wide range of systems such as sensor networks, cloud computing complexes, and communication networks. They require both the cyber and physical components to function, and hence are susceptible to attacks on either. A cyber-physical system is characterized by the physical space that represents physical components, and the cyber space that represents computations and communications. In this paper, we present a number of game theoretic formulations of attack and defense aspects of cyber-physical systems under different cost and benefit functions and different budgets of the attacker and defender. We discuss the outcomes of the underlying game under linear, negative exponential, and S-shaped benefit functions. We show that the outcomes are determined by the Nash Equilibria (which sometimes occur at budget limits), which in turn determine the system survival.

1. Introduction

A number of engineering infrastructure systems involve two spaces: the physical space of hardware components, and the cyber space of computations and communications. Such systems can be quite varied, ranging from computing and data server farms that require computing hardware and power and cooling facilities, to networks of sensors that require sophisticated computations and communications. The cyber-physical systems are susceptible to attacks that disrupt through cyber or physical means, which can cause potentially huge losses, such as bringing down the entire system. Modeling of such critical infrastructure systems is studied in [5], [3]. A study of the dependability of such systems is proposed in [4].

A defender of cyber-physical systems must appropriately analyze the attack and defense strategies in view of both the cyber and physical components. The defender, however, is at an inherent disadvantage in having to ensure adequate cyber and physical resources simultaneously to keep the system operational within allocated budget. On the other hand, the attacker can bring down the system by attacking either the cyber or physical part.

In this paper, we present game theoretic formulations to capture the attack and defense of a class of cyber-physical systems. The game is between the attacker that tries to disrupt the system and the defender that attempts to sustain its operation. Their actions are driven by payoff functions which incorporate both the cost and benefit terms at various levels of details, and also the knowledge of one player about the other. We consider a number of games to capture different payoff functions and budgets of the players, and determine the outcome of each game that indicates whether or not the system will survive. The outcome of the game is generally determined by the Nash Equilibrium (NE) which specifies a saddle-point in the player's actions from which neither (rational) player has an incentive to unilaterally deviate. Sometimes, the NE exist at the cost boundaries defined by the players' available budgets. We show payoff functions that illustrate both the survival and disruption of the system at NE.

Our objective is to study the survival of a cyber-physical system in the presence of an attacker and a defender within the framework of game theory [2]. The presence and interactions of two players over potentially disparate cyber and physical spaces makes the study interesting. We first consider the case of fixed costs and Boolean attack outcomes, and show that the system survival is deterministic even under probabilistic attack and defense strategies. Then, we consider more general cases in which system performance is determined by the number of resources deployed by the defender minus that disrupted by the attacker. Hence, an attack may disrupt a subset of the resources, and thus degrade the performance of the system without necessarily bringing it down. For this formulation, we consider linear, negative exponential, and S-shaped benefit functions. Our conclusions are: (a) pure strategy NE may not exist for some benefit functions and budget settings, (b) sometimes cost boundaries determine the game's NE outcome, and (c) the overall system may or may not survive at NE. Hence, while several useful insights are provided by the game-theoretic analysis, additional domain-specific analysis is needed to assess the survival of the system.

The organization of the paper is as follows. We describe our system model in Section 2. The case of Boolean outcomes is considered in Section 3. The general case is considered in Section 4, where intermediate levels of system performance are determined by the number of deployed resources and intensity level of attack.

2. System Model

The system consists of the cyber ($i = c$) and physical ($i = p$) spaces, which require a minimum of k_i+1, $i = c, p$,

978-1-4244-9920-5/11/$26.00 ©2011 IEEE

resources to function. Let x_i, $i = c, p$, be the number of resources deployed by the defender in space i, and y_i be the number of the resources disrupted by the attacker, which we refer to as the attack intensity. The quantity $x_i - k_i$ is the *robustness* of the system in that attacks at level $x_i - y_i \geq k_i + 1$ will not disrupt the system. Then the game is described as follows.

- *Players:* Given that the payoff is positive, the defender's basic objective is to keep the system functioning, $x_i - y_i \geq k_i + 1$, and the ultimate goal of the attacker is to disrupt, i.e., so that $x_i - y_i < k_i + 1$.
- *Actions:* The sets of actions N_D and N_A represent the resources deployed by the defender and disrupted by the attacker, respectively.
- *Costs and benefits:* Each player has a payoff function U consisting of two parts: benefit B and/or cost C. The attacker incurs a cost in launching an attack, and the defender incurs a cost in deploying the resources. In a game, either player will aim to maximize its payoff given the other player's best strategy.

In general, the costs could be quite different for the cyber and physical components. For a cloud complex example, cyber attacks on the complex can be launched from remote sites whereas physical attacks will require physical proximity. For a sensor network example, the sensors deployed in open space are harder to defend compared with ensuring the cyber security of servers connected over an isolated network.

3. Boolean Attack and Defense

We now consider a special case of $k_i = 0$, $i = c, p$, where the cyber and physical parts can be attacked or defended as whole units such that $x_i = 0, 1$ and $y_i = 0, 1$, for $i = c, p$:

- The attacker's action set is $N_A = \{0, c, p\}$, where 0 represents no attack, c represents an attack on the cyber part, and p represents an attack on the physical part, either of which will disrupt the system. Note that the attacker will not launch a simultaneous cyber and physical attack.
- The defender's action set is $N_D = \{0, cp\}$, where 0 represents the default, and cp represents reinforcing both the cyber and physical parts.

We consider that a successful attack on either the physical or cyber part will disrupt the system. Let p_c and p_p correspond to the attack probabilities of the cyber and physical parts, respectively; $p_c + p_p \leq 1$, and $1 - p_c - p_p$ is the probability that no attack is launched. We assume that that defender will reinforce both the cyber and physical parts with probability q. The game matrices G^A and G^D of the attacker and defender represent the payoff of each action pair $(a, d) \in N_A \times N_D$, such that a and d correspond to the row and column indices, respectively. The (a, d)-entry of G^A specifies the payoff of the attacker when the defender employs action d in defense of attack a. Similarly, the (a, d)-entry of G^D specifies the payoff of the defender under action d in defense of attack a. We consider that the gain matrix of each player in each case is the sum of the player's cost and payoff matrices defined as follows:

$$G^A = \begin{bmatrix} A_c & A_c \\ A_p & A_p \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} S & -S \\ S & -S \\ S & S \end{bmatrix},$$

$$G^D = \begin{bmatrix} D_{cp} & 0 \\ D_{cp} & 0 \\ D_{cp} & 0 \end{bmatrix} - \begin{bmatrix} S & -S \\ S & -S \\ S & S \end{bmatrix}.$$

In each case, the first matrix specifies the fixed cost of the attack or defense, and the second matrix specifies the benefit of each player, as a "zero-sum" between disrupting or sustaining the system by the attacker and the defender, respectively. Note that S is a constant matrix determining the zero sum, and the magnitudes of the cost and benefit terms reflect their importance relative to each other. Let $p_A = [p_c \quad p_p \quad 1 - p_c - p_p]$ and $p_D = [q \quad 1 - q]$ be the vectors that correspond to the probabilities of N_A and N_D, respectively.

Both the attacker and defender in this game employ probabilistic strategies in general. Being a game over finite action sets, the game is guaranteed to have a mixed strategy Nash equilibrium [1]. The NE outcome is given by the minimization of $p_A G^A p_D^T$ and $p_A G^D p_D^T$ for the attacker and defender, respectively. For the attacker, we have

$$p_A G^A p_D^T = p_c A_c + p_p A_p + S\left[1 - 2(p_c + p_p)(1 - q)\right].$$

whose minimization is guided by the following choices:

$$p_c = \begin{cases} 0 & \text{if } A_c > 2S(1-q) \\ > 0 & \text{otherwise} \end{cases},$$

$$p_p = \begin{cases} 0 & \text{if } A_p > 2S(1-q) \\ > 0 & \text{otherwise} \end{cases}.$$

If $p_c = 0$ and $p_p = 0$, then $p_A G^A p_D^T = S$ and the system continues to function. Otherwise, the minimization is achieved at $p_c + p_p = 1$ such that $p_c = 1$ if $A_c \leq A_p$, and $p_p = 1$ otherwise; thus the attacker chooses to attack the component having a lower cost of attack.

By considering

$$p_A G^D p_D^T = q D_{cp} - S\left[1 - 2(p_c + p_p)(1 - q)\right],$$

we have the following choice for the defender

$$q = \begin{cases} 0 & \text{if } D_{cp} > 2S(p_c + p_p) \\ 1 & \text{otherwise} \end{cases}.$$

Summarizing the outcomes, we note that the Nash equilibrium is deterministic in that the underlying probabilities are either 0 or 1. The choice of the attacker requires the knowledge of q, whereas the defender only needs to know if $p_c + p_d = 1$. Given the knowledge, the NE specifies a stable outcome of this game. The survival of the system at the Nash equilibrium is determined by the deterministic condition $A_c > 2S(1-q)$ or $A_p > 2S(1-q)$ or $D_{cp} < 2S$. If a player's game matrix is not known to the other player, the actions corresponding to the NE cannot be computed.

4. Systems with Robustness

In this section, we study systems that require a certain minimum number of resources to function, but for which the defender can deploy additional resources to increase the robustness of the system. We will consider different forms of benefit functions for the players as shown in Fig. 2(a), while the cost functions for both players are the same as shown in Fig. 2(b). The benefit function of the attacker is the drop (≤ 1) in payoff of the defender because of the attack, or it is one if the system is down or not deployed, as these outcomes represent the ultimate goal of the attacker. Notice that being a game over finite action sets, the game is guaranteed to have a mixed strategy Nash equilibrium.

4.1. Analysis of single spaces

The study of the cyber-physical system can be simplified to a one-space study if the attacker and the defender have "independent" budgets for the two spaces, and the actions of a player on one space do not affect the operation of the other space. Another justification for a one-space study is that one of the two spaces is well insulated from attacks by the attacker, such as if the cyber space is fully isolated from external access. We assume that the payoff functions are known to both players.

4.1.1. Linear cost for both defender and attacker. We assume that the attacker disrupts y resources, while the defender deploys x resources. The payoff function of the attacker is given by

$$U_a(y, x) = 1_{\{y \geq x-k\}} - C_a(y),$$

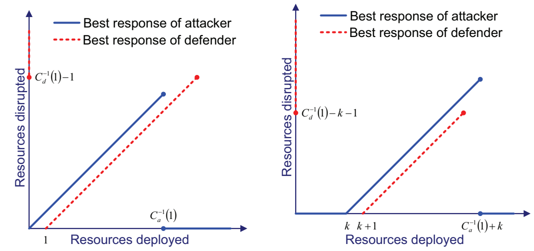
where 1_a is an indicator function of value one if the condition a is true, or zero otherwise, and $C_a(y)$ is the cost function of the attacker for disrupting y resources. The payoff function of the defender is given by

$$U_d(x, y) = 1_{\{x > y+k\}} - C_d(x),$$

where $C_d(x)$ is the cost function of the defender for deploying x resources.

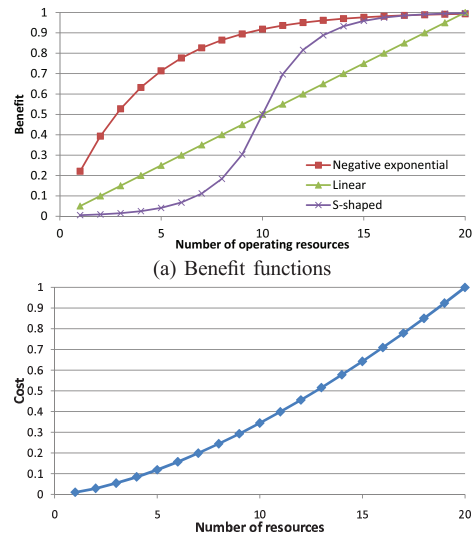
Consider the strategy of the defender if $x \leq y+k$, i.e., the number of resources deployed is not sufficient to make the system operational after the attack. In this case, the defender prefers x to be zero because of the cost that would be incurred in a deployment. Otherwise, the defender considers if $1 - C_d(y + k + 1)$ is positive or not. If it is negative, meaning that the benefit is less than the cost needed to make the system operational, then the defender prefers x to be zero; otherwise $x = y + k + 1$ is the defender's best response.

Similarly, consider the strategy of the attacker if $y < x-k$. In this case, the attacker prefers y to be zero because of the cost that would be incurred for an attack. Otherwise, the attacker considers if $1-C_a(x-k)$ is positive or not. If it is negative, then the attacker prefers y to be zero; otherwise $y = x - k$ is the attacker's best response.



(a) $k = 0$ (b) k is non-zero

Figure 1. The players' best response functions.



(a) Benefit functions

(b) Cost function

Figure 2. Benefit and cost functions for the players.

Fig. 1 illustrates the best response functions of the attacker and defender under two situations, i.e., k is zero and k is non-zero. The best response functions of the two players do not intersect. Hence, there is no pure strategy NE in this game. The presence of a budget limit for either player will only put an upper bound on the maximum number of resources deployed by the defender or disrupted by the attacker. It will not affect the existence of pure strategy NE in the game.

4.1.2. Benefit functions. We consider more general forms of the payoff functions (Fig. 2(a)) in this section, while the cost function is kept the same for both the attacker and defender (Fig. 2(b)). Again, the benefit function of the attacker is the drop (≤ 1) in payoff of the defender because of the attack, or one if the system is down or not deployed, which corresponds to the ultimate goal of the attacker.

The payoff function of the defender is given by

$$U_d(x, y) = B(x - y)1_{\{x>y+k\}} - C_d(x),$$

where the range of x is such that $0 \leq C_d(x) \leq$ budget, $B(n)$ is the benefit function of the defender given that there are n working resources in the system. The negative exponential benefit function is given by

$$B(x) = 1 - e^{-c_e \times x},$$

where c_e is a constant. The linear benefit function is given by

$$B(x) = c_l \times x,$$

where c_l is a constant. And the S-shaped benefit function is given by

$$B(x) = \frac{1}{1 + e^{\frac{c_{s1} - x}{c_{s2}}}},$$

where c_{s1} and c_{s2} are constants.

The payoff function of the attacker is given by

$$U_a(x, y) = \begin{cases} B(x) - B(x - y) - C_a(y) & \text{if } y < x - k \\ 1 - C_a(y) & \text{otherwise} \end{cases},$$

where the range of y is such that $0 \leq C_a(y) \leq$ budget.

Fig. 3 shows the best response functions of the two players, which are computed by maximizing one player's payoff given every possible action by the other player. We assume that the budget of the defender is one, while that of the attacker is significantly lower as indicated by the number in brackets in the label of each plot. The minimum number of working resources needed for the system to be operational is three, i.e., $k = 2$.

(a) Negative exponential benefit function: Fig. 3(a) depicts the best response functions of the two players for the negative exponential benefit function. Observe the presence of a ridge in each best response plot of the attacker. The ridge happens when the budget limit is reached for the attacker. Notice that when the defender deploys more resources, a budget-limited attacker may choose to disrupt fewer resources than it could or may even choose not to attack at all, since the benefit would be out-weighed by the cost of the attack due to the diminishing returns in benefit characterized by the negative exponential function.

(b) Linear benefit function: Fig. 3(b) depicts the best response functions of the two players for the linear benefit function. Again, each best response function of the attacker exhibits a ridge due to reaching the attacker's budget limit.

(c) S-shaped benefit function: Fig. 3(c) depicts the best response functions of the two players for the S-shaped benefit function. Note the presence of a ridge in the attacker's best response functions, similar to the two previous cases. However, the ridge is not continuous in this case because of the S-shaped benefit function of the defender. In particular, when the number of resources deployed by the defender is within the steep-ascent portion of the benefit function, the attacker by disrupting a few resources will gain a lot of benefit. This results in a sharp drop in the number of resources that the attacker will choose to disrupt as the number of resources deployed increases, which gives rise to the "valleys" in the attacker's best response functions as shown in Fig. 3(c). However, when the defender deploys a large enough number of resources, there is no more incentive for a budget-limited attacker to disrupt the system at all, which is similar to the situation of the negative exponential benefit function.

Note from the plotted results that a pure strategy Nash Equilibrium exists in a game when the budget of the attacker is limited and much lower than that of the defender. However, if we increase the budget of the attacker, then such an equilibrium will no longer exist. Particularly for the given numerical example, the equilibrium will vanish when the attacker has enough budget to disrupt up to six resources for the negative exponential benefit function, three resources for the linear function, and four resources for the S-shaped function. When the budget of the attacker is high enough to disrupt all the deployed resources, there is no incentive for the defender to deploy the system as doing so will invite the attacker to attack and bring down the system. At the same time, there is no incentive for the attacker to attack (and spend) if the defender decides not to deploy the system. Hence, a pure strategy NE does not exist in this situation.

4.2. Analysis of cyber and physical spaces together

In this section, we consider that the cost functions of the attacker and defender are the same, and that both the cyber and physical spaces are considered together for deployment and attack. We assume that the benefit of the system to the defender is given by the summation of the individual benefit functions of the two spaces if the overall system survives, or it is zero if the system is down. If the number of working resources in either space does not meet a given threshold k, we assume that the overall system will be down. Hence, the defender needs to invest enough resources in both spaces for the system to be up.

The payoff function of the defender is given by

$$U_d(x_1, x_2, y_1, y_2) = \tag{1}$$
$$\frac{1}{2}\Big[(B_1(x_1 - y_1) + B_2(x_2 - y_2))1_{\{x_1 > y_1 + k\} \text{ and } \{x_2 > y_2 + k\}} - C_{d1}(x_1) - C_{d2}(x_2)\Big],$$

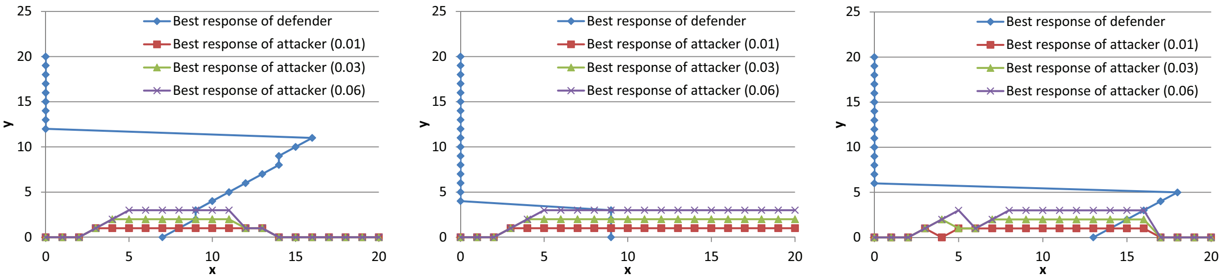
where B_i is the defender's benefit function in space i, C_{di} is the defender's cost function in space i, and x_1 and x_2 satisfy the constraint that $0 \leq C_{d1}(x_1) + C_{d2}(x_2) \leq$ budget.

The payoff function of the attacker is given by Equation (2), where y_1 and y_2 satisfy the constraint that $0 \leq C_{a1}(y_1) + C_{a2}(y_2) \leq$ budget. The benefit function of the attacker is the drop in benefit of the defender because of the attack if the system survives, and it is one if the system is down.

In the following, we give numerical examples of the Nash Equilibrium in different game settings under the cost and benefit functions depicted in Fig. 2. We assume $k = 2$.

4.2.1. Same benefit function for both spaces.

In this section, we study the case that the benefit functions of the two spaces are the same. Consider the problem for the defender to decide where (i.e., in cyber vs. physical spaces) to invest resources in order to maximize its own



(a) Negative exponential benefit (b) Linear benefit (c) S-shaped benefit

Figure 3. The players' best response functions.

$$U_a(x_1,x_2,y_1,y_2) = \begin{cases} \frac{1}{2}\left[B_1(x_1) - B_1(x_1-y_1) + B_2(x_2) - B_2(x_2-y_2) - C_{a1}(y_1) - C_{a2}(y_2)\right] & y_1 < x_1 - k \text{ and } y_2 < x_2 - k \\ 1 - \frac{1}{2}(C_{a1}(y_1) - C_{a2}(y_2)) & y_1 \geq x_1 - k \text{ or } y_2 \geq x_2 - k \end{cases}. \quad (2)$$

payoff, assuming that there are no attackers. Even without consideration for attackers, the problem is non-trivial. To illustrate, consider a greedy allocation strategy by which the defender decides where to deploy the next available resource by maximizing the marginal gain in the achieved payoff, or the defender will decide not to deploy the next resource if neither space will increase the payoff.

For the defender, one sufficient (but not necessary) condition for the optimality of the above greedy algorithm is that the marginal gain in payoff is monotonically decreasing, or the marginal gain in payoff is strictly monotonically increasing and the initial payoff is positive. This condition is satisfied for the negative exponential benefit function. In general, however, the greedy algorithm is sub-optimal for a budget-limited defender. An example is the S-shaped benefit function. Since initially the cost of deploying the first few resources may be greater than the benefit, the greedy algorithm will choose not to deploy the system at all. The decision may be myopic, however, since the benefit of deploying further resources than the initial (unproductive) investment may finally outweigh the cost.

Now consider the more general problem in which an attacker may be present. In this case, the existence of the attacker may change the defender's payoff function. For instance, the greedy approach may not return the optimal solution in any of the changed payoff functions $U_d(x-y)$. It is because the deployment of some initial resources will bring no benefit but only incur a cost when the system is under attack. The greedy algorithm would thus choose not to deploy the system at all. But in fact, the defender could become better off by deploying enough resources to withstand the disruption, and bringing about a positive payoff in the final deployment.

We now present numerical examples under different budgets and benefit functions.

(1) Negative exponential benefit function. When the budget of the defender is one and that of attacker is 0.02, the system is in NE when the defender deploys $(8, 8)$ resources and the attacker disrupts $(1, 1)$ resources in the two spaces.

By changing the budget of the attacker to 0.01 or 0.03, there is no longer a pure strategy NE. It is because with these budget limits, the attacker will only disrupt the space that has fewer resources, while the defender will deploy more resources in the attacked space only to overcome the disruption, because of the diminishing returns in benefit. Hence, the attacker can always improve its payoff by deviating from the original strategy and disrupting the less protected space instead. However, a mixed strategy NE will always exist. For instance, when the attacker has a budget of 0.01, consider the mixed strategy where the attacker has the same probability of picking $(1, 0)$ and $(0, 1)$ as the attack, and the defender's strategy is to deploy $(7, 7)$ resources. In this case, neither player may improve its payoff by deviating from the original strategy.

(2) Linear benefit function. We assume that the budget of the defender is one. In this case, a pure strategy NE exists as long as the budget of the attacker is less than 0.138, beyond which the payoff of the defender is less than zero because of the disruption by the attacker, even though the overall system is still operational. Hence, there is no incentive for the defender to deploy the system as doing so will invite the attacker to attack and make the defender's payoff negative. At the same time, there is no incentive for the attacker to attack (and spend) if the defender decides not to deploy the system. When there is an NE, the strategy of the defender is always to deploy $(9, 9)$ when its budget is greater than 0.6. This is in contrast to the case of the other benefit functions, where the strategy in general will also depend on that of the attacker.

(3) S-shaped benefit function. We assume that the budget of the defender is 0.5, while that of the attacker is 0.01. Without the attacker, the best strategy of the defender is $(3, 11)$. Notice that because of the S-shaped benefit function, the defender will not allocate resources equally in the two spaces. In particular, the payoff of the space where only three resources are deployed is negative, but the payoff of the other space is much higher, so that an equal allocation will be sub-optimal. Although the game has no pure strategy NE, there are mixed strategy equilibria in the game. For instance, consider the mixed strategy in which the attacker has the same probability of picking $(1, 0)$ and $(0, 1)$ to attack, and the defender has the same probability of picking $(4, 11)$ and $(11, 4)$ as the defense. In this case, neither player can achieve a better payoff by deviating from the original strategy.

When the budget of the defender is one, while that of the attacker is 0.02, a pure strategy NE is found as $(12, 13)$ for the defender and $(1, 1)$ for the attacker. By symmetry, another NE is $(13, 12)$ for the defender and $(1, 1)$ for the attacker.

4.2.2. Different benefit functions for the two spaces. In this section, we study the case that the benefit functions of the two spaces are different.

(1) Negative exponential and linear benefit functions. We assume that the budget of the defender is one, while that of the attacker is 0.02. A pure strategy NE is found when the defender deploys eight resources in the negative exponential benefit space and nine resources in the linear benefit space, while the attacker disrupts $(1, 1)$ resources in the two spaces.

When the budget of the attacker is changed to 0.03, no pure strategy NE exist. However, when the budget of the attacker is changed to 0.01, a pure strategy NE is for the defender to deploy seven resources in the negative exponential benefit space and nine resources in the linear benefit space, while the attacker disrupts one resource in the linear benefit space. Notice that for the above two attacker budgets (i.e., 0.03 and 0.01) and the defender budget, if both spaces have the same linear benefit function, a pure strategy NE exists. When they both have the same negative exponential function, however, a pure strategy NE will not exist.

(2) Negative exponential and S-shaped benefit functions. We assume that the budget of the defender is one, while that of the attacker is 0.02. A pure strategy NE is such that the defender deploys eight resources in the negative exponential benefit space and 14 resources in the S-shaped benefit space, while the attacker disrupts $(1, 1)$ resources in the two spaces.

(3) Linear and S-shaped benefit functions. We assume that the budget of the defender is one, while that of the attacker is 0.02. A pure strategy NE is such that the defender deploys nine resources in the linear benefit space and 14 resources in the S-shaped benefit space, while the attacker disrupts $(1, 1)$ resources in the two spaces.

When the budget of the defender is 0.5, and that of the attacker is 0.02, a pure strategy NE is such that the defender deploys four resources in the linear benefit space and 11 resources in the S-shaped benefit space, while the attacker disrupts $(1, 1)$ resources in the two spaces. Notice that for the above attacker and defender budgets, if both spaces have the same linear benefit function, a pure strategy NE exists. When they both have the same S-shaped function, however, a pure strategy NE will not exist.

4.2.3. Discussion. From the above results (e.g., the examples in Section 4.2.2(1)), the absence of a pure strategy NE when both spaces have the same benefit function A or B does not imply the absence of such an equilibrium when one space has the benefit function A and the other space has the function B. Therefore, the NE results for the individual benefit functions cannot be readily combined to give results of composite cases involving different benefit functions. In general, the analysis is intricate and the NE results are sensitive to detailed parameters of the payoff functions in the two spaces. Furthermore, although we illustrate sample problems in which pure strategy Nash equilibria exist, the existence of such NE appears to be uncommon under general budget constraints.

5. Conclusions

We have presented a game theoretic formulation of the interplay between a rational attacker and a rational defender in cyber-physical system security. We have discussed the existence and solutions of pure- and mixed-strategy Nash equilibria in various game settings and related the analysis to the survival of the overall system. We consider the presented results to be preliminary towards a detailed understanding of the game-theoretic aspects of cyber-physical system security. In particular, detailed models incorporating specific cyber and physical costs of defense and attack would be valuable towards the understanding of real-life deployments. Furthermore, we have considered the cyber and physical components as abstracted "single" systems. The networking components in cyber-physical networks can be considered explicitly, and corresponding game-theoretic results accounting for the more detailed network parameters would be of future interest.

Acknowledgment

Research was supported in part by U.S. Department of Energy under SensorNet grant number AC05-00OR22725 and Mathematics of Complex, Distributed, Interconnected Systems program, Office of Advanced Computing Research, in part by U.S. National Science Foundation under grant number CNS-0964086, and in part by NSFC under grant number 61028007.

References

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

[2] D. Fudenberg and J. Tirole. *Game Theory*. MIT Press, 2003.

[3] J.-C. Laprie, K. Kanoun, and M. Kaaniche. Modelling interdependencies between the electricity and information infrastructures. In *Proc. of the Intl Conf. on Computer Safety, Reliability and Security*, 2007.

[4] J. Lin, S. Sedigh, and A. Miller. A general framework for quantitative modeling of dependability in cyber-physical systems: A proposal for doctoral research. In *Proc. of the IEEE Int'l Computer Software and Applications Conf.*, 2009.

[5] S. M. Rinaldi. Modeling and simulating critical infrastructures and their interdependencies. In *Proc. of the Hawaii Intl. Conf. on System Sciences*, 2004.