Proceedings of the 2012 Industrial and Systems Engineering Research Conference
G. Lim and J.W. Herrmann, eds.

Game-Theoretic Analysis of Attack and Defense in Cyber-Physical Network Infrastructures

Fei He, Jun Zhuang
Department of Industrial and Systems Engineering
State University of New York at Buffalo
Buffalo, NY 14260, United States

Nageswara S. V. Rao
Oak Ridge National Laboratory
Oak Ridge, TN 37831, United States

Abstract

Critical infrastructures rely on cyber and physical components that are both subject to natural, incidental or intentional degradations. Game theory has been used in studying the strategic interactions between attackers and defenders for critical infrastructure protection, but has not been extensively used in complex cyber-physical networks. This paper fills the gap by modeling the probabilities of successful attacks in both cyber and physical spaces as functions of the number of components that are attacked and defended. The results show that the attack effort would first increase then decrease in (a) defense effort, (b) the probability of successful attack on each component, (c) the number of minimum required functioning resources, and (d) the maximum number of available resources. Comparing simultaneous and sequential games, our results show that the defender performs better when she moves first. Our research provides some novel insights into the survival of such infrastructures and optimal resource allocation under various costs and target valuations that players may have.

Keywords
Cyber-physical network infrastructure, attack, defense, game theory, Nash equilibrium

1. Introduction
Cyber-Physical Network Infrastructure (CPNI) consists of hardware, software, people, organizational policies and procedures, all linked by high speed networks [4]. The successful functioning of CPNI requires that both cyber and physical components run smoothly including the functionality after being attacked. CPNI could be viewed as a subset of cyber-physical systems (CPS), which has been studied in the literature. For example, [13] discusses building a trustworthy CPS for power grids at both device and protocol levels; [1] and [8] study both physical and cyber components; [14] analyzes the risk of both cyber infrastructure and physical power controls within electric power grid using a layered approach; [5] proposes a risk assessment methodology to account both physical and cyber security withstanding attacks; [10] uses the dynamic detection method to identify attacks in power networks.

The functioning of CPNI depends on both the defensive resource deployment and the attack effort. Game theory has been used to study the strategic interactions between attackers and defenders, both on a single target [6, 7, 17], and on a network [2, 9, 12, 15, 16]. Within the CPNI field, [3] and [11] formulate the attack and defense as a simultaneous matrix game and use first-order conditions to obtain the best response strategies. However, no previous research studies the probability of system failure in such CPNI games. This paper fills the gap by modeling the probabilities of successful attack in both cyber and physical spaces as functions of the number of components that are attacked and defended. The rest of this paper is organized as follows. Section 2 introduces the probability of system functioning. Section 3 models the interactions between attacker and defender in CPNI and present best responses. Section 4 presents equilibria analysis for both simultaneous and sequential games. Section 5 concludes and provides some future research directions.

2. Probability of System Survival

Table 1 lists the notation that is used in the paper. For simplicity, this paper assumes that the defender and attacker have complete information about each other, including costs, the target valuations, and the successful probability of attack for each components.

Table 1: Notation that is used in this paper

Notation	Explanation
Parameters:	
$i = c, p$	Cyber and physical spaces, respectively
n_i	Maximum number of available resources in cyber and physical spaces, respectively
$k_i \geq 0,$	Parameter for operational resources requirement for space i
$Y_i = 0, 1, 2, \cdots, n_i$	Random variable representing the number of successful attacks in space i
P_i	Probability of system functions in space i
$V \geq 0$	Defender's target valuation
$v \geq 0$	Attacker's target valuation
$p_i \in [0, 1]$	Probability of successful attack on each component in space i
$c_D \geq 0$	Unit cost of defense effort
$c_A \geq 0$	Unit cost of attack effort
Decision variables:	
$x_i = 0, 1, 2, \cdots, n_i$	Defender's resource deployment in space i
$z_i = 0, 1, 2, \cdots, n_i$	Attacker's attack attempts in space i
$\hat{x}_i(z_i) = 0, 1, 2, \cdots, n_i$	Defender's best response of resources deployment in space i
$\hat{z}_i(x_i) = 0, 1, 2, \cdots, n_i$	Attacker's best response of attack attempts in space i
Utilities:	
$U_D(x_i, z_i)$	Defender's utility
$U_A(x_i, z_i)$	Attacker's utility

We assume that there are n_c and n_p components in cyber and physical spaces, respectively. The attacker and defender could attack and defend each component, respectively. We use the attack effort z_i, $i = c, p$ denote the number of components that are attacked in cyber and physical spaces, respectively. Similarly, we use the defense effort x_i, $i = c, p$ denote the number of components that are deployed by the defender in cyber and physical spaces, respectively. Let the random variable Y_i represent the number of components that are successfully attacked in space i, thus we must have $Y_i \leq z_i$. Let p_i be a constant representing the conditional probability of a successful attack, given the component is attacked, on each component in space i. Therefore, the probability of having Y_i components that are successfully attacked, given there are z_i attacks, is given by

$$P_i(Y_i = y_i | z_i) = \binom{z_i}{y_i} p_i^{y_i} (1 - p_i)^{z_i - y_i} \tag{1}$$

Following [3], we assume that the system functions in space i if and only if the number of components survived from attacks $x_i - Y_i$ is strictly greater than the number of minimum operational resources requirement for space i, k_i; that is, $x_i - Y_i \geq k_i + 1$. Therefore, the probability that the system functions in system i could be calculated as follows:

$$\begin{aligned} & P_i(\{\text{System Functions in Space } i \mid \text{Given the attack effort is } z_i \text{ in space } i\}) \\ = \; & P_i(x_i, z_i) \\ = \; & P_i(x_i - Y_i \geq k_i + 1) \\ = \; & \begin{cases} 0 & \text{if } 0 \leq x_i < k_i + 1 \\ \sum_{y_i=0}^{x_i - k_i - 1} \binom{z_i}{y_i} p_i^{y_i} (1 - p_i)^{z_i - y_i} & \text{if } k_i + 1 \leq x_i < z_i + k_i + 1 \\ 1 & \text{if } z_i + k_i + 1 \leq x_i \leq n_i \end{cases} \end{aligned} \tag{2}$$

Figure 1(a-d) illustrate the contours of $P_i(x_i, z_i)$ in Equation (2) when $(k = 2, p = 0.5)$, $(k = 10, p = 0.5)$, $(k = 2, p = 0.1)$, and $(k = 10, p = 0.1)$, respectively. In particular, we observe that $P_i(x_i, z_i)$ increases in x_i and decreases in z_i for each of the four subfigures. Comparing between the subfigures, we observe that P_i decreases in the probability of successful attack p_i and decreases in the number of minimum required functioning servers k_i.

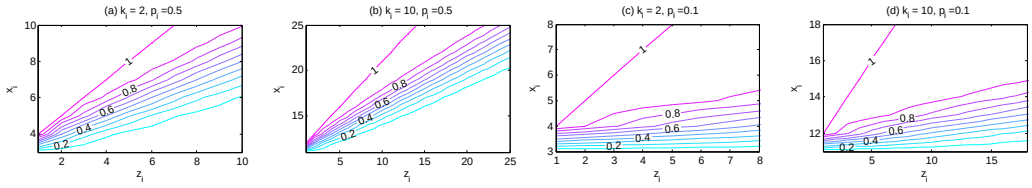

Figure 1: Contours of $P(x_i, z_i)$ when Y_i follows binomial distribution (x_i, p)

3. The Model

3.1 Optimization Problems and Definition of Best Responses

We assume that the defender wants to minimize the cost and system loss; i.e., to maximize her utility as the following:

$$\max_{x_c,x_p} U_D(x_c,x_p,z_c,z_p) = E[u_D(x_c,x_p,z_c,z_p)] - C_D(z_c,z_p) \tag{3}$$

where $E[u_D]$ is the expected payoff of defender, and $C_D(x_c,x_p)$ is the cost of defense. We consider the expected utility of defender as, $E[u_D(x_c,x_p,z_c,z_p)] = P_{cp}V$, where P_{cp} is the probability of system functions, and V is the defender's valuation of the system. Meanwhile the attacker attacks certain amount of components in the two spaces and wants to maximize his utility as the following:

$$\max_{z_c,z_p} U_A(x_c,x_p,z_c,z_p) = E[u_A(x_c,x_p,z_c,z_p)] - C_A(z_c,z_p) \tag{4}$$

where $E[u_A]$ is the expected utility of attacker, and $E[u_A(x_c,x_p,y_c,y_p)] = P_{cp}v$, where v is the attacker's valuation of the system. $C_A(z_c,y_p)$ is the cost of attack.

We define the players' best responses as follows:

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

$$\{\hat{x}_c,\hat{x}_p\}(z_c,z_p) = \arg\max_{x_c\geq 0,x_p\geq 0} U_D(x_c,x_p,z_c,z_p), \quad \forall x_c = 0,1,2,\cdots,n_c; x_p = 0,1,2,\cdots,n_p. \tag{5}$$

and the strategy $\{\hat{z}_c,\hat{z}_p\}(x_c,x_p)$ *is a best response of attacker to defender's defense strategy* (x_c,x_p) *if*

$$\{\hat{z}_c,\hat{z}_p\}(x_c,x_p) = \arg\max_{z_c\geq 0,z_p\geq 0} U_A(x_c,x_p,z_c,z_p), \quad \forall z_c = 0,1,2,\cdots,n_c; z_p = 0,1,2,\cdots,n_p. \tag{6}$$

In the rest of this paper, for simplicity we analyze cyber and physical spaces separately.

3.2 The Attacker's Best response for $n_i = 2$

This subsection studies the simple network containing only two maximum components; i.e., $n_i = 2$. Based on Equation (6), given $n_i = 2, k_i = 0$, the attacker's best response in space i could be calculated as:

$$\hat{z}_i(x_i) = \begin{cases} 0 & \text{if } x_i = 0, \text{ or } \{x_i = 1 \text{ and } v \leq \frac{c_A}{p_i}\}, \text{ or } \{x_i = 2, \text{ and } v \leq \frac{2c_A}{p_i^2}\} \\ 1 & \text{if } x_i = 1, \text{ and } \frac{c_A}{p_i} < v \leq \frac{c_A}{p_i - p_i^2} \\ 2 & \text{if } \{x_i = 1 \text{ and } v > \frac{c_A}{p_i - p_i^2}\} \text{ or } \{x_i = 2 \text{ and } v > \frac{2c_A}{p_i^2}\} \end{cases} \tag{7}$$

The result in Equation (7) shows that the attacker's best response $\hat{z}_i$ increases in his target valuation v, increases in probability of successful attack p_i, and decreases in attack cost c_{A_i}. One interesting finding is that given the high defense level (i.e., $x_i = 2$), the attacker would either attack all targets (when v is high), or not attack at all (when v is low), but he will not choose $z_i = 1$. Figure 2 illustrates the sensitivity of attacker's best responses $\hat{z}_i(x_i)$ when $n_i = 2$ with baseline values $n_i = 2, k = 0, p = 0.5, c_A = 0.2, v = 4$. In particular, Figure 2(a) shows that under the baseline case, the attacker starts to attack when $x_i = 1$ and keeps attacking when $x_i = 2$. Figure 2(b) shows that when k increases to 1, which means the system functionality requirement increases, the attacker does not have to attack when deployment is less than two, but attacks two targets when the defender deploys two. Figure 2(c) shows that if the successful attack probability decreases to 0.1, the attacker is deterred when the defender deploys two resources. Figure 2(d) shows that when the unit cost of attack increases to 1.5, the attacker decreases attack effort to one when the deployment is one, and is fully deterred when the deployment is two. Figure 2(e) presents that the attacker does not launch any attack when his target valuation is as low as 0.4.

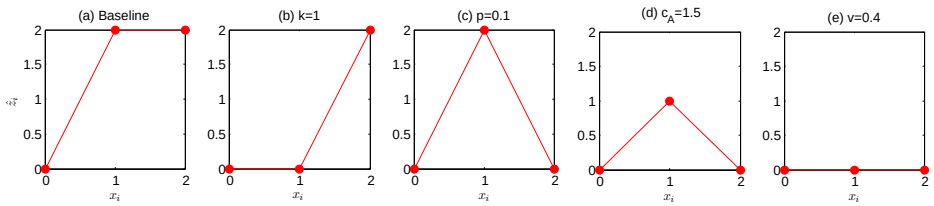

Figure 2: Attacker's best attempts $\hat{z}_i$ given the defender's resource deployment x_i with baseline values $n_i = 2, k = 0, p = 0.5, c_A = 0.2, v = 4$; (a) Baseline; (b) when k = 1; (c) when p = 0.1; (d) when c_A = 1.5; (e) when v = 0.4

3.3 The Attacker's Best response for General n_i

For large values of n_i, it is almost impossible to calculate the analytical solution for the attacker's best response. Therefore, we use numerical solutions to illustrate. For example, Figure 3 shows the attacker's best response given the defender's deployment of resources when n_c(or n_p) = 20. Figure 3(a) shows that when the base line value case that the attacker increases attack effort with the defense effort until the resources defender deploys reaches to 9. Afterwards the attacker is fully deterred. Figure 3(b) presents that when k increases from 2 to 10, the attacker begins to attack when the defender's deployment is larger than 10, and is deterred when defender increases deployment to 17. Figure 3(c) shows that when the probability of successful attack decreases to 0.1, the attacker is deterred when the defender just defend more than 3 resources. Figure 3(d) illustrates that when the cost of attack increase from 0.1 to 0.5, the attacker will only attack if the defender defends 3 or 4 resources. Figure 3(e) shows that when the attacker's target valuation increases from 4 to 10, the attack would like to attack more targets and he is deterred until the defender defends 12 or more resources.

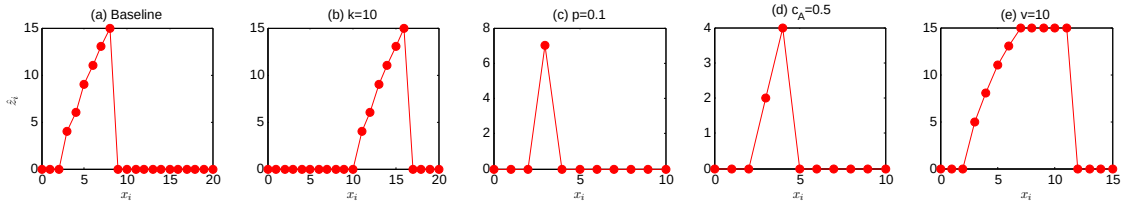

Figure 3: Attacker's best attempts $\hat{z}_i$ given the defender's resource deployment x_i with baseline values $n_i = 20, k = 2, p = 0.5, c_A = 0.2, v = 4$; (a) Baseline; (b) when k = 10; (c) when p = 0.1; (d) when c_A = 0.5; (e) when v = 10

3.4 The Defender's Best Response for $n_i = 2$

Similarly, when $n_i = 2$, the defender's best response in space i could be calculated as:

$$\hat{x}_i(z_i) = \begin{cases} 0 & \text{if } \{z_i = 0, \text{ and } V \le c_D\}, \text{ or } \{z_i = 1 \text{ and } V \le \min(2c_D, \frac{c_D}{1-p_i})\}, \text{ or } \{z_i = 2, \text{ and } V \le \min(\frac{c_D}{(1-p_i)^2}, \frac{2c_D}{1-p_i^2})\} \\ 1 & \text{if } \{z_i = 0, \text{ and } V > c_D\}, \text{ or } \{z_i = 1, \text{ and } \frac{c_D}{1-p_i} < V \le \frac{c_D}{p_i}\}, \text{ or } \{z_i = 2, \text{ and } \frac{c_D}{(1-p_i)^2} < V \le \frac{c_D}{2p_i(1-p_i)}\} \\ 2 & \text{if } \{z_i = 1 \text{ and } V > \max(2c_D, \frac{c_D}{p_i})\} \text{ or } \{z_i = 2 \text{ and } V > \max(\frac{2c_D}{1-p_i^2}, \frac{c_D}{2p_i(1-p_i)})\} \end{cases} \quad (8)$$

From Equation (8) we observe that the defender's best response increases in the target valuation V, decreases in the successful attack probability p_i, and decreases in the defense cost c_{D_i}. Figure 4 represents the defender's best response when $n_i = 2$ with the baseline values $k = 0, p = 0.8, c_D = 0.2, V = 1$. In particular, Figure 4(a) is the baseline case, where the defender deploys one resource, increases to two resources when the attacker attacks one target, and gives up deployment when attack effort is two, due to the defender's relatively low target valuation and high defense cost. Figure 4(b) shows that when k increases to 1, the defender will deploy two resources when no attack, but withdraw defense when the attacker attacks. Figure 4(c) illustrates that when the successful attack probability decreases to 0.1, defender only needs to deploy one resource when the attacker attacks one target, and increases to two resources when he attacks two. Figure 4(d) presents when the unit deployment cost deceases to 0.1, the defender will keep deployment of two resources when the attacker attacks two. Figure 4(e) displays when the defender's target valuation is decreased to 0.1, she will not deploy any resource.

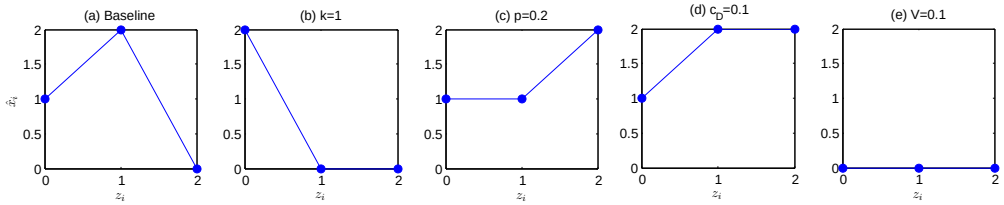

Figure 4: Defender's best deployment $\hat{x}_i$ given the attacker's attack effort z_i with baseline values $k = 0, p = 0.8, c_D = 0.2, V = 1$; (a) Baseline; (b) when k = 1; (c) when p = 0.2; (d) when c_D = 0.1; (e) when V = 0.1

3.5 The Defender's Best Response for General n_i

Figure 5 represents the defender's best response when $n_i = 50, k = 2, p = 0.5, c_D = 0.2, V = 10$. Figure 5 (a) shows the defender increases the deployment when the attacker increases the attack effort until the attack effort is large enough as $z_i = 33$ here. Figure 5 (b) shows that when k increases from 2 to 10, the defender begins to deploy with 10 resources and gives up defense when $z_i = 20$. Figure 5 (c) presents when the probability of successful attack deceases to 0.3, the defender keeps defense until attack effort is high enough, which is $z_i = 42$. Figure 5 (d) shows that when the unit cost of deployment increases to 0.5, the defender gives up defense when the attack effort is as small as $z_i = 12$. Figure 5 (e) shows that when the defender's target valuation decreases to 2, the defender gives up defense when the attacker effort is as low as $z_i = 12$.

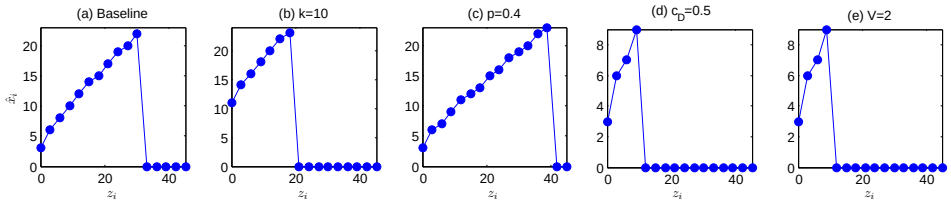

Figure 5: Defender's best deployment $\hat{x}_i$ given the attacker's attack effort z_i with baseline values $n_i = 50, k = 2, p = 0.5, c_D = 0.2, V = 10$; (a) Baseline; (b) when k = 10; (c) when p = 0.4; (d) when c_D = 0.5; (e) when V = 2

4. Equilibrium Analysis

4.1 Simultaneous Game

For simultaneous-move game, we define the equilibrium as follows:

Definition 2. *We call a collection of strategy $(x_c^*, x_p^*, z_c^*, y_p^*)$ a Nash equilibrium, or "equilibrium", if and only if both Equations (9) and (10) are satisfied:*

$$U_D(x_c^*, x_p^*, y_c^*, y_p^*) \geq U_D(x_c, x_p, y_c^*, y_p^*), \quad \forall x_c, x_p = 0, 1, 2, \cdots \tag{9}$$

$$U_A(x_c^*, x_p^*, z_c^*, y_p^*) \geq U_A(x_c^*, x_p^*, z_c, y_p), \quad \forall y_c, y_p = 0, 1, 2, \cdots . \tag{10}$$

Figure 6 illustrates the equilibrium dynamics with baseline values $n_i = 20, k = 2, p = 0.5, c_D = 0.1, c_A = 1, V = 10, v = 2$. In particular, Figure 6(a) shows that the attack effort decreases in the unit cost of attack, while the defense will decrease consequently. Figure 6(b) shows that the both the attacker's and defender's utility decrease in the defender's unit cost of attack. Figure 6(c) shows that when k increases, both attacker and defender efforts will first increase then decrease to zero. Figure 6(d) shows the defender's utility increases in V. Figure 6(e) shows the attacker's utility increases in v. Figure 6(f) shows that both the defense and attack first increase then decrease in the component's successful attack probability. Finally Figure 6(g) shows that both the attacker and defender effort will first increase and then decrease in n_i.

4.2 Sequential Game

The interaction between the defender and attacker can be considered as a sequential game, in which case, the defender moves first to deploy the cyber and physical components, then the attacker observes and decides the attack effort. The

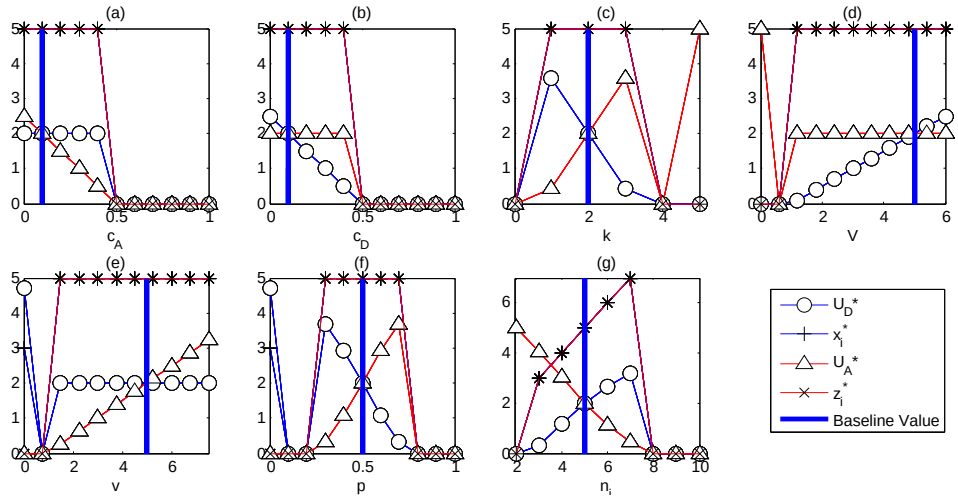

Figure 6: Sensitivity of Nash Equilibrium in a simultaneous game with baseline values $n_i = 5, k = 2, p = 0.5, c_D = 0.1, c_A = 0.1, V = 5, v = 5$

defender and attacker's utility functions are presented as Equation (3) and (4), respectively. We define the equilibrium as follows:

Definition 3. *We call a collection of strategy* $(x_c{}^*, x_p{}^*, z_c{}^*, z_p{}^*)$ *a subgame perfect Nash equilibrium, or "equilibrium", if and only if Equations (11), (12) and (13) are satisfied:*

$$\{\hat{z_c}(x_c, x_p), \hat{z_p}(x_c, x_p)\} = \arg\max_{z_c, z_p \geq 0} U_A(x_c, x_p, z_c, z_p), \tag{11}$$

$$\{x_c^*, x_p^*\} = \arg\max_{x_c, x_p \geq 0} U_D(x_c, x_p, \hat{z_c}(x_c, x_p), \hat{z_p}(x_c, x_p)) \tag{12}$$

$$\{z_c^*, z_p^*\} = \{\hat{z_c}(x_c^*, x_p^*), \hat{z_p}(x_c^*, x_p^*)\} \tag{13}$$

where $\{\hat{z_c}(x_c, x_p), \hat{z_p}(x_c, x_p)\}$ is the attacker's best response.

When $n_i = 2$, based on the attacker's best response $\hat{z}_i(x_i)$ in Equation (7), we are able to solve for the subgame perfect Nash equilibrium and obtain the following equilibrium results:

$$\{\hat{x}_i^*, z_i^*\} = \begin{cases} \{0,0\} & \text{if } \{V \leq c_D\} \\ \{1,0\} & \text{if } \{V > c_D \text{ and } v > \frac{c_A}{p_i}\} \\ \{1,1\} & \text{if } \{\frac{c_D}{1-p_i} \leq V \leq \frac{c_D}{p_i} \text{ and } \frac{c_A}{p_i} < v \leq \frac{c_A}{p_i - p_i^2}\} \\ \{2,2\} & \text{if } \{V > \frac{2c_D}{1-p_i^2} \text{ and } v > \frac{2c_A}{p_i^2}\} \end{cases} \tag{14}$$

For general n_i, we use simulation to illustrate. Figure 7 shows the equilibrium dynamics of $x_i{}^*$, $z_i{}^*$, $U_D{}^*$ and $U_A{}^*$ when one of the parameter varies. Figure 7(a) shows that when the cost of attack increases, the attack effort decreases, as well as the attacker's utility. The defender will use positive defensive investment to deter the attack. After the attacker is deterred, the defender will decrease the defense effort and the her utility increases. Figure 7(b) illustrates that when the cost of deployment increases, the defender will decrease the defensive investment and the system does not function when the resources the defender defends are less than $k+1$. The defender's utility decreases and the attacker gains from the system not functioning. Figure 7(c) shows that when the requirement of resources for the system functioning increases, the defender increases his defensive investment, while the attacker is deterred, then the defender would decrease the defense effort, which makes the system disfunction and benefit the attacker. Figure 7(d) presents that when the defender's target valuation increases, the defender increases the defensive investment and her utility decreases; while the attacker gains when the defender does not defend but he is fully deterred when defender defends. Figure 7(e) shows that when the attacker's target valuation increases, the defender increases defensive investment then decreases to zero due to the high cost. Figure 7(f) illustrates that when the probability of successful attack increases, the attacker first increases the attack effort to destroy the system, and then decreases attack effort when the system becomes so vulnerable that there is no need to attack. Figure 7(g) illustrates that when the maximum number of

available resources increases, the attack effort would first increase then decrease when it becomes too costly for the attacker to succeed. Finally, comparing Figure 6 with Figure 7, we observe that the defender gains (weakly) higher utility by moving first in a sequential game for all ranges of parameter values.

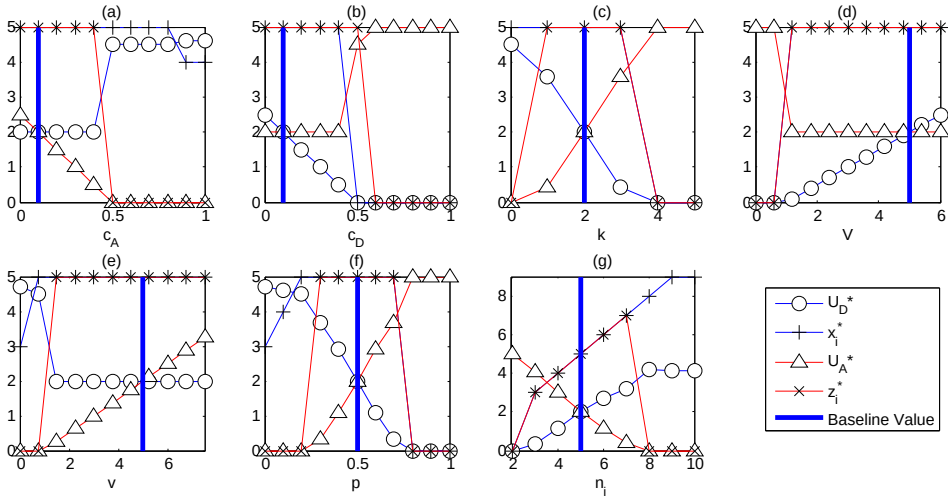

Figure 7: Sensitivity of NE in a sequential game, when y_i follows binomial distribution and $n_i = 5, k = 2, p = 0.5, c_D = 0.1, c_A = 0.1, V = 5, v = 5$

5. Conclusion and Future Research Directions

In this paper we use game theory to model and analyze the attack and defense in CPNI. Critical infrastructures rely on cyber and physical components that are both subject to natural, incidental or intentional degradations. Game theory has been used in studying the strategic interactions between attackers and defenders for critical infrastructure protection, but has not been extensively used in complex cyber-physical networks. This paper fills the gap by modeling the probabilities of successful attack in both cyber and physical spaces as functions of the number of components that are attacked and defended. The results show that the attack effort would first increase then decrease in (a) defense effort, (b) the probability of successful attack on each component, (c) the number of minimum required functioning resources, and (d) the maximum number of available resources. Comparing between simultaneous and sequential games, our results show that the defender performs better when moving first. Our research provides some novel insights into the survival of such infrastructures and optimal resource allocation under various costs and target valuations that players may have.

Future research directions include the study of interdependent coupling effect between the cyber and physical components in the CPNI, as well as the game with incomplete information.

6. Acknowledgements

This work was funded by the Mathematics of Complex, Distributed, Interconnected Systems Program, Office of Advanced Computing Research, U.S. Department of Energy, and was 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 was 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. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security, or CREATE. We also thank Ms. Marie Catalano (University at Buffalo) for editorial help.

References

[1] Amin, S. M, 2010, Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems, *Proceedings of the Power and Energy Society General Meeting, IEEE*, Minneapolis, MN,

September.

[2] Brown, G., Carlyle, M., Salmeron, J., and Salmeron, K., 2006, Defending critical infrastructure, *Interfaces*, 36 (6):530–544.

[3] Rao, N. S. V., Ma, C. Y. T., and Yau, D. K. Y., 2011, A game theoretic study of attack and defense in cyber-physical systems, *IEEE INFOCOM Workshop*, Shanghai, China.

[4] Chittister, C. G., and Haimes, Y. Y., 2011, The role of modeling in the resilience of cyberinfrastructure systems and preparedness for cyber intrusions, *Journal of Homeland Security and Emergency Management*, 8(1), Article 6.

[5] Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G. B., and Wyss, G., 2005, Risk assessment for physical and cyber attacks on critical infrastructures, *Military Communications Conference, 2005. MILCOM 2005. IEEE*, pages 1961–1969. IEEE.

[6] Hausken, K. and Zhuang, J., 2011, Governments' and terrorists' defense and attack in a T-period game, *Decision Analysis*, 8(1):46–70.

[7] He, F. and Zhuang, J., 2011, Modeling 'contracts' between a terrorist group and a government in a sequential game, *Journal of the Operational Research Society*, August, doi10.1057/jors.2011.49.

[8] LaRocca, S. and Guikema, S., 2011, A survey of network theoretic approaches for risk analysis of complex infrastructure systems, *Vulnerability, Uncertainty, and Risk: Analysis, Modeling, and Management Proceedings of the International Conference on Vulnerability and Risk Analysis and Management (ICVRAM) and International Symposium on Uncertainty Modeling and Analysis (ISUMA)*, Hyattsville, MD, April.

[9] Lye, K. and Wing, J.M., 2005, Game strategies in network security, *International Journal of Information Security*, 4(1):71–86.

[10] Pasqualetti, F., Dörfler, F., and Bullo, F., 2011, Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design, pages 2195–2201, Orlando, FL, USA, December.

[11] Rao, N. S. V., Poole, S. W., Ma, C. Y. T., He, F., Zhuang, J., and Yau, D. K. Y., 2012, Cloud computing infrastructure robustness: A game theory approach, *Proceedings of the International Conference on Computing, Networking and Communications*, Maui, Hawaii, January.

[12] Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., and Wu, Q., 2010, A survey of game theory as applied to network security, *Hawaii International Conference on System Sciences*, pages 1–10, IEEE Computer Society.

[13] Sanders, W.H., 2010, Progress towards a resilient power grid infrastructure, *Proceedings of the Power and Energy Society General Meeting, 2010 IEEE*, pages 1–3, Minneapolis, MN, IEEE.

[14] Sridhar, S., Hahn, A., and Govindarasu, M., 2011, Cyber–physical system security for the electric power grid, *Proceedings of the IEEE*, (99):1–15.

[15] Zhuang, J., 2010, Impacts of subsidized security on stability and total social costs of equilibrium solutions in an N-Player game with errors, *The Engineering Economist*, 55(2):131–149.

[16] Zhuang, J. and Bier, V. M., 2007, Balancing terrorism and natural disasters—Defensive strategy with endogenous attacker effort, *Operations Research*, 55(5):976–991.

[17] Zhuang, J., Bier, V. M., and Alagoz, O., 2010, Modeling secrecy and deception in a multiple-period attacker-defender signaling game. *European Journal of Operational Research*, 203(2):409–418.