An attack-defense game on interdependent networks

Rui Peng[a], Di Wu[b*], Mengyao Sun[c], Shaomin Wu[d]
[a]School of Economics & Management, Beijing University of Technology, Beijing, China
[b]School of Management, Xi'an Jiaotong University, Xian, China
[c]Meituan Dianping Inc, Beijing, China
[d]Kent Business School, University of Kent, Canterbury CT2 7FS, United Kingdom

Abstract: This paper analyzes the optimal strategies for an attacker and a defender in an attack-defense game on a network consisting of interdependent subnetworks. The defender moves first and allocates its resource to protect the network nodes. The attacker then moves and allocates its resources to attack the network nodes. The binary decision diagram is employed to obtain all potential states of the network system after attack. Considering each of its opponent's strategies, the game player tries to maximize its own cumulative prospect value. The backward induction method is employed to obtain the game players' optimal strategies, respectively. Different resource relationships are analyzed to testify the robustness of the main conclusions and players' risk attitudes are also investigated. Numerical examples are used to illustrate the analysis.

Keywords: attack-defense game; interdependent network; nodes; binary decision diagram; prospect value

1. Introduction

Reliability analysis of complex networks has gained popularity in the literature, which is especially the case in recent years. Existing research has analyzed the reliability of networks of different structures (Albert et al. 2000, Archibald et al. 2010, Levitin & Hausken, 2009, Chopra & Khanna, 2015). Most authors, however, restrict their assumptions to a single network such as an electrical network or a computer network. In practice, node failures in different networks may be interdependent. For example, Buldyrev et al. (2010) investigated the blackouts of a power gird, occurred in

* Corresponding Author: Di Wu. Email Address: wd_0824@stu.xjtu.edu.cn.
Suggested citation: Peng, R., Wu, D., Sun, M., Wu, S., An attack-defense game on interdependent networks, Journal of the Operational Research Society, DOI: 10.1080/01605682.2020.1784048

Italy on 28 September 2003, which is composed of an electrical subnetwork and an Internet subnetwork. These two subnetworks function interdependently since the Internet subnetwork serves as communication nodes to control the actions of the electrical subnetwork and the electrical subnetwork supplies power to the Internet subnetwork. Some researches investigate maintenance policies of interdependent subnetworks, considering the unintentional impact such as natural aging (Mo et al. 2015). Little research, however, has analyzed risk analysis of intelligent adversaries on interdependent networks, which motivates the research of this paper.

This paper analyzes the attack-defense game with one attacker and one defender, where the defender defends the nodes in a network consisting of interdependent subnetworks and the attacker attacks these nodes, both players needing to allocate their resources. It represents the states of the network with the binary decision diagram (BDD) and assumes the survivability of each node depends on the protection/attack resources allocated by the players. The cumulative prospect theory (CPT), a model for descriptive decisions under risk and uncertainty (Tversky & Kehneman, 1992), is employed to obtain the players' cumulative prospect value (CPV).

Our work is relevant to three streams of literature: the attack-defense game, interdependent networks, and reliability modelling. The attack-defense game typically involves a strategic attacker who aims to destroy the defender's targets. Levitin & Hausken (2010) analyzed the defense and attack strategies of systems considering different system structure detection probabilities by the attacker. Hausken & Bier (2011) studied the defending issue against multiple different attackers, which was further studied by Zhang & Ramirez-Marquez (2013), who consider incomplete information. Bier & Hausken (2013) conducted an attack-defense analysis to study intentional attacker's impact on transportation systems. Zhai et al. (2016) studied the defense and attack strategies for a system with a common bus performance-sharing mechanism. Wu et al. (2018) considered an attack-defense game where the defender allocates its resource to preventive strike and false targets. Peng et al. (2018) considered both intentional and unintentional impact on a typical attack-defense game. Li et al. (2018) analyzed the attack-defense game from a network science perspective.

Research on the attack-defense game in a complex interdependent system is scarce. Hausken (2017a) proposed a framework to numerically analyze the strategic defense of a complex and dependent system with one strategic attacker. They assume that the defender minimizes the expected damage and costs while the attacker maximizes the difference between the cost due to the expected damage and the attack costs. Hausken (2017b) considered a similar problem of attack and defense strategies on two interdependent targets. Hausken (2019) theoretically showed the optimal defense and attack strategies, and discussed the impact of contest intensity, unit effort costs, and target values. Nonetheless, in reality, the game players' strategies may depend not only on their expected losses but also on their risk attitudes. The present paper employs the players' CPVs as their respective objective functions such that their risk preferences are considered.

As for the interdependent network, Kunreuther & Heal (2003) constructed a framework of interdependent security. Later on, Hausken (2006) considered the security investment problem and substitution effects. Zhuang et al. (2007) further constructed a subsidy problem with discount rates in interdependent security. Nganje et al. (2008) extended the interdependent security model through a case-study on a real-world example of a milk supply chain. Hardy et al. (2007) and Xing (2007) studied the reliability of networks with multiple terminals using the BDD technique. Zio & Sansavini (2011) modeled interdependent network systems to identify cascade-safe operating margins. Li & Sansavini (2013) investigated the multi-objective optimization of cascading failure protection in complex networks. Johansson & Hassel (2010) proposed an approach to modelling interdependent infrastructures in the context of vulnerability analysis. Wu et al. (2016) modeled cascading failures in interdependent infrastructures under terrorist attacks. Mackenzie et al. (2016) analyzed the static and dynamic resource allocation models for recovery of interdependent systems with a case study on the Deepwater Horizon oil spill to illustrate it. Peng (2018) studied the reliability of a network consisting of interdependent subnetworks, with the focus on the internal failure of the nodes, rather than on the impacts from the strategic attackers.

Traditionally, the Tullock model is widely employed in the reliability modelling in the attack-defense game and has been adapted to different scenarios by many researchers (see Tullock, 2001; Hausken & Zhuang, 2011, for example). Nonetheless, the Tullock model cannot properly depict players' risk attitudes in the game. To fill in this gap, Liu et al. (2014) proposed a risk-decision analysis method based on the cumulative prospect theory to predict defender's emergency response confronting with unintentional impact, say that, natural disasters.

This paper uses the BDD to represent the different combinations of destructed nodes, where each node has binary states being "destructed" and "not destructed". The state of a system is assumed to depend on not only the system structure but also the players' strategies and their risk attitudes.

The novelty and main contributions of this paper are summarized in the following:

- The novelty is: We utilize cumulative prospect theory to investigate the attack-defense strategy of a network composed of interdependent subnetworks.
- The main contributions include: (1) Different resource relationships and different cost relationships are considered, respectively, in seeking the optimal attack and defense strategies, and (2) Cumulative prospect theory is combined with the traditional Tullock model to obtain the players' CPVs, which can better depict the players' risk preferences and reflect their risk attitudes than merely considering their expected system losses.

The remainder of this paper is organized as follows. Section 2 describes the model setup. Sections 3 analyzes the optimal attack strategies for the attacker. Section 4 employs the backward induction method to solve the optimal defense strategies for the defender. Section 5 analyzes the impact of risk preferences. Section 6 discusses the case for complex system with amounts of nodes. Section 7 concludes the paper and proposes future research suggestions.

2. Model Foundation

Consider a network composed of a power subnetwork and a control subnetwork. The nodes in the control subnetwork require power supply from the power subnetwork whilst the nodes in the power subnetwork are controlled by the nodes in the control subnetwork. Suppose that an intelligent adversary, or the attacker, intends to attack the nodes in the network and the owner of the network is regarded the defender who protects the network from damage. Both players need resources for their actions.

Assume that the defender allocates an amount, r, of its limited resource to protecting the nodes in the network and the attacker spends an amount, R, of its limited resource on attacking the nodes. Due to the interdependence, the failure of a node in one subnetwork may cause some nodes in other subnetwork to fail. Once a node fails, no matter whether the destruction is due to the attacker or the failure propagation from other nodes, the node and its connections with other nodes will be removed from the network it belongs to. After the removal, if the number of the connected nodes in a cluster in a subnetwork is smaller than a pre-specified number, the cluster will fail. In particular, we consider the case where a node fails if it stands alone from any other nodes within a subnetwork, that is, any single node cannot survive but any cluster with no smaller than 2 nodes can survive. Since the failure of a node in one subnetwork may cause several nodes in the other subnetwork to fail, more nodes in the first subnetwork may fail. Such cascading failures may have a catastrophic effect on the network.

Notations

R, r	Resource for the attacker and the defender, respectively
$A_j, B_j, j \in [1,6]$	Nodes of the two subnetworks of the network, respectively
$r_{ij}, R_{ij}, i \in \{A, B\}, j \in [1,6]$	Resource allocation on different nodes, respectively
c, C	Unit cost for protection and attack effort, respectively
m_{ij}	Contest intensity parameters
p_{ij}	Survivability of each node of the network, respectively
u_{dk}, u_{ak}	Utility for the defender and the attacker, respectively
p_k	Probability of the different outcomes, respectively
V_a, V_d	CPVs of the attacker and the defender, respectively

$v(u_{lk})$	Value of the potential outcome
π_k^+, π_k^-	Decision weight for the value of the potential gain and loss, respectively
g, l, λ	Risk parameters
w^+, w^-	Weighting functions for gains and losses, respectively
χ, δ	Weighting function parameters

Consider an illustrative network that has been analyzed by several researchers (Buldyrev et al. 2010; Peng 2018), as shown in Figure 1 (a). There are two interdependent subnetworks *A* and *B*, each of which consists of six nodes, denoted by $A_j, j \in \{1,2,3,4,5,6\}$ and $B_j, j \in \{1,2,3,4,5,6\}$, respectively, and the connections of these nodes are shown with arcs. Besides, the failure of A_j always causes B_j to fail, and vice versa. Suppose that subnetwork *A* is the power subnetwork in which each electricity station A_j is controlled by B_j, which is powered by A_j. Therefore, either the failure of A_j or that of B_j causes the other one to fail.

Suppose that A_5 fails, then B_5, which is connected with A_5, will fail. The failures of A_5 and B_5 will then cause their connections with other nodes to be removed. After the removals, the network will become the one shown in Figure 1 (b), where both A_4 and A_6 then become isolated. Thus, A_4 and A_6 will fail and then cause B_4 and B_6 to fail as well. B_3 is then isolated and thus causes A_3 to fail. Finally, the network will degenerate to the one shown in Figure 1 (c).

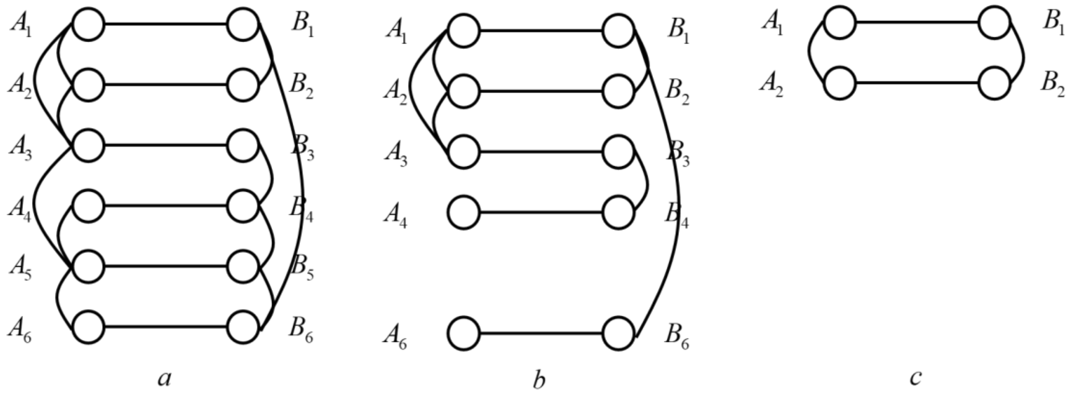

Figure 1 An Illustrative Network Consisting of Interdependent Networks

As for the defender, as assumed, it spends the amount, r, of its resources on protecting the twelve nodes. We further denote that the defender will spend the amount, r_{ij} of its resources on protecting each node in the network and the attack will spend the amount, R_{ij}, of its resources on attacking each node, where $i \in \{A, B\}$, $j \in \{1,2,3,4,5,6\}$, $\sum_{j=1}^{6}(r_{Aj} + r_{Bj}) = r$, and $\sum_{j=1}^{6}(R_{Aj} + R_{Bj}) = R$.

Employing the traditional Tullock model, we can obtain the survivability of each node of the subnetworks

$$p_{ij} = \frac{(r_{ij}/c)^{m_{ij}}}{(r_{ij}/c)^{m_{ij}} + (R_{ij}/C)^{m_{ij}}}, i \in \{A, B\}, j \in \{1,2,3,4,5,6\}. \quad (1)$$

Among, (r_{ij}/c) represents the contest effort (resource spent on the node divided by the unit cost) that the defender takes by spending the resource on defending the ij-th node, and (R_{ij}/C) denotes the contest effort of the attacker on the ij-th node. Additionally, m_{ij} is the contest intensity on the ij-th node where low intensity occurs if neither players get a significant advantage and vice versa.

To formulate the utility of both players, we should note that each node in the subnetworks can either be destroyed or survive, which ultimately forms many different cases for the final state of the network. The probability for each case can be calculated and the CPVs for both players can be obtained for all the cases, for which we employ the BDD. Typically, a BDD is a directed acyclic graph in which all paths start at the root vertex and terminate in one of two states, either representing a system failure or a system success. A BDD is composed of terminal and non-terminal vertices, which are connected by branches, where the non-terminal vertices correspond to all the potential events of the fault tree (Bartlett & Andrews, 2001; Peng et al. 2016).

Take the network in Figure 1 for illustration, the BDD is as constructed as in Figure 2. Note that the left branch of each BDD node represents that both network nodes in the BDD node are undestroyed by the attacker and the right branch represents that at least one network node in the BDD node is destroyed by the attacker. The terminal BDD constructed for each branch contains all failed network nodes no matter whether the nodes are destroyed by attackers or fail due to their own failure propagation.

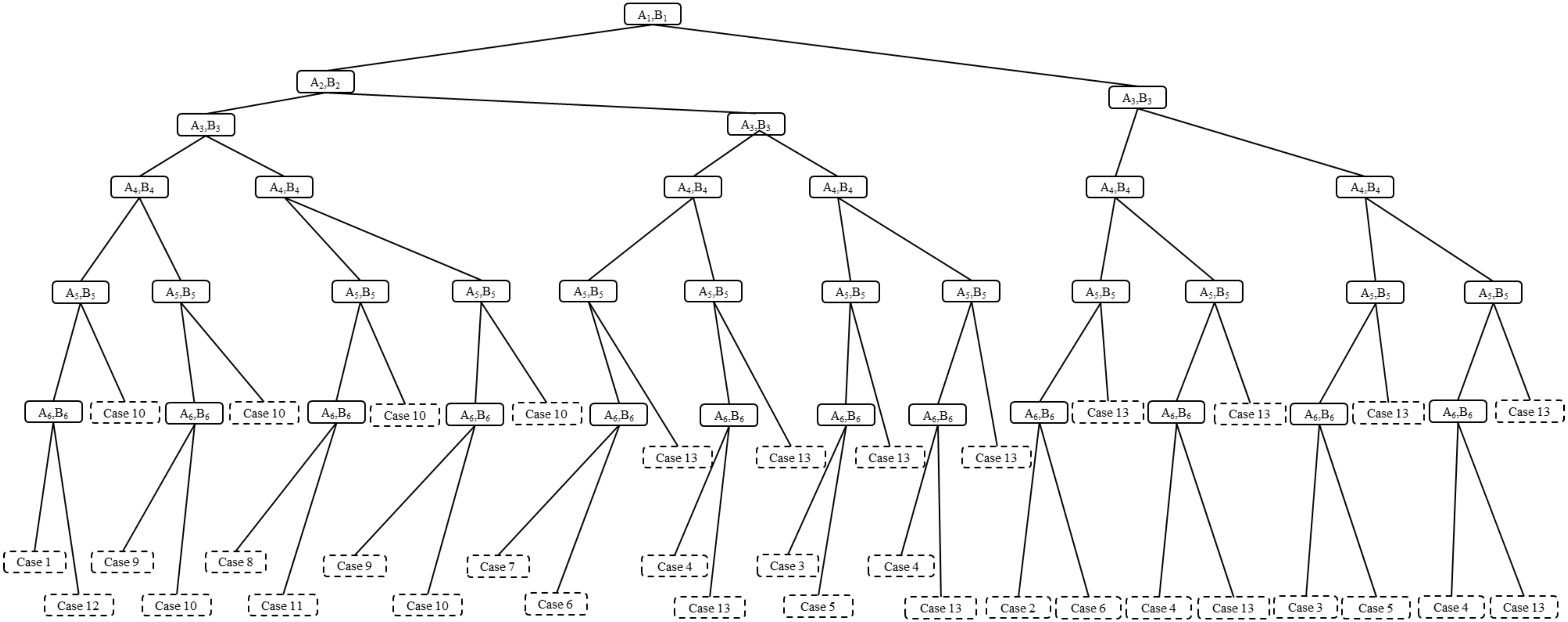

Figure 2. The Binary Decision Diagram for Figure 1

Starting from the nodes $\{A_1, B_1\}$, and then iteratively considering $\{A_2, B_2\}$, …, $\{A_6, B_6\}$, we represent all the possible final states of the network. Take the first two layers as an example. The binary decision diagram starts from the first concerned nodes $\{A_1, B_1\}$. On the left branch, both nodes survive and then we should consider the possible cases for $\{A_2, B_2\}$. However, on the right branch, since at least one of the nodes in $\{A_1, B_1\}$ fails, leading to the failure of $\{A_2, B_2\}$, then we should not add the BDD node $\{A_2, B_2\}$ but consider $\{A_3, B_3\}$ as the next possible nodes to fail after the failure of A_1, B_1, A_2, B_2. Continuing in this way until all the nodes are considered, Figure 2 can be obtained. It can be seen that there are thirteen different possible final states for the network. We specifically illustrate the thirteen cases and their corresponding failed nodes as below.

- Case 1: No failure.
- Case 2: A_1 or B_1 fails, leading to the failure of A_1, A_2, B_1, and B_2, then no other node fails.
- Case 3: A_1 or B_1 fails and A_3 or B_3 fails, leading to the failure of A_1, A_2, A_3, B_1, B_2, and B_3, then no other node fails.
- Case 4: A_1 or B_1 fails, A_3 or B_3 fails, and A_4 or B_4 fails, leading to the failure of A_1, A_2, A_3, A_4, B_1, B_2, B_3, and B_4, then no other node fails.
- Case 5: A_1 or B_1 fails, A_3 or B_3 fails, and A_6 or B_6 fails, leading to the failure of A_1, A_2, A_3, A_6, B_1, B_2, B_3, and B_6, then no other node fails.
- Case 6: A_1 or B_1 fails and A_6 or B_6 fails, leading to the failure of A_1, A_2, A_6, B_1, B_2, and B_6, then no other node fails.
- Case 7: A_2 or B_2 fails, leading to the failure of A_2 and B_2, then no other node fails.
- Case 8: A_3 or B_3 fails, leading to the failure of A_3 and B_3, then no other node fails.
- Case 9: A_3 or B_3 fails and A_4 or B_4 fails, leading to the failure of A_3, A_4, B_3, and B_4, then no other node fails.
- Case 10: A_3 or B_3 fails, A_4 or B_4 fails, A_5 or B_5, and A_6 or B_6 fails, leading to the failure of A_3, A_4, A_5, A_6, B_3, B_4, B_5, and B_6, then no other node fails.
- Case 11: A_3 or B_3 fails and A_6 or B_6 fails, leading to the failure of A_3, A_6, B_3, and B_6, then no other node fails.

- Case 12: A_6 or B_6 fails, leading to the failure of A_6 and B_6, then no other node fails.
- Case 13: Network destruction. More than four nodes in each network are destroyed.

For each case, we denote $u_{dk}, k \in \{1,2,...,12,13\}$ and $u_{ak}, k \in \{1,2,...,12,13\}$ as the utility of the defender and the attacker and $p_k, k \in \{1,2,...,12,13\}$ as the probability of the occurrence of each case, respectively. The destruction of each pair of nodes in the networks is assumed to deal 5 units of utility damage to the defender. The survival of each pair of nodes is assumed to cause 10 units of utility bonus while the network is still operating since the defender cares more about the safety of the network. Similarly, each pair destruction will let the attacker gain 10 units of utility and the survival of each pair will deal 5 units of utility when the network is not under destruction. Specifically, if the network is destroyed by the attacker, the attacker will obtain 60 units of utility and the defender will obtain -30 units of utility. We perform the value under each case in Table 1.

Table 1 Players' utility under Different Cases

Number of failed pairs of nodes	u_{dk}	u_{ak}	Case
0	60	-30	1
1	45	-15	7,8,12
2	30	0	2,9,11
3	15	15	3,6
4	0	30	4,5,10
(5)6	-30	60	13

The probability of each outcome can be calculated through basic permutation and combination and we directly perform the results here.

$$p_1 = \prod_{j=1}^{6} p_{Aj} p_{Bj}, \tag{2}$$

$$p_2 = (1 - p_{A1} p_{B1}) \prod_{j=2}^{6} p_{Aj} p_{Bj}, \tag{3}$$

$$p_3 = (1 - p_{A1} p_{B1})(1 - p_{A3} p_{B3}) p_{A2} p_{B2} \prod_{j=4}^{6} p_{Aj} p_{Bj}, \tag{4}$$

$$p_4 = (1 - p_{A1}p_{B1})(1 - p_{A3}p_{B3})(1 - p_{A4}p_{B4})p_{A2}p_{B2}\prod_{j=5}^{6} p_{Aj}p_{Bj}, \tag{5}$$

$$p_5 = (1 - p_{A1}p_{B1})(1 - p_{A3}p_{B3})(1 - p_{A6}p_{B6})p_{A2}p_{B2}\prod_{j=4}^{5} p_{Aj}p_{Bj}, \tag{6}$$

$$p_6 = (1 - p_{A1}p_{B1})(1 - p_{A6}p_{B6})\prod_{j=2}^{5} p_{Aj}p_{Bj}, \tag{7}$$

$$p_7 = (1 - p_{A2}p_{B2})p_{A1}p_{B1}\prod_{j=3}^{6} p_{Aj}p_{Bj}, \tag{8}$$

$$p_8 = (1 - p_{A3}p_{B3})\prod_{j=1}^{2} p_{Aj}p_{Bj}\prod_{j=4}^{6} p_{Aj}p_{Bj}, \tag{9}$$

$$p_9 = (1 - p_{A3}p_{B3})(1 - p_{A4}p_{B4})\prod_{j=1}^{2} p_{Aj}p_{Bj}\prod_{j=5}^{6} p_{Aj}p_{Bj}, \tag{10}$$

$$p_{10} = \prod_{j=3}^{6}(1 - p_{Aj}p_{Bj})\prod_{j=1}^{2} p_{Aj}p_{Bj}, \tag{11}$$

$$p_{11} = (1 - p_{A3}p_{B3})(1 - p_{A6}p_{B6})\prod_{j=1}^{2} p_{Aj}p_{Bj}\prod_{j=4}^{5} p_{Aj}p_{Bj}, \tag{12}$$

$$p_{12} = (1 - p_{A6}p_{B6})\prod_{j=1}^{5} p_{Aj}p_{Bj}, \tag{13}$$

and

$$p_{13} = 1 - \sum_{i=1}^{12} p_i. \tag{14}$$

To obtain the players' CPV, we introduce the concept of weighting functions w^+ and w^- for gains and losses as below.

$$w^+(p) = \frac{p^\chi}{[p^\chi + (1-p)^\chi]^{1/\chi}}, \tag{15}$$

and

$$w^-(p) = \frac{p^\delta}{[p^\delta + (1-p)^\delta]^{1/\delta}}. \tag{16}$$

where both χ and δ are weighting parameters, which are usually determined through the experiments. The decision weights can therefore be represented by

$$\pi_k^+ = w^+(\sum_{j=k}^{n} p_j) - w^+(\sum_{j=k+1}^{n} p_j), \tag{17}$$

and

$$\pi_k^- = w^-(\sum_{j=1}^{k} p_j) - w^-(\sum_{j=1}^{k-1} p_j), \tag{18}$$

respectively.

The value of the potential outcome can be denoted by

$$v(u_{lk}) = \begin{cases} u_{lk}{}^{g} & u_{ik} > 0, \\ -\lambda(-u_{lk})^{l} & otherwise, \end{cases}, l \in \{d, a\}. \tag{19}$$

where both g and l are the exponent parameters (risk-seeking and risk-averse) and λ is the sensitivity parameter, which measures the sensitivity to losses than gains. Therefore, the CPV is given by

$$V_d = \sum_{k=1}^{12} v(u_{dk})\pi_k^+ + v(u_{d13})\pi_k^-, \tag{20}$$

and

$$V_a = \sum_{k=2,3,4,5,6,9,10,11,13} v(u_{ak})\pi_k^+ + \sum_{k=1,7,8,12} v(u_{ak})\pi_k^-. \tag{21}$$

respectively.

In this paper, it is assumed that the defender allocates the resource evenly into the network nodes, thus the defender's CPV depends only on the attacker's strategy. On the other hand, the attacker knows the defender's allocation and chooses its resource allocation to maximize its own CPV as represented by Eq. (8). Thus, the attacker has $(R_{ij}^*) = ArgMax(V_a(r_{ij})), i \in \{A, B\}, j \in \{1,2,3,4,5,6\}$. As for the defender, there should be $(r_{ij}^*) = ArgMax(V_d(R_{ij}^*)), i \in \{A, B\}, j \in \{1,2,3,4,5,6\}$.

3. Optimal Attack Strategies

Without loss of generality, we first assume that the resources of both players are the same, $r = R = 12$, for instance, and will relax this assumption in the extension.

Further, in the benchmark, we assume that both the unit cost of protection and the unit cost of attack equal to one, i.e., $c = C = 1$. Moreover, we set the risk parameters as $g = 0.85, l = 0.85, \lambda = 4.10, \chi = 0.60$ and $\delta = 0.70$, and conduct sensitivity analysis to study the influence of risk preferences. First, we calculate the situation where both the attacker and the defender evenly spend their resources on each node and the results go to $V_d = -51$ and $V_a = 24.1$. Later, the backward induction is employed to obtain the optimal attack and defense strategies. For a given defense strategies combination $(r_{Aj}, r_{Bj}) = (r_{A1}, r_{B1}, ..., r_{A6}, r_{B6})$, the attacker will choose the optimal attack strategies combination $(R_{Aj}, R_{Bj}) = (R_{A1}, R_{B1}, ..., R_{A6}, R_{B6})$ to maximize its CPV, say that, $(R_{Aj}{}^*, R_{Bj}{}^*) = \arg\max(V_a(r_{Aj}, r_{Bj}))$.

In this section, we assume that the defender will evenly allocate all its resource into all nodes in the interdependent networks, that is, $r_{ij} = 1$. For simplicity, it is assumed that the resource allocation on each node must be integer. Thus, the optimal attack strategy combination can be obtained, as performed in Table 2. Note that the entries without any number equal to zero by default.

Table 2 The Optimal Attack Strategies when Defender Evenly Distribute the Resource

R^*_{A4}	R^*_{A5}	R^*_{B4}	R^*_{B5}	V_a	V_d
3	3	3	3	32.13	-73.5

In Table 2, variables such as $R^*_{ij}, i \in \{A, B\}, j = 1, 2, 3, 6$ are not assigned any values, and similarly hereinafter. It is interesting to point out that in Table 2, the optimal attack strategies require the attacker to spend all resource into A_4, B_4, A_5, and B_5, respectively. In fact, when the defender evenly distributes the resource into all nodes, the optimal strategies for the attacker is to allocate all resource evenly into four nodes: A_4, B_4 A_5, and B_5 and the corresponding CPV for both players will go to $V_d = -73.5$ and $V_a = 32.13$. Since the failure of A_5 and B_5 will finally lead to the failure of A_3-A_6 and B_3-B_6, the network will be destructed, as shown in Figure 1. Moreover, the failures of A_4 and B_4 will lead to the failure of A_4 and B_4, which divides the original network into two parts with each part combining two interdependent pairs of nodes. Any further node failure will result in the destruction of the network, which makes the whole network more vulnerable than before.

4. Optimal Defense Strategies

For the defender who moves first, the optimal defense strategies go to the case where the CPV of the defender is maximized. Since the attacker can observe the action of the defender, it will always take the strategy that benefits itself most. Thus, the defender should compare the CPVs under all possible combinations of defense strategies and choose the largest one among them. That is, $(r_{Aj}^*, r_{Bj}^*) = \arg\max(V_d(R_{Aj}^*, R_{Bj}^*))$.

Solving the optimal defender strategy needs a two-fold optimization scheme where the optimal attack strategy needs to be solved for any fixed defense strategy, based on which the optimal defense strategy should be solved. It would be time consuming to use enumeration to solve the two-fold optimization, thus we employ an improved algorithm to simplify the calculation of the optimal defense strategy.

Two methods are applied to decrease the complexity of the problem: memory search and spiritually pruning (Polyn et al. 2005; Ng et al. 1998). From the system structure, it can be seen that the CPV of both players remain the same if the defender and the attacker simultaneously swap the resource spent on a node in subnetwork A and the corresponding node in subnetwork B. Therefore, without loss of generality, we assume that the resource the defender spends into the network of A will always be less than or equal to those spent into B, for instance, $r_{Aj} \le r_{Bj}$. Moreover, it is easy to notice that: if the defender spends no resource on one node, the attacker will never spend more than 1 unit of its resource into attacking the node. This is because 1 attack resource is enough to destroy an unprotected node. We can therefore use spiritually pruning to eliminate the irrational cases.

Hence, the optimal defense strategy, the responsive attack strategy and their corresponding CPVs are performed in Table 3.

Table 3 Optimal Strategies under Benchmark

r_{A2}^{*}	r_{A4}^{*}	r_{A5}^{*}	r_{B1}^{*}	r_{B2}^{*}	r_{B3}^{*}	r_{B4}^{*}	r_{B5}^{*}	r_{B6}^{*}	V_d
2	2	2		2		2	2		-68.4
R_{A2}^{*}	R_{A4}^{*}	R_{A5}^{*}	R_{B1}^{*}	R_{B2}^{*}	R_{B3}^{*}	R_{B4}^{*}	R_{B5}^{*}	R_{B6}^{*}	V_a
		4	1		1		5	1	30.15

In Table 3, variables such as $r_{Aj}^{*}, j=1,3,6$ and $R_{Aj}^{*}, j=1,3,6$ are not assigned any values. We now obtain the optimal defense and attack strategies under the benchmark. The defender moves first and allocates 2 units of resource into each node of A_2, B_2, A_4, B_4 and A_5, B_5. The attacker, having observed the defender's action, will now choose to spare 4 units of resource for A_5, 5 units of resource into B_5, and 1 unit of resource into each of the nodes of B_1, B_3, and B_6. The CPV of the defender under this case is higher than the case in Table 2 where the defender evenly distributes the resource and the CPV of the attacker decreases. The results here again prove the significance of the node A_4, B_4 and A_5, B_5.

There are two additional cases that deserve mentioning: the attacker moves first, and both players move simultaneously. For the former scenario, the attacker and the defender in backward induction should be exchanged, as well as their decision variables. The defender first chooses the optimal strategy to maximize its CPV, i.e., $(r_{Aj}{}^{*}, r_{Bj}{}^{*}) = \arg\max(V_d(R_{Aj}, R_{Bj}))$. The attacker then compares all possible outcomes and chooses the dominating strategy, i.e., $(R_{Aj}{}^{*}, R_{Bj}{}^{*}) = \arg\max(V_a(r_{Aj}{}^{*}, r_{Bj}{}^{*}))$. The specific calculating approach is exactly the same as the case where the defender moves first. As for the latter scenario, there will be no need for the application of backward induction. For each player, it independently chooses its strategy through maximizing its CPV. In general, one can obtain the optimal attack and defense strategies through repetitively going through Section 3, introducing the attacker's and the defender's decision variables, respectively. The reader is referred to Hausken et al. (2009) and Hausken (2011) for more details on the simultaneous game.

5. Impact of Risk Preferences

For the sake of distinguishing our proposed CPT model from the traditional Tullock model, we concentrate on the analysis of risk preferences in this section. We also conduct sensitivity analysis on the resource held by the defender and the attacker as well as the unit cost of each player. To facilitate the exposition, the expressions, proofs, and relevant figures are given in the online appendix.

The comparative analysis on resource shows that: if the defender owns more resource than the attacker and evenly distributes it into all nodes, then the optimal attack strategy is to centralize fire, say that, attack the most vulnerable nodes. In contrast, when the attacker owns more resource than the defender, then the optimal strategy for the attacker is to spend all resource into four vulnerable nodes: A_4, B_4 and A_5, B_5. In addition, if the defender evenly distributes resource into all nodes, then the summation of both players' CPV only depends on the risk parameter. Results on the analysis of resource vary from the traditional wisdom proposed in previous literature. The traditional Tullock model, used by many researchers, i.e., Wu et al. (2018), showed that the reliability of the defender, will be severely damaged if the counterpart owns resource advantage. The CPT model, through taking the risk attitude into account, demonstrated the existence of another equilibrium. The advantageous player in our proposed model will allocate the majority of its resource to the most vulnerable nodes within the subnetwork and the passive player will allocate the majority of its resource to defending these nodes, leading to a higher summation of CPV than the benchmark. In other words, when players are risk-sensitive, their strategies will change and the second mover benefits more. The players can therefore assess the risk parameters for the counterpart from the historical data, precisely deduce the action that is going to take, and then respond in a more efficient way.

We continue our analysis through concentrating on two different risk behaviors: risk-seeking or risk-averse. When $0 < g < 1$, the value function exhibits risk aversion over gains and when $0 < l < 1$, the function favors risk seeking over risk losses. In fact, the CPV is influenced by the risk preferences, which makes the changes on the attacker's risk parameters may not only alter the attacker's CPV but also correspondingly change the optimal attack strategies. As the defender should anticipate the optimal attack strategy when choosing its defense strategies, the optimal defense strategies will change accordingly. Therefore, to analyze the influence of risk preferences on the attack-defense game, we now alter the parameters of g, l and λ, respectively, to analyze the behavior of each party under the case where the players become more risk-averse, risk seeking or more sensitive to losses than gains.

In the online Appendix 1, we prove the optimality of optimal attack strategies and the invariance of the summation of CPV of both players. Therefore, we directly show that the optimal attack strategies when the defender evenly allocate the resource are $r_{i4} = 3$ and $r_{i5} = 3$. The CPV of each player are presented in Figure 3 and the summation of CPVs under the alteration of g and l are performed in Figure 4.

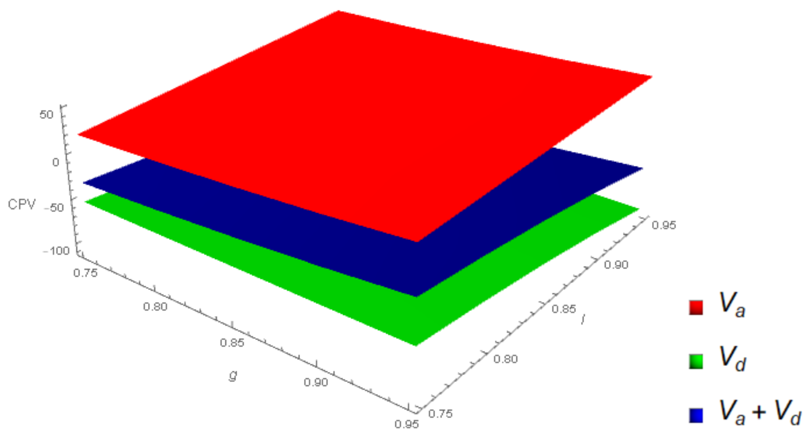

Figure 3 CPVs of Both Players under Different Risk Preferences

Observation 1. The CPV of the attacker depends the majority on g while the CPV of the defender depends the majority on l. When the attacker becomes more risk-averse than its attitude in benchmark, its CPV increases. When the attacker becomes more risk-seeking, its CPV slowly decreases. Additionally, the summation of the CPV decreases with the increase of l and increases with the increase of g.

It is easy to understand the relationship between CPV and the risk parameters from the equations. We can therefore conclude that: when the defender evenly distributes the resource into all nodes, the attacker should choose the most conservative method in order to maximize the CPV. Note that we do not discuss the influence of risk preferences on the CPV of the defender here since we have already fixed the defending strategy. From the blue plane shown in Figure 3, when both players become more risk-averse, then the CPV of defender increases faster than the decrease of the CPV of the attacker. In reality, when the attacker cares more about the risk, then the strategy will become more conservative than before and thus increase the social welfare. Interestingly, we find that the attacker has the incentive to become risk-averse, which may finally increase the social welfare. This is counterintuitive since the reliability model applied in previous literature demonstrates that the attacker's radical strategies will lead to a lose-lose situation. In contrast, for the interdependent network, the design of attacking strategy is more challenging than the normal system without interdependency since the resource should be divided. In effect, a more risk-averse attacker and its conservative strategy increases the summation of CPV.

Now we perform the results under the alteration of λ in Figure 4.

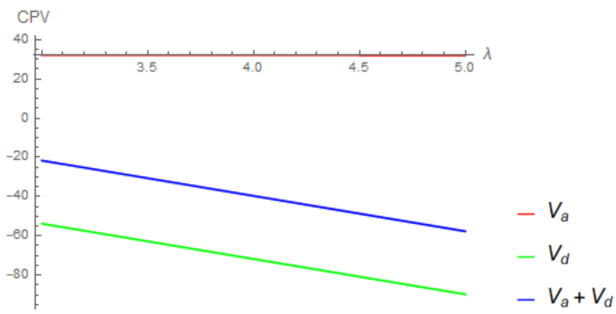

Figure 4 CPVs under the Alteration of λ

Observation 2. If the players become more sensitive to losses than gains, the attacker's CPV will decrease indistinctively. However, the defender's CPV will greatly decrease, thus lower down the summation of CPVs.

Observation 2 is easy to understand based on Eqs. (20) and (21). In reality, if the players care more about its losses, then the strategy will alter to a conservative way, which reaches the same effort as shifting g.

Interestingly, we find the same optimal attack and defense strategy as shown in Table 3 under the alteration of the risk preferences, for instance, no matter whether both players become more risk-averse or risk-seeking, the optimal strategy for both players remain the same. Therefore, we now directly perform the CPV for both players when the defender is dynamic allocating its resource in Figure 5.

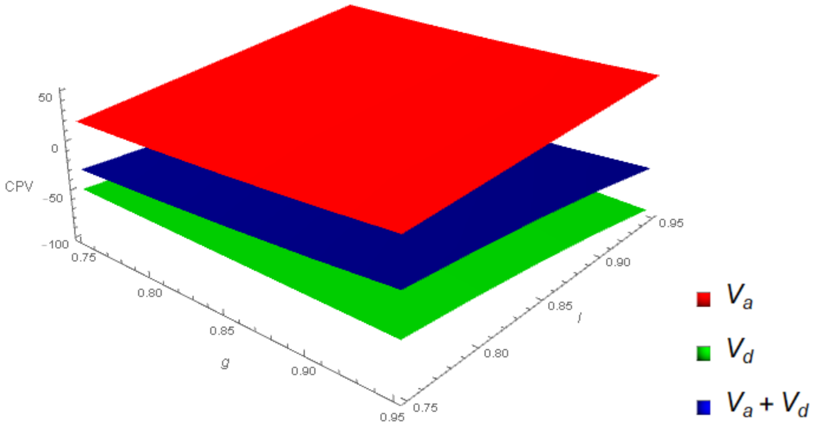

Figure 5 CPVs of Both Players under Different Risk Preferences

Observation 3. The defender's CPV only depends on the risk preference of l and the attacker's CPV only depends on the risk preference of g. Additionally, the summation of the CPV decreases with the increase of l and increases with the increase of g.

Since the attacker will always choose the strategy to maximize its CPV after observing the action of the defender, then for the attacker, cases 1, 7, 8, or 12 will never occur. Therefore, the terms conclude parameter l in the expression of the attacker's CPV will be eliminated, making the CPV only depends on g. Similar, since the strategy of the defender will be countered by the attacker, the network will fall in case 13 with no doubt. Thus, the CPV of the defender will only depend on l.

We continue our analysis by examining the impact of the sensitivity to loss than gains. The results of CPV are shown in Figure 6.

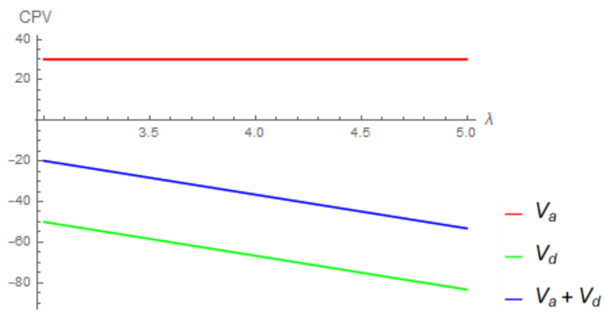

Figure 6 CPVs under the Alteration of λ

Observation 4. If the players become more sensitive to losses than before, the CPV of the attacker will remain the same. However, the CPV of the defender will greatly decrease, thus lower down the summation of CPVs.

Recall that the CPV of the attacker under this case does not depend on l and λ, making the reason behind is similar as the explanation of observation 2. Before ending this section, we summarize the impact of CPT model and how can the new model be applied in providing guidance to the attacker and the defender in interdependent network. Traditional reliability modelling techniques usually assume that all players are entirely reasonable and risk-neutral. However, in reality, some players are engaging risk and endeavoring to take radical strategy to destroy its enemy regardless of cost. On the contrary, some players are afraid of taking risk and will always choose the most conservative strategy to minimize the expected loss. The CPT model, benefits to the literature since it incorporates player's risk attitude into concern. Taking the benchmark as an example. The Tullock model results in a static strategy set for both the attacker and the defender. However, the CPT model provides suggestions in a dynamic strategy set where more risky strategy, i.e., giving up some nodes, or more conservative strategy, i.e., evenly protection, can be employed based on different risk parameter combinations. Both the attacker and the defender, can always try to deduce the risk sensitivity for the other side, and make their decision more wisely and targeted.

6. Discussion

The preceding sections investigate the situation for a network that is composed of a small number of nodes. For complex networks composed of a large number of nodes, one can use simulation to estimate its reliability. In the literature, there are several methods have been proposed.

- Wandelt et al. (2018) proposed a new framework, referred to as quick robustness estimation, for assessing the robustness of a network in sub-quadratic time. Its computational speed is significantly faster than betweenness centrality.
- One can consider the reorganization of data structure. For example, Benson et al. (2016) proposed a method to solve the large-scale complex networks through clustering the network on the basis of higher-order connectivity patterns. A series of meta-heuristic algorithms can also benefit the computational speed (Šenkeřík et al. 2018).

To calculate the robustness of a complex system, one cannot theoretically derive the dominating strategies for all players (see the game theoretical approach in Li et al. (2019)). But it is possible to numerically investigate the optimal strategy based on the design of algorithms and simulation. Additionally, quantum computer and quantum computation are gaining extreme popularity these years. The construction of quantum system accelerates the computational efficiency and benefits all fields, i.e., machine learning and large-scale calculation. With the introduction of quantum computer, even for complex systems with amounts of node, BDD can produce accurate results in an acceptable time duration.

7. Conclusions and Future Works

This paper analyzes the attack-defense game of a network consisting of interdependent subnetworks. The defender moves first and allocates its limited resource to the nodes and the attacker then moves. Both players choose their strategies to maximize their own cumulative prospect values. The binary decision diagram is used to obtain the potential outcomes of the given network. Since the cumulative prospect theory is used, the risk preferences of both players can be depicted and the alterations of the optimal strategy combination are illustrated to find the influence under different cases.

Our future work will consider a possible extension of the case where both players in the attack-defense game own unlimited resource. Then they should only optimize the allocation and some close-formed solution may be obtained. Besides, our future research will incorporate the use of false targets of the defender to increase the survivability of each node in the networks. Additionally, as we mentioned in Section 4, our future work will also incorporate two different scenarios: the attacker moves first, and both players move simultaneously, and compare the result with our proposed model. Finally, one can consider the calculation efficiency optimization. Simulation methods, heuristic algorithms, and data reorganization are all potentially useful in employing BDD to solve a large-scale complex system.

Acknowledgment

The research was supported by the NSFC under grant numbers 71671016 and 71832011.

Reference

Albert, R., Jeong, H., & Barabasi, A. L. 2000. Error and attack tolerance of complex networks. *Nature*, 340(1), 378-382.

Archibald, T. W., Black, D. P., & Glazebrook, K. D. 2010. The use of simple calibrations of individual locations in making transshipment decisions in a multi-location inventory network. *Journal of the Operational Research Society*, 61(2), 294-305.

Bartlett, L. M., & Andrews, J. D. 2001. An ordering heuristic to develop the binary decision diagram based on structural importance. *Reliability Engineering & System Safety*, 72(1), 31-38.

Benson, A. R., Gleich, D. F., & Leskovec, J. 2016. Higher-order organization of complex networks. *Science*, 353(6295), 163-166.

Bier, V. and Hausken, K. 2013. Defending and attacking a network of two arcs subject to traffic congestion, *Reliability Engineering & System Safety*, 112, 214-224.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. 2010. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291), 1025-1028.

Chopra, S. S., & Khanna, V. 2015. Interconnectedness and interdependencies of critical infrastructures in the US economy: Implications for resilience. *Physica A:*

Statistical Mechanics and its Applications, 436, 865-877.

Hardy, G., Lucet, C., & Limnios, N. 2007. K-terminal network reliability measures with binary decision diagrams. *IEEE Transactions on Reliability*, 56(3), 506-515.

Hausken, K. 2006. Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy*, 25(6), 629-665.

Hausken, K. 2011, Strategic Defense and Attack of Series Systems when Agents Move Sequentially, *IIE Transactions*, 43(7), 483-504.

Hausken, K. 2017a. Defense and attack of complex and dependent systems. *Reliability Engineering & System Safety*, 95(1), 29-42.

Hausken, K. 2017b. Defense and Attack for Interdependent Systems. *European Journal of Operational Research*, 256(2), 582-591.

Hausken, K. 2019. Defence and attack of complex interdependent systems. *Journal of the Operational Research Society,* 70(3), 364-376.

Hausken, K., & Bier, V. M. 2011. Defending against multiple different attackers. *European Journal of Operational Research*, 211(2), 370-384.

Hausken, K., Bier, V. and Zhuang, J. 2009, Defending Against Terrorism, Natural Disaster, and All Hazards, in Bier, V.M. and Azaiez, M.N. (eds.), Game Theoretic Risk Analysis of Security Threats, Springer, New York, 65-97.

Hausken, K., & Zhuang, J. 2011. Governments' and terrorists' defense and attack in a t-period game. *Decision Analysis*, 8(1), 46-70.

Johansson, J., & Hassel, H. 2010. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering & System Safety*, 95(12), 1335-1344.

Kunreuther, H., & Heal, G. 2003. Interdependent security. *Journal of risk and uncertainty*, 26(2-3), 231-249.

Levitin, G., & Hausken, K. 2009. Redundancy vs. protection in defending parallel systems against unintentional and intentional impacts. *IEEE Transactions on Reliability*, 58(4), 679-690.

Levitin, G., & Hausken, K. 2010. Defence and attack of systems with variable attacker system structure detection probability. *Journal of the Operational Research Society*, 61(1), 124-133.

Li, Y., Deng, Y., Xiao, Y., & Wu, J. 2019. Attack and Defense Strategies in Complex Networks Based on Game Theory. *Journal of Systems Science and Complexity*, 32(6), 1630-1640.

Li, Y. F., & Sansavini. 2013. Non-dominated sorting binary differential evolution for the multi-objective optimization of cascading failures protection in complex networks. *Reliability Engineering & System Safety*, 111(1), 195-205.

Li, Y. P., Tan, S. Y., Deng, Y., & Wu, J. 2018. Attacker-defender game from a network science perspective. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 28(5), 051102.

Liu, Y., Fan, Z. P., & Zhang, Y. 2014. Risk decision analysis in emergency response: a method based on cumulative prospect theory. *Computers & Operations Research*, 42(2), 75-82.

Mackenzie, C. A., Baroud, H., & Barker, K. 2016. Static and dynamic resource allocation models for recovery of interdependent systems: application to the deepwater horizon, oil spill. *Annals of Operations Research*, 236(1), 103-129.

Mo, H., Xie, M., & Levitin, G. 2015. Optimal resource distribution between protection and redundancy considering the time and uncertainties of attacks. *European Journal of Operational Research*, 243(1), 200-210.

Ng, R. T., Lakshmanan, L. V. S., Han, J., & Pang, A. 1998. Exploratory mining and pruning optimizations of constrained associations rules. ACM Sigmod International Conference on Management of Data (Vol.27, pp.13-24). ACM.

Nganje, W., Bier, V., Han, H., & Zack, L. 2008. Models of interdependent security along the milk supply chain. *American Journal of Agricultural Economics*, 90(5), 1265-1271.

Peng, R., 2018. Reliability of interdependent networks with cascading failures. *Eksploatacja i Niezawodnosc - Maintenance and Reliability*, 20(2), 273-277.

Peng, R., Wu, D., & Zhai, Q. 2018. Defense resource allocation against sequential unintentional and intentional impacts. *IEEE Transactions on Reliability*, 68(1), 364-374.

Peng, R., Zhai, Q. Q., & Levitin, G. 2016. Defending a single object against an attacker trying to detect a subset of false targets. *Reliability Engineering & System Safety*, 149, 137-147.

Polyn, S. M., Natu, V. S., Cohen, J. D., & Norman, K. A. 2005. Category-specific cortical activity precedes retrieval during memory search. *Science*, 310(5756), 1963-1966.

Šenkeřík, R., Zelinka, I., Pluhacek, M., Viktorin, A., Janostik, J., & Oplatkova, Z. K. 2018. Randomization and Complex Networks for Meta-Heuristic Algorithms. In Evolutionary Algorithms, Swarm Dynamics and Complex Networks (pp. 177-194). Springer, Berlin, Heidelberg.

Tversky, A. and Kahneman, D. 1992. Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and uncertainty*, 5(4), pp.297-323.

Tullock G. 2001. Efficient Rent Seeking. Springer, Boston, MA.

Wandelt, S., Sun, X., Zanin, M., & Havlin, S. 2018. QRE: quick robustness estimation for large complex networks. *Future Generation Computer Systems*, 83, 413-424.

Wu, B., Tang, A., & Wu, J. 2016. Modeling cascading failures in interdependent infrastructures under terrorist attacks. *Reliability Engineering & System Safety*, 147, 1-8.

Wu, D., Xiao, H., & Peng, R. 2018. Object defense with preventive strike and false targets. *Reliability Engineering & System Safety*, 169, 76-80.

Xing, L. 2007. An efficient binary-decision-diagram-based approach for network reliability and sensitivity analysis. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 38(1), 105-115.

Zhai, Q., Ye, Z. S., Peng, R., & Wang, W. 2016. Defense and attack of performance-sharing common bus systems. *European Journal of Operational Research*, 256(3), 962-975.

Zhang, C., & Ramirez-Marquez, J.E. 2013. Protecting critical infrastructures against intentional attacks: a two-stage game with incomplete information. *IIE Transactions*, 45(3), 244-258.

Zhuang, J., Bier, V. M., & Gupta, A. 2007. Subsidies in interdependent security with heterogeneous discount rates. *The Engineering Economist*, 52(1), 1-19.

Zio, E., & Sansavini, G. 2011. Modeling interdependent network systems for identifying cascade-safe operating margins. *IEEE Transactions on Reliability*, 60(1), 94-101.