Bayesian Games for Optimal Cybersecurity Investment with Incomplete Information on the Attacker

Yunfei Zhao[a], Linan Huang[b], Quanyan Zhu[b], and Carol Smidts[a]

[a] Nuclear Engineering Program, Department of Mechanical and Aerospace Engineering, The Ohio State University, 201 W 19th Ave, Columbus, OH 43210, United States of America, zhao.2263@osu.edu, smidts.1@osu.edu

[b] Department of Electrical and Computer Engineering, New York University, 370 Jay Street, Brooklyn, NY 11201, United States of America, lh2328@nyu.edu, qz494@nyu.edu

Abstract: The trend of digitization in various industrial systems has exposed them to an increasing number of cyberattacks. Therefore, it is of vital importance to reduce the cybersecurity risk of industrial systems through cost-effective decisions on cybersecurity investment. In making such decisions, the defender is usually faced with challenges that arise from incomplete information about the attacker. In this paper, we propose a Bayesian game approach to model the optimal cybersecurity investment strategy under such situations. In this approach, the defender categorizes the attacker into a finite number of types, e.g., various levels of capability, and assigns a probability distribution over the different types of attackers. Then, the defender optimizes his/her cybersecurity investment based on risk assessment considering the possible attack efforts of these various types of attackers, with the objective of minimizing the expected cyberattack loss and the cybersecurity investment cost. The proposed method is demonstrated using a numerical example. We perform a sensitivity analysis for model parameters that can be difficult to obtain in practical applications, e.g., the defender's loss caused by a successful attack. Key observations of the example include the threshold principle (i.e., the defender should not make any investment if the loss of a successful attack is below a certain threshold) and the conservation of loss (i.e., losses for one type of attacker may correspond to gains for another type of attacker). The proposed method can be used to support cybersecurity investment decisions by industrial system owners.

1. INTRODUCTION

Digital technologies are in pervasive use today in various industrial systems, for example, electric power systems and nuclear power plants. Although the increased digitization will yield many benefits in terms of the safety and efficiency of the industrial systems, it may also create new vulnerabilities that must be mitigated [1]. Past events caused by cyberattacks and leading to material consequences include the one against Iranian nuclear facilities in 2010 [2] and the one against Ukrainian electric power systems in 2015 [3].

To improve cybersecurity, stakeholders of industrial systems can invest in security hardening mechanisms to manage cyber risk. These include measures to reduce vulnerabilities, boost the capability of intrusion detection [4], and enhance the capability of incident response [5]. Although general guidelines for improving cybersecurity are available [6], optimal cybersecurity investment remains a challenging problem, and is identified as one of the gaps in cybersecurity capabilities [7]. Cybersecurity investment belongs to the broader area of economics of information security [8].

The challenge in cybersecurity investment is due to the need of the decision-maker to consider the trade-off between the investment itself (i.e., cost) and its impact on cyber risk (i.e., benefit). The existence of the malicious attacker in cybersecurity investment problems further implies that cyber risk is not only influenced by the decision-maker's (i.e., defender's) own investment, but also by the attacker's effort. This contrasts with investment problems that are only concerned about natural failures in industrial

systems. In most cases, the defender has incomplete information about the attacker. For example, the defender may not be sure of the capability of the attacker, or the motivation of the attacker. This incomplete information further complicates cybersecurity investment.

In this research, we study how to optimally make investment decisions to improve the cybersecurity of industrial systems. The primary contribution of this research is the Bayesian game-theoretic approach to address the challenge of cybersecurity investment under incomplete information about the attacker. The results from this research can be used to support industrial system owners in making cybersecurity investment decisions.

2. RELATED WORK

One of the foundational works on cybersecurity investment is the Gordon-Loeb model developed by Gordon and Loeb [9]. The Gordon-Loeb model uses a security breach probability function to link investment in security and the probability that a threat once realized (i.e., an attack) would be successful. It identifies the optimality condition under which the expected net benefit of information security is maximized. Various extensions of this model have been studied in later research [10-12]. For example, Hausken [10, 11] investigated different forms of the security breach probability function and studied their effect on the optimality condition. Krutilla et al. [12] extended the original Gordon-Loeb model, which is for one-period decision-making, to a dynamic model. In the dynamic model, cybersecurity investment is formulated as an infinite-horizon decision-making problem, and the depreciation of cybersecurity investment is considered explicitly. Uncertainties usually exist in the loss caused by a successful cyberattack and the availability of cybersecurity controls. Chronopoulos et al. [13] proposed a real options framework to consider such uncertainties and their effect on cybersecurity investment. Real options analysis was also applied in [14] to study whether cybersecurity expenditures should be invested now or deferred and in [15] to study how information sharing, which can reduce the uncertainty surrounding cost savings from security investment, influences the investment decision. Simon and Omar [16] considered the interdependence between protected nodes in cybersecurity investment in a supply chain, i.e., the attack on one node may cause damage to another node. They investigated conditions where the defense may be coordinated or uncoordinated and the attacker may be strategic or non-strategic. It is worth noting that the studies introduced above all formulate cybersecurity investment as a single-agent decision-making problem.

Since in cybersecurity investment problems, there exist both the defender, who aims to protect the systems he/she owns or operates, and the attacker, who aims to cause damage to the systems owned or operated by the defender, it is more natural and sensible to consider such problems as games [17-19]. This suggests the use of game theory to address cybersecurity, and more generally security, investment problems.

For cybersecurity investment problems, Fielder et al. [20] applied game theory to optimal implementation of discrete cybersecurity controls for several data assets against commodity attacks under a limited cybersecurity budget. Gao and Zhong [21] studied the decisions on cybersecurity investment, among others, of two competing firms, both faced with cyberattacks, using differential games. The effects of cooperation and non-cooperation between the two firms on the firms' cybersecurity investments and benefits were investigated. In addition to the theoretical analysis introduced above, Frey et al. [22] designed a tabletop game to study the cybersecurity decision of three different stakeholders, i.e., security experts, computer scientists, and managers, within an organization. The game can be used as a sandbox in which different stakeholders can experiment with security decisions and learn about their decisions. Maccarone and Cole [23] studied nuclear power plant defender defense strategies using Bayesian games to address the incomplete information on the attacker, but the study was focused on discrete defender actions. In this research, we focus on continuous defender investment in improving cybersecurity. Zhao et al. [24] recently created a multi-stage game framework to develop the security investment strategies to combat ransomware. An optimal security investment can significantly reduce the likelihood of ransomware infection and ransom payment.

Research focused on the evaluation of cybersecurity investment impact has also been performed in the literature. For example, Armenia et al. [25] developed a system dynamics methodology for cyber risk assessment and investment impact evaluation, with a focus on dynamic organizational environments.

Game theory has also been used to study how to optimally allocate limited resources among several potential physical targets to enhance their security. Powell [26] studied the optimal allocation of resources against terrorist attacks in four settings using game theory. These include the basic setting where the resource allocated to one target has no effect on any other site, to more complex settings, where certain resources allocated can protect all sites, both strategic and non-strategic threats exist, and the defender is unsure of the terrorist's valuation of the targets. Zhuang and Bier [27] researched how to optimally balance resource allocation for terrorism and natural disasters. Both the simultaneous game and the sequential game were analyzed. The analysis suggested that the defender should in general use a sequential game (for example, by advertising the defensive investments instead of keeping them secret) because it provides the defender the first-mover advantage. This is consistent with the observation in [28]. Instead of only considering two states, i.e., failed or operating, Hausken and Levitin [29] modeled systems as multi-state, and combined game theory and genetic algorithm to determine the optimal defense strategy, to minimize the expected loss from an attack. Zhang et al. [30] studied the effect of player risk attitudes on the decisions on resource allocation in a defender-attacker game. The observation from this study is that misconception of the attacker's risk attitude can significantly increase the expected damage from an attack. Secrecy has also been an important topic in defensive resource allocation. Using signaling games, Powell [31] studied defensive resource allocation when the defender has private information about the target vulnerability. The analysis shows how the resource allocation strategy is affected by the vulnerability characteristics of the targets, i.e., the required marginal effort to protect the more vulnerable targets. Zhuang and Bier [32] provided a thorough perspective on how defender private information can be used to improve defense effectiveness. They discussed several conditions that motivate the secrecy of resource allocation information.

3. PROBLEM DESCRIPTION

This research focuses on the protection of a piece of cyber equipment from malicious cyberattacks. The equipment could be, for example, a workstation or a data historian used in the control system in a nuclear power plant. The compromise of the equipment will lead to a loss of C, which may correspond to, for example, the impact of the compromise of the control system on the physical systems. To protect the equipment, the defender can make an investment of $a_1 \in [0, +\infty)$ in the form of firewalls, cybersecurity personnel, etc. The investment is the defender's action, and the set $[0, +\infty)$ is the defender's action space. This investment reduces the vulnerability of the equipment, or in other words the probability that the equipment can be compromised by the attacker.

This vulnerability is also affected by the attacker's effort, denoted by $a_2 \in [0, +\infty)$, in compromising the equipment. This effort is referred to as the attacker's action, and the set $[0, +\infty)$ is the attacker's action space. In this work, we consider one attacker who can belong to multiple types. We define Θ_2 as the set of all types, which are determined based on the attacker's unknown information (e.g., the attacker's capability, tools, and goals). The attacker's type $\theta_2 \in \Theta_2$ remains unknown to the defender. For example, we can let Θ_2 be a binary set. The first element in Θ_2, denoted as θ_2^h, represents a more capable attacker. The other element, denoted as θ_2^l, represents a less capable one. The defender does not know the attacker's capability.

The attacker determines his/her action based on his/her type, thus we represent the attacker's action as a function of the type of the attacker, i.e., $a_2 = \sigma_2(\theta_2)$, where σ_2 is the attacker's decision-making policy. While the attacker takes the same action a_2, the type of the attacker can affect the outcome of this action. Following the previous example, given the same amount of effort a_2, the attacker of the more capable type θ_2^h will compromise the equipment with a higher probability. Therefore, the vulnerability of the equipment is a function of the investment made by the defender a_1, the type of the attacker θ_2, and the effort made by the attacker $a_2 = \sigma_2(\theta_2)$, i.e., $v(a_1, \sigma_2(\theta_2), \theta_2)$.

Although the defender does not know about the type of the attacker, he/she holds beliefs in the types of the attacker, denoted by $p(\theta_2)$. This portrays the fact that the defender only possesses incomplete information about the attacker.

The defender, uncertain about the type of the attacker, aims to find the amount of investment a_1 to maximize the utility $u_1(a_1, \sigma_2)$ formulated below while considering the effort of an attacker of all types,

$$u_1(a_1, \sigma_2) = \sum_{\theta_2 \in \Theta_2} -C \cdot p(\theta_2) \cdot v(a_1, \sigma_2(\theta_2), \theta_2) - a_1, \quad (1)$$

In (1), a_1 denotes the defender's investment; σ_2 denotes the attacker's attack policy; C denotes the loss to the defender caused by a successful cyberattack; $p(\theta_2)$ denotes the defender's belief in the type of the attacker of type θ_2; and $v(a_1, \sigma_2(\theta_2), \theta_2)$ denotes the probability that a cyberattack will be successful given a_1, θ_2, and $\sigma_2(\theta_2)$. In the utility function for the defender in (1), the summation term on the right side defines the risk caused by a cyberattack. The utility can be explained as the negative of the sum of the expected loss caused by a cyberattack and the defender's investment.

The attacker of type θ_2, knowing his/her type, aims to find the decision policy to maximize his/her utility $u_2(a_1, \sigma_2(\theta_2), \theta_2)$ defined below:

$$u_2(a_1, \sigma_2(\theta_2), \theta_2) = C \cdot v(a_1, \sigma_2(\theta_2), \theta_2) - \sigma_2(\theta_2). \quad (2)$$

In defining the utility for an attacker of each type in (2), we assume that the attacker aims to maximize the loss to the defender. This assumption can be relaxed easily, and a more general utility function can be defined. The utility for the attacker of type θ_2 in (2) can be explained as the expected loss to the defender minus the attacker's investment.

The assumption required for solving this problem using game theory is that the action spaces of the defender and the attacker, the type set of the attacker, the probability distribution over the type set, and the utility functions of the defender and the attacker are all common knowledge. This means that each player (i.e., the defender or the attacker) knows the information above; each player knows that the other player knows the information; each player knows that the other player knows that he/she knows the information, etc.

4. BAYESIAN GAMES AND BAYESIAN NASH EQUILIBRIUM

In the problem described in Section 3, the defender is uncertain about the type of the attacker, so it can be formulated as a game of incomplete information or a Bayesian game. In this research, we consider a specific form of Bayesian games. In such a Bayesian game, the two players move simultaneously without knowing the opponent's action.

The solution concept for solving such a Bayesian game is the Bayesian Nash equilibrium [33]. A strategy profile (a_1^*, σ_2^*) is a Bayesian Nash equilibrium if, for the defender, we have

$$a_1^* \in \underset{a_1 > 0}{\operatorname{argmax}}\, u_1(a_1, \sigma_2^*), \quad (3)$$

and for the attacker of all types $\theta_2 \in \Theta_2$, we have

$$\sigma_2^*(\theta_2) \in \underset{\sigma_2(\theta_2)}{\operatorname{argmax}}\, u_2(a_1^*, \sigma_2(\theta_2), \theta_2). \quad (4)$$

To find the equilibrium, we first need to obtain the following first-order conditions:

$$\frac{\partial u_1(a_1, \sigma_2)}{\partial a_1} = \sum_{\theta_2 \in \Theta_2} -C \cdot p(\theta_2) \cdot \frac{\partial v(a_1, \sigma_2(\theta_2), \theta_2)}{\partial a_1} - 1 = 0, \quad (5)$$

$$\frac{\partial u_2(a_1, \sigma_2(\theta_2), \theta_2)}{\partial \sigma_2(\theta_2)} = C \cdot \frac{\partial v(a_1, \sigma_2(\theta_2), \theta_2)}{\partial \sigma_2(\theta_2)} - 1 = 0, \forall \theta_2 \in \Theta_2. \quad (6)$$

The Bayesian Nash equilibrium can then be obtained by solving the system of equations for a_1 and $\sigma_2(\theta_2)$ in (5) and (6). In (5), the defender considers all possible types of attackers, each denoted by θ_2, as well as their corresponding probabilities, denoted by $p(\theta_2)$ for type θ_2. In (6), the attacker of each type θ_2 considers how the defender's investment is affected by all the possible types of attackers.

5. NUMERICAL EXAMPLE

In this section, an example cybersecurity investment problem is analyzed based on the Bayesian game introduced in Section 4. In this example, a loss of C is incurred for the defender if a piece of cyber equipment is compromised by the attacker. There are two types of attackers, one with high capability and the other with low capability. Denote these two types by $\theta_2 = H$ and $\theta_2 = L$, respectively. The defender believes that $\theta_2 = H$ with probability $p(H)$ and $\theta_2 = L$ with probability $p(L) = 1 - p(H)$. For defender investment a_1, attacker type θ_2, and attacker effort $\sigma_2(\theta_2)$, the vulnerability of the equipment is

$$v(a_1, \sigma_2(H), H) = \frac{\sigma_2(H)}{\alpha_H(a_1 + \sigma_2(H) + \beta)} \quad (7)$$

for type $\theta_2 = H$, where $\alpha_H \geq 1$ and $\beta > 0$, and

$$v(a_1, \sigma_2(L), L) = \frac{\sigma_2(L)}{\alpha_L(a_1 + \sigma_2(L) + \beta)} \quad (8)$$

for type $\theta_2 = L$, where $\alpha_L > 1$ and $\alpha_L > \alpha_H$. The form of the vulnerability functions in (9) and (10) follows the example considered in [27]. By varying α_H or α_L, we can increase or decrease the capability of an attacker. It is clear that both successful attack probabilities in (7) and (8) increase with increasing attacker effort and decrease with increasing defender investment. The probabilities also increase with decreasing α_H and α_L. The parameter β in the denominators reflects the inherent security measures already placed in the equipment.

In this numerical example, the nominal values of the parameters in the middle column in Table 1 are considered. The value ranges of the parameters are used to study the effect of the change in each parameter on the result.

Table 1: The Nominal Values and the Value Ranges of the Parameters in the Numerical Example.

Parameters (unit)	Nominal Value	Value Range
C (in USD)	1000	[0, 2000]
$p(H)$ (unitless)	0.6	[0, 1]
α_H (unitless)	5	[1, 10)
α_L (unitless)	10	(5, 20]
β (in USD)	5	[1, 10]

Using the expressions in (7) and (8), the utility functions for the players can be expressed explicitly as

$$\begin{aligned} u_1(a_1, \sigma_2) &= \sum_{\theta_2 \in \Theta_2} -C \cdot p(\theta_2) \cdot v(a_1, \sigma_2(\theta_2), \theta_2) - a_1 \\ &= -C \cdot p(H) \cdot \frac{\sigma_2(H)}{\alpha_H(a_1 + \sigma_2(H) + \beta)} - C \cdot p(L) \cdot \frac{\sigma_2(L)}{\alpha_L(a_1 + \sigma_2(L) + \beta)} - a_1 \end{aligned} \quad (9)$$

for the defender,

$$u_2(a_1, \sigma_2(H), H) = C \cdot v(a_1, \sigma_2(H), H) - \sigma_2(H) = C \cdot \frac{\sigma_2(H)}{\alpha_H(a_1 + \sigma_2(H) + \beta)} - \sigma_2(H) \qquad (10)$$

for the attacker of type H, and

$$u_2(a_1, \sigma_2(L), L) = C \cdot v(a_1, \sigma_2(L), L) - \sigma_2(L) = C \cdot \frac{\sigma_2(L)}{\alpha_L(a_1 + \sigma_2(L) + \beta)} - \sigma_2(L) \qquad (11)$$

for the attacker of type L.

The Bayesian Nash equilibrium for a static Bayesian game with a particular parameter setting can be obtained by solving (3) and (4), or equivalently (5) and (6) for the utility functions in (9), (10), and (11). For the particular parameter setting in Table 1 (nominal values) considered in this numerical example, the Bayesian Nash equilibrium can be obtained as $(a_1^* = 33.97\ USD, \sigma_2^*(H) = 49.31\ USD, \sigma_2^*(L) = 23.46\ USD)$. At this equilibrium, the utilities for the defender, the attacker of type H, and the attacker of type L are $u_1(a_1^*, \sigma_2^*) = -116.03\ USD$, $u_2(a_1^*, \sigma_2^*(H), H) = 62.40\ USD$, and $u_2(a_1^*, \sigma_2^*(L), L) = 14.12\ USD$, respectively.

We further investigate the effects of changes in parameter values on the outcome of the game. Specifically, for each of the five parameters in Table 1, its value is changed within the range for the parameter while the other parameters are maintained at their nominal values. Then, for each parameter setting, the Bayesian Nash equilibrium is obtained as well as the utilities for the players. The results are presented in Figure 1 to Figure 5.

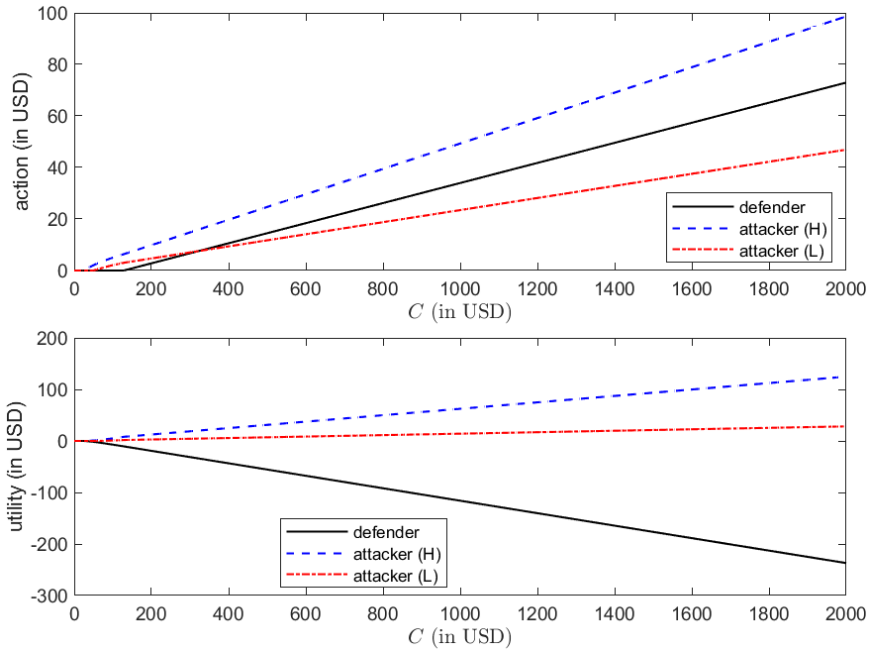

Figure 1. The effect of C on the outcome.

Player actions and utilities at the equilibrium vs. parameter C are plotted in Figure 1. From the results, we see that for a broad range of C, both the defender investment and the attacker effort increase almost linearly with C. Correspondingly, the utility for the attacker of either type and the loss for the defender increase with C. From Figure 1, we also see that when C is smaller than a certain value (about 120 USD), the defender does not make any investment. However, even when C is smaller than this value, the attacker of either type makes an effort in an attack.

Figure 2 plots player actions and utilities at the equilibrium vs. parameter $p(H)$, i.e., the defender's belief that the attacker is of type H. The result shows that, as $p(H)$ increases, the defender will make more investment, but this increase in investment does not help increase the utility for the defender. As

$p(H)$ increases, the effort made by the attacker of type H will increase, while the effort made by the attacker of type L will decrease. This means that if the attacker is of type L, but the defender highly believes that the attacker is of type H, then the attacker (of type L) will make less effort in the cyberattack. It is a deterrence effect commonly observed in security research. We also observe that the utility of the attacker of either type will decrease as $p(H)$ increases, which in part is due to the increased investment of the defender.

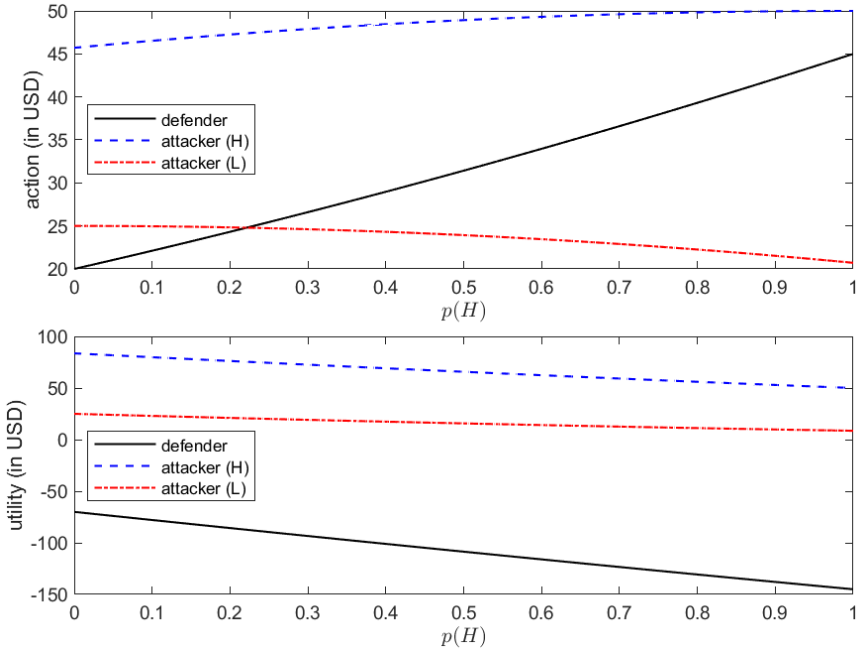

Figure 2. The effect of $p(H)$ on the outcome.

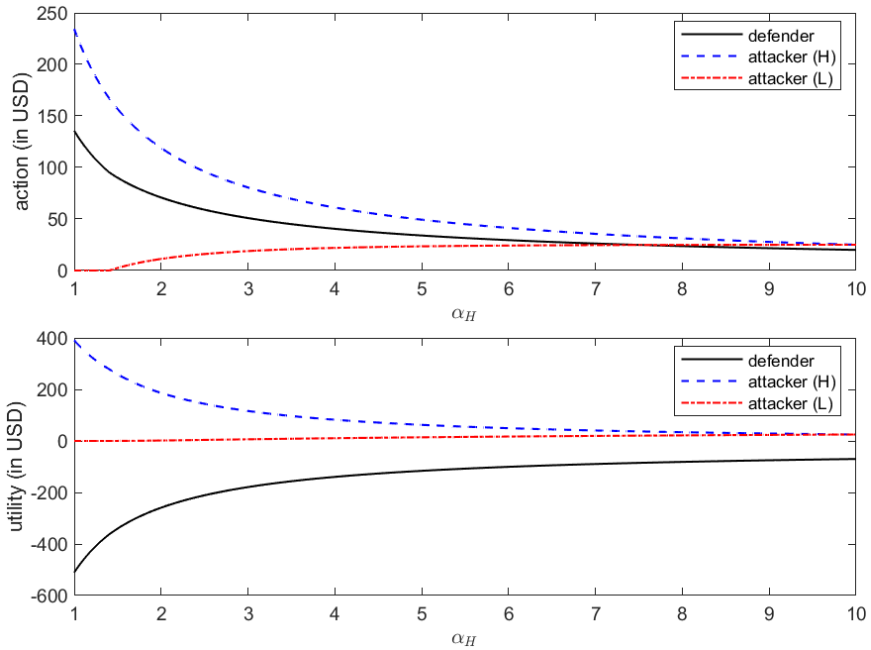

Figure 3. The effect of α_H on the outcome.

Figure 3 plots player actions and utilities at the equilibrium vs. parameter α_H. According to (7), the smaller α_H is, the more capable the attacker of type H is. The result shows that when α_H is small, the investment required by the defender is significantly large. Correspondingly, the loss incurred for the defender when α_H is small is large. We can also observe that as α_H increases, i.e., the capability of the attacker of type H decreases, the utility of the attacker of type L increases slightly, which means that

the attacker of type L benefits from the increased α_H. This can be explained by the decreased investment of the defender.

Figure 4 plots player actions and utilities at the equilibrium vs. parameter α_L. The smaller α_L is, the more capable the attacker of type L is. Similar to the observation from Figure 3, as α_L increases, the investment required by the defender decreases, and its utility increases. We can also observe that as α_L increases, the utility of the attacker of type H increases, which means that the attacker of type H benefits from the decreased capability of an attacker of type L.

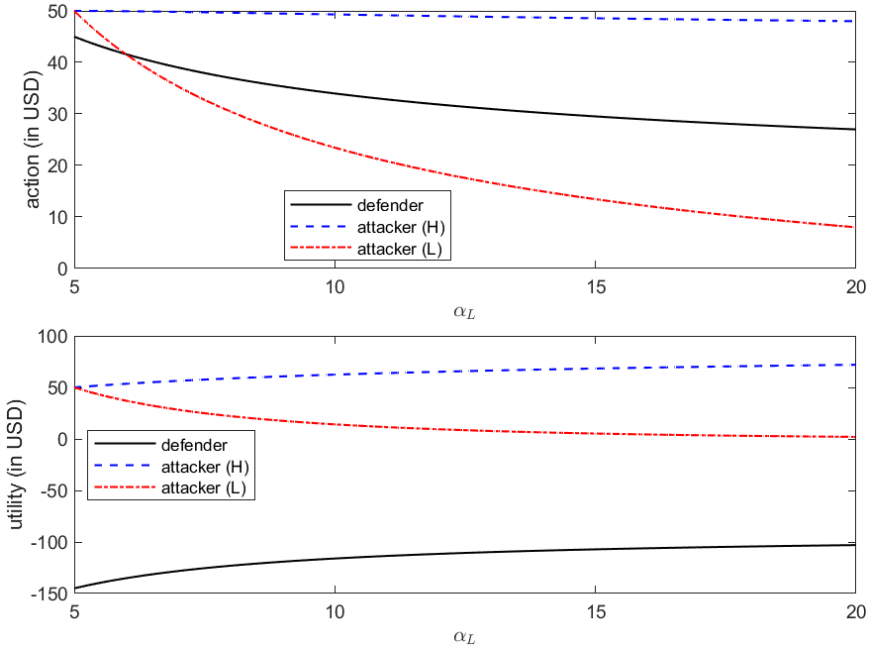

Figure 4. The effect of α_L on the outcome.

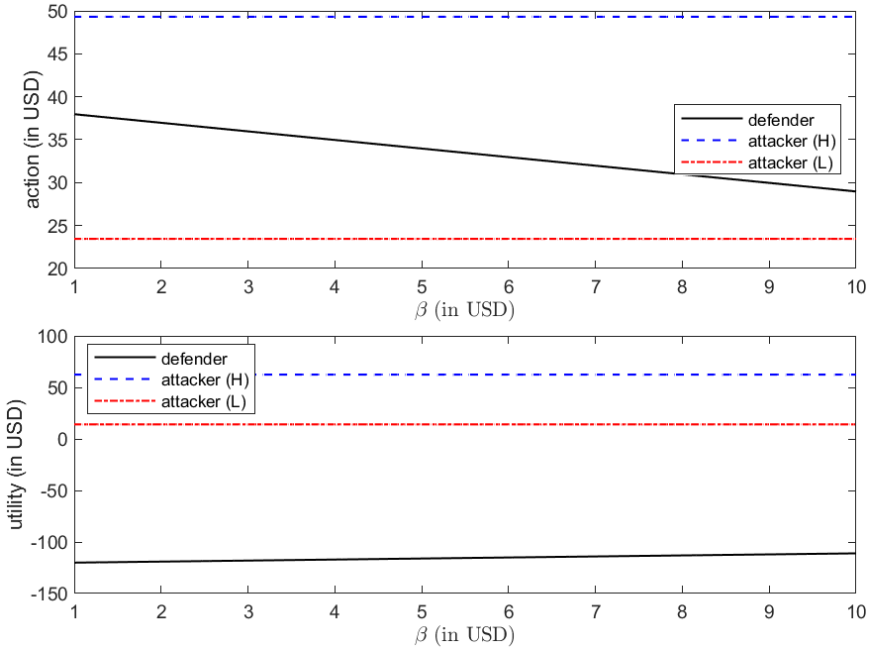

Figure 5. The effect of β on the outcome.

Figure 5 plots player actions and utilities at the equilibrium vs. parameter β. Since β can be viewed as the existing cybersecurity measures embedded in the equipment, from Figure 5 we see that as β increases the defender's investment decreases. The effort made by the attacker of either type does not

change. This can be explained by the fact that any deficiency in existing cybersecurity measures will be compensated by the defender. The utility of the defender increases slightly as β increases, since the investment itself is smaller.

6. CONCLUSION AND FUTURE RESEARCH

In view of the rapid digitization in various industrial systems, for example, nuclear power plants, making optimal decisions on cybersecurity investment becomes a critical task. In this research, we propose a Bayesian game approach to this problem. Compared with the Gordon-Loeb model and other methods that solely focus on the defender investment, the proposed method considers the role of the attacker and the adaptive nature of the attacker. Compared with existing studies based on game theory, we consider the situation where the defender has incomplete information on the attacker. The proposed method is demonstrated using a numerical example, with discussions on the results.

It is worth mentioning that cybersecurity investment is a complex problem. Our research is only one of the attempts to address it, and more future efforts in this field are warranted. In this research, we only consider one single defender and one single attacker, though various types of attackers may exist. In future research, for certain problems, it may be necessary to expand the analysis in this paper to multiple players. For example, there may be attackers from different groups. The analysis in this research is based on given parameters and functions, including the loss due to a successful attack, the vulnerability function, and utility functions for the defender and the attacker. In practical applications, these parameters and functions are typically unknown and need to be determined. A credible way of determining these parameters and functions is worth further research. It is also useful to extend the analysis in this research to investment against both strategic threats, i.e., attackers, and non-strategic threats, e.g., natural system failures, as was done in [27].

Acknowledgments

This research is being performed using funding received from the DOE Office of Nuclear Energy's Nuclear Energy University Programs.

References

1. U.S. DHS, Roadmap to Enhance Cyber Systems Security in the Nuclear Sector, Technical Report, U.S. Department of Homeland Security, 2011.
2. N. Falliere, L. O. Murchu, E. Chien, W32. stuxnet dossier, Technical Report, Symantec Corp., 2011.
3. U.S. Cybersecurity & Infrastructure Security Agency, ICS Alert (IRALERT-H-16-056-01): Cyber-attack against ukrainian critical infrastructure, https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01, 500 2021. (Accessed: 07/30/2021).
4. P. K. Vaddi, M. C. Pietrykowski, D. Kar, X. Diao, Y. Zhao, T. Mabry, I. Ray, C. Smidts, Dynamic bayesian networks based abnormal event classifier for nuclear power plants in case of cyber security threats, Progress in Nuclear Energy 128 (2020) 103479.
5. Y. Zhao, L. Huang, C. Smidts, Q. Zhu, Finite-horizon semi-markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants, Reliability Engineering & System Safety 201 (2020) 106878.
6. NIST, Framework for improving critical infrastructure cybersecurity, Technical Report, National Institute of Standards and Technology, 2018.
7. U.S. DHS, Cyber Risk Economics Capability Gaps Research Strategy, Technical Report, U.S. Department of Homeland Security, 2018.
8. R. Anderson, T. Moore, The economics of information security, science 314 (2006) 610-613.
9. L. A. Gordon, M. P. Loeb, The economics of information security investment, ACM Transactions on Information and System Security (TISSEC) 5 (2002) 438-457.

10. K. Hausken, Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability, Information Systems Frontiers 8 (2006) 338-349.
11. K. Hausken, Returns to information security investment: Endogenizing the expected loss, Information Systems Frontiers 16 (2014) 329-336.
12. K. Krutilla, A. Alexeev, E. Jardine, D. Good, The benefits and costs of cybersecurity risk reduction: A dynamic extension of the gordon and loeb model, Risk Analysis (2021).
13. M. Chronopoulos, E. Panaousis, J. Grossklags, An options approach to cybersecurity investment, IEEE Access 6 (2017) 12175-12186.
14. L. A. Gordon, M. P. Loeb, W. Lucyshyn, Information security expenditures and real options: A wait-and-see approach, Computer Security Journal 19 (2003).
15. L. A. Gordon, M. P. Loeb, W. Lucyshyn, L. Zhou, The impact of information sharing on cybersecurity underinvestment: A real options perspective, Journal of Accounting and Public Policy 34 (2015) 509-519.
16. J. Simon, A. Omar, Cybersecurity investments in the supply chain: Coordination and a strategic attacker, European Journal of Operational Research 282 (2020) 161-171.
17. M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacsar, J.-P. Hubaux, Game theory meets network security and privacy, ACM Computing Surveys (CSUR) 45 (2013) 1-39.
18. P. Jeffrey, Q. Zhu. Game Theory for Cyber Deception. Springer International Publishing, 2021.
19. S. Rass, S. Schauer, S. König, Q. Zhu. Cyber-Security in Critical Infrastructures. Springer International Publishing, 2020.
20. A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi, Decision support approaches for cyber security investment, Decision support systems 86 (2016) 13-23.
21. X. Gao, W. Zhong, A differential game approach to security investment and information sharing in a competitive environment, IIE Transactions 48 (2016) 511-526.
22. S. Frey, A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque, S. A. Naqvi, The good, the bad and the ugly: a study of security decisions in a cyber-physical systems game, IEEE Transactions on Software Engineering 45 (2017) 521-536.
23. L. T. Maccarone, D. G. Cole, Bayesian games for the cybersecurity of nuclear power plants, International Journal of Critical Infrastructure Protection 37 (2022) 100493.
24. Y. Zhao, Y. Ge, Q. Zhu. Combating Ransomware in Internet of Things: A Games-in-Games Approach for Cross-Layer Cyber Defense and Security Investment. In International Conference on Decision and Game Theory for Security, pp. 208-228. Springer, Cham, 2021.
25. S. Armenia, M. Angelini, F. Nonino, G. Palombi, M. F. Schlitzer, A dynamic simulation approach to support the evaluation of cyber risks and security investments in smes, Decision Support Systems (2021) 113580.
26. R. Powell, Defending against terrorist attacks with limited resources, American Political Science Review 101 (2007) 527-541.
27. J. Zhuang, V. M. Bier, Balancing terrorism and natural disasters-defensive strategy with endogenous attacker effort, Operations Research 55 (2007) 976-991.
28. V. M. Bier, Choosing what to protect, Risk Analysis 27 (2007) 607-620.
29. K. Hausken, G. Levitin, Minmax defense strategy for complex multi-state systems, Reliability Engineering & System Safety 94 (2009) 577-587.
30. J. Zhang, J. Zhuang, V. R. R. Jose, The role of risk preferences in a multi-target defender-attacker resource allocation game, Reliability Engineering & System Safety 169 (2018) 95-104.
31. R. Powell, Allocating defensive resources with private information about vulnerability, American Political Science Review 101 (2007) 799-809.
32. J. Zhuang, V. M. Bier, Reasons for secrecy and deception in homeland-security resource allocation, Risk Analysis: An International Journal 30 (2010) 1737-1743.
33. D. Fudenberg, J. Tirole, Game Theory, MIT Press, Cambridge, Massachusetts, 1991.