

Kent Academic Repository

Full text document (pdf)

Citation for published version

Peng, Rui and Wu, Di and Sun, Mengyao and Wu, Shaomin (2020) An attack-defense game on interdependent networks. *Journal of Operational Research Society* . ISSN 0160-5682. (In press)

DOI

<https://doi.org/10.1080/01605682.2020.1784048>

Link to record in KAR

<https://kar.kent.ac.uk/81743/>

Document Version

Author's Accepted Manuscript

Copyright & reuse

Content in the Kent Academic Repository is made available for research purposes. Unless otherwise stated all content is protected by copyright and in the absence of an open licence (eg Creative Commons), permissions for further reuse of content should be sought from the publisher, author or other copyright holder.

Versions of research

The version in the Kent Academic Repository may differ from the final published version.

Users are advised to check <http://kar.kent.ac.uk> for the status of the paper. **Users should always cite the published version of record.**

Enquiries

For any further enquiries regarding the licence status of this document, please contact:

researchsupport@kent.ac.uk

If you believe this document infringes copyright then please contact the KAR admin team with the take-down information provided at <http://kar.kent.ac.uk/contact.html>

An attack-defense game on interdependent networks

Rui Peng^a, Di Wu^{b*}, Mengyao Sun^c, Shaomin Wu^d

^aSchool of Economics & Management, Beijing University of Technology, Beijing, China

^bSchool of Management, Xi'an Jiaotong University, Xian, China

^cMeituan Dianping Inc, Beijing, China

^dKent 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 grid, 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

30 Italy on 28 September 2003, which is composed of an electrical subnetwork and an
31 Internet subnetwork. These two subnetworks function interdependently since the
32 Internet subnetwork serves as communication nodes to control the actions of the
33 electrical subnetwork and the electrical subnetwork supplies power to the Internet
34 subnetwork. Some researches investigate maintenance policies of interdependent
35 subnetworks, considering the unintentional impact such as natural aging (Mo et al.
36 2015). Little research, however, has analyzed risk analysis of intelligent adversaries on
37 interdependent networks, which motivates the research of this paper.

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

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

60 Research on the attack-defense game in a complex interdependent system is scarce.
61 Hausken (2017a) proposed a framework to numerically analyze the strategic defense of
62 a complex and dependent system with one strategic attacker. They assume that the
63 defender minimizes the expected damage and costs while the attacker maximizes the
64 difference between the cost due to the expected damage and the attack costs. Hausken
65 (2017b) considered a similar problem of attack and defense strategies on two
66 interdependent targets. Hausken (2019) theoretically showed the optimal defense and
67 attack strategies, and discussed the impact of contest intensity, unit effort costs, and
68 target values. Nonetheless, in reality, the game players' strategies may depend not only
69 on their expected losses but also on their risk attitudes. The present paper employs the
70 players' CPVs as their respective objective functions such that their risk preferences are
71 considered.

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

89 Traditionally, the Tullock model is widely employed in the reliability modelling in

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

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

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

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

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

115

116 **2. Model Foundation**

117 Consider a network composed of a power subnetwork and a control subnetwork.
118 The nodes in the control subnetwork require power supply from the power subnetwork
119 whilst the nodes in the power subnetwork are controlled by the nodes in the control

120 subnetwork. Suppose that an intelligent adversary, or the attacker, intends to attack the
 121 nodes in the network and the owner of the network is regarded the defender who
 122 protects the network from damage. Both players need resources for their actions.

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

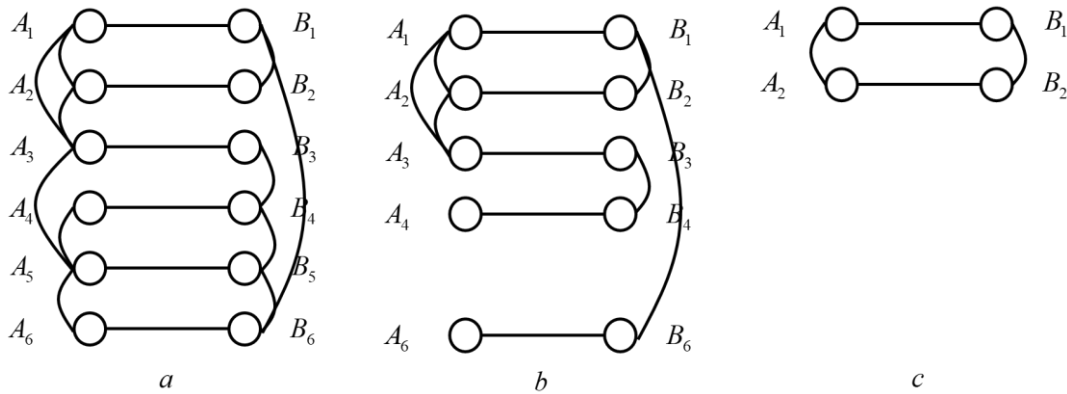
Notations

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

$v(u_{ik})$	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

136 Consider an illustrative network that has been analyzed by several researchers
137 (Buldyrev et al. 2010; Peng 2018), as shown in Figure 1 (a). There are two
138 interdependent subnetworks A and B , each of which consists of six nodes, denoted by
139 $A_j, j \in \{1, 2, 3, 4, 5, 6\}$ and $B_j, j \in \{1, 2, 3, 4, 5, 6\}$, respectively, and the connections of
140 these nodes are shown with arcs. Besides, the failure of A_j always causes B_j to fail,
141 and vice versa. Suppose that subnetwork A is the power subnetwork in which each
142 electricity station A_j is controlled by B_j , which is powered by A_j . Therefore, either
143 the failure of A_j or that of B_j causes the other one to fail.

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



150
151

Figure 1 An Illustrative Network Consisting of Interdependent Networks

152 As for the defender, as assumed, it spends the amount, r , of its resources on
153 protecting the twelve nodes. We further denote that the defender will spend the amount,
154 r_{ij} of its resources on protecting each node in the network and the attack will spend the
155 amount, R_{ij} , of its resources on attacking each node, where $i \in \{A, B\}$, $j \in$
156 $\{1, 2, 3, 4, 5, 6\}$, $\sum_{j=1}^6 (r_{Aj} + r_{Bj}) = r$, and $\sum_{j=1}^6 (R_{Aj} + R_{Bj}) = R$.

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

$$159 \quad p_{ij} = \frac{(r_{ij} / c)^{m_{ij}}}{(r_{ij} / c)^{m_{ij}} + (R_{ij} / C)^{m_{ij}}}, i \in \{A, B\}, j \in \{1, 2, 3, 4, 5, 6\}. \quad (1)$$

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

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

174 Take the network in Figure 1 for illustration, the BDD is as constructed as in Figure
175 2. Note that the left branch of each BDD node represents that both network nodes in the
176 BDD node are undestroyed by the attacker and the right branch represents that at least
177 one network node in the BDD node is destroyed by the attacker. The terminal BDD

178 constructed for each branch contains all failed network nodes no matter whether the
179 nodes are destroyed by attackers or fail due to their own failure propagation.

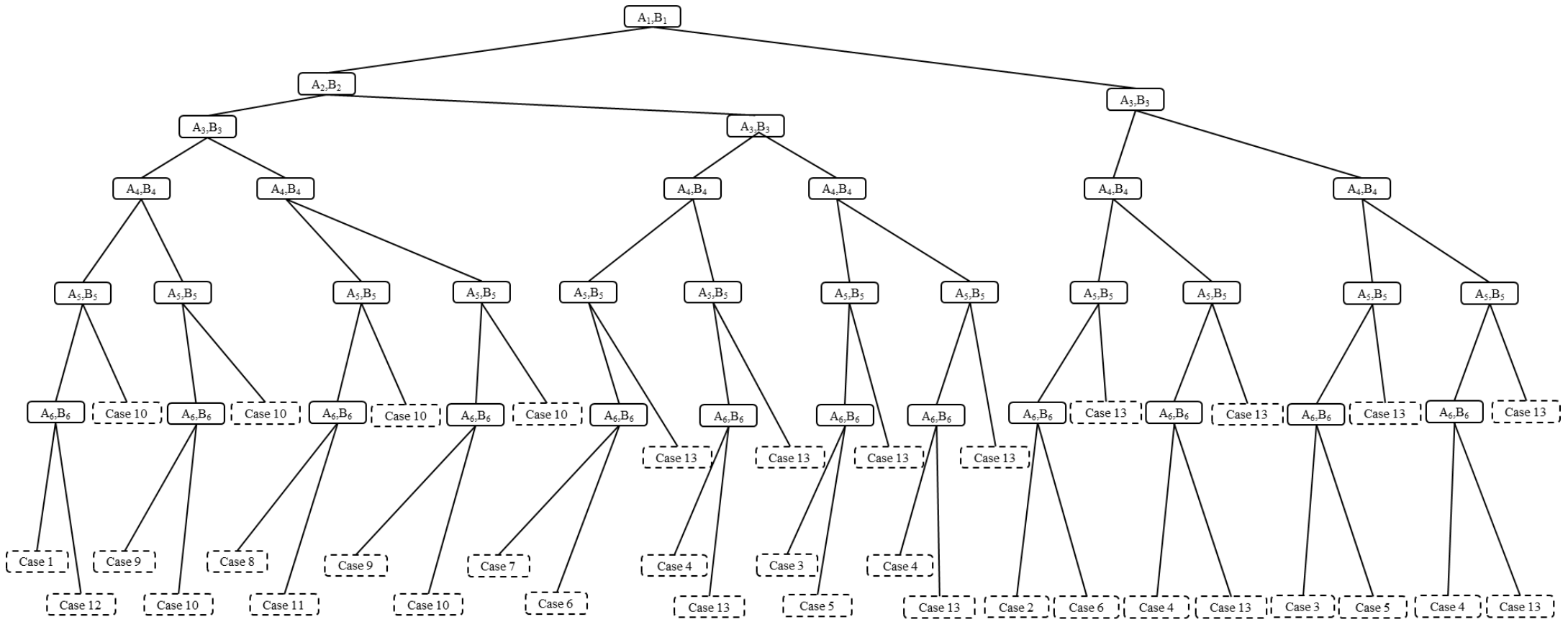


Figure 2. The Binary Decision Diagram for Figure 1

200 Starting from the nodes $\{A_1, B_1\}$, and then iteratively considering $\{A_2, B_2\}, \dots, \{A_6,$
 201 $B_6\}$, we represent all the possible final states of the network. Take the first two layers
 202 as an example. The binary decision diagram starts from the first concerned nodes $\{A_1,$
 203 $B_1\}$. On the left branch, both nodes survive and then we should consider the possible
 204 cases for $\{A_2, B_2\}$. However, on the right branch, since at least one of the nodes in $\{A_1,$
 205 $B_1\}$ fails, leading to the failure of $\{A_2, B_2\}$, then we should not add the BDD node $\{A_2,$
 206 $B_2\}$ but consider $\{A_3, B_3\}$ as the next possible nodes to fail after the failure of $A_1, B_1,$
 207 A_2, B_2 . Continuing in this way until all the nodes are considered, Figure 2 can be
 208 obtained. It can be seen that there are thirteen different possible final states for the
 209 network. We specifically illustrate the thirteen cases and their corresponding failed
 210 nodes as below.

- 211 • Case 1: No failure.
- 212 • 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
 213 fails.
- 214 • Case 3: A_1 or B_1 fails and A_3 or B_3 fails, leading to the failure of $A_1, A_2, A_3, B_1, B_2,$
 215 and B_3 , then no other node fails.
- 216 • 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 $A_1,$
 217 $A_2, A_3, A_4, B_1, B_2, B_3,$ and B_4 , then no other node fails.
- 218 • 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 $A_1,$
 219 $A_2, A_3, A_6, B_1, B_2, B_3,$ and B_6 , then no other node fails.
- 220 • Case 6: A_1 or B_1 fails and A_6 or B_6 fails, leading to the failure of $A_1, A_2, A_6, B_1, B_2,$
 221 and B_6 , then no other node fails.
- 222 • Case 7: A_2 or B_2 fails, leading to the failure of A_2 and B_2 , then no other node fails.
- 223 • Case 8: A_3 or B_3 fails, leading to the failure of A_3 and B_3 , then no other node fails.
- 224 • 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 $B_4,$
 225 then no other node fails.
- 226 • 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
 227 failure of $A_3, A_4, A_5, A_6, B_3, B_4, B_5,$ and B_6 , then no other node fails.
- 228 • 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 $B_6,$
 229 then no other node fails.

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

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

243 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

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

$$246 \quad p_1 = \prod_{j=1}^6 P_{A_j} P_{B_j}, \quad (2)$$

$$247 \quad p_2 = (1 - P_{A_1} P_{B_1}) \prod_{j=2}^6 P_{A_j} P_{B_j}, \quad (3)$$

$$248 \quad p_3 = (1 - P_{A_1} P_{B_1})(1 - P_{A_3} P_{B_3}) P_{A_2} P_{B_2} \prod_{j=4}^6 P_{A_j} P_{B_j}, \quad (4)$$

249
$$p_4 = (1 - p_{A1}p_{B1})(1 - p_{A3}p_{B3})(1 - p_{A4}p_{B4})p_{A2}p_{B2} \prod_{j=5}^6 p_{Aj}p_{Bj}, \quad (5)$$

250
$$p_5 = (1 - p_{A1}p_{B1})(1 - p_{A3}p_{B3})(1 - p_{A6}p_{B6})p_{A2}p_{B2} \prod_{j=4}^5 p_{Aj}p_{Bj}, \quad (6)$$

251
$$p_6 = (1 - p_{A1}p_{B1})(1 - p_{A6}p_{B6}) \prod_{j=2}^5 p_{Aj}p_{Bj}, \quad (7)$$

252
$$p_7 = (1 - p_{A2}p_{B2})p_{A1}p_{B1} \prod_{j=3}^6 p_{Aj}p_{Bj}, \quad (8)$$

253
$$p_8 = (1 - p_{A3}p_{B3}) \prod_{j=1}^2 p_{Aj}p_{Bj} \prod_{j=4}^6 p_{Aj}p_{Bj}, \quad (9)$$

254
$$p_9 = (1 - p_{A3}p_{B3})(1 - p_{A4}p_{B4}) \prod_{j=1}^2 p_{Aj}p_{Bj} \prod_{j=5}^6 p_{Aj}p_{Bj}, \quad (10)$$

255
$$p_{10} = \prod_{j=3}^6 (1 - p_{Aj}p_{Bj}) \prod_{j=1}^2 p_{Aj}p_{Bj}, \quad (11)$$

256
$$p_{11} = (1 - p_{A3}p_{B3})(1 - p_{A6}p_{B6}) \prod_{j=1}^2 p_{Aj}p_{Bj} \prod_{j=4}^5 p_{Aj}p_{Bj}, \quad (12)$$

257
$$p_{12} = (1 - p_{A6}p_{B6}) \prod_{j=1}^5 p_{Aj}p_{Bj}, \quad (13)$$

258 and

259
$$p_{13} = 1 - \sum_{i=1}^{12} p_i. \quad (14)$$

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

262
$$w^+(p) = \frac{p^\chi}{[p^\chi + (1-p)^\chi]^{1/\chi}}, \quad (15)$$

263 and

264
$$w^-(p) = \frac{p^\delta}{[p^\delta + (1-p)^\delta]^{1/\delta}}. \quad (16)$$

265 where both χ and δ are weighting parameters, which are usually determined

266 through the experiments. The decision weights can therefore be represented by

$$267 \quad \pi_k^+ = w^+ \left(\sum_{j=k}^n p_j \right) - w^+ \left(\sum_{j=k+1}^n p_j \right), \quad (17)$$

268 and

$$269 \quad \pi_k^- = w^- \left(\sum_{j=1}^k p_j \right) - w^- \left(\sum_{j=1}^{k-1} p_j \right), \quad (18)$$

270 respectively.

271 The value of the potential outcome can be denoted by

$$272 \quad v(u_{lk}) = \begin{cases} u_{lk}^g & u_{lk} > 0, \\ -\lambda(-u_{lk})^l & \text{otherwise,} \end{cases}, l \in \{d, a\}. \quad (19)$$

273 where both g and l are the exponent parameters (risk-seeking and risk-averse) and

274 λ is the sensitivity parameter, which measures the sensitivity to losses than gains.

275 Therefore, the CPV is given by

$$276 \quad V_d = \sum_{k=1}^{12} v(u_{dk}) \pi_k^+ + v(u_{d13}) \pi_k^-, \quad (20)$$

277 and

$$278 \quad V_a = \sum_{k=2,3,4,5,6,9,10,11,13} v(u_{ak}) \pi_k^+ + \sum_{k=1,7,8,12} v(u_{ak}) \pi_k^-. \quad (21)$$

279 respectively.

280 In this paper, it is assumed that the defender allocates the resource evenly into the

281 network nodes, thus the defender's CPV depends only on the attacker's strategy. On the

282 other hand, the attacker knows the defender's allocation and chooses its resource

283 allocation to maximize its own CPV as represented by Eq. (8). Thus, the attacker has

284 $(R_{ij}^*) = \text{ArgMax}(V_a(r_{ij})), i \in \{A, B\}, j \in \{1, 2, 3, 4, 5, 6\}$. As for the defender, there should

285 be $(r_{ij}^*) = \text{ArgMax}(V_d(R_{ij}^*)), i \in \{A, B\}, j \in \{1, 2, 3, 4, 5, 6\}$.

286

287 3. Optimal Attack Strategies

288 Without loss of generality, we first assume that the resources of both players are

289 the same, $r = R = 12$, for instance, and will relax this assumption in the extension.

290 Further, in the benchmark, we assume that both the unit cost of protection and the unit
 291 cost of attack equal to one, i.e., $c = C = 1$. Moreover, we set the risk parameters as
 292 $g = 0.85, l = 0.85, \lambda = 4.10, \chi = 0.60$ and $\delta = 0.70$, and conduct sensitivity analysis to
 293 study the influence of risk preferences. First, we calculate the situation where both the
 294 attacker and the defender evenly spend their resources on each node and the results go
 295 to $V_d = -51$ and $V_a = 24.1$. Later, the backward induction is employed to obtain the
 296 optimal attack and defense strategies. For a given defense strategies combination
 297 $(r_{Aj}, r_{Bj}) = (r_{A1}, r_{B1}, \dots, r_{A6}, r_{B6})$, the attacker will choose the optimal attack strategies
 298 combination $(R_{Aj}, R_{Bj}) = (R_{A1}, R_{B1}, \dots, R_{A6}, R_{B6})$ to maximize its CPV, say that,
 299 $(R_{Aj}^*, R_{Bj}^*) = \arg \max(V_a(r_{Aj}, r_{Bj}))$.

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

305 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

306 In Table 2, variables such as $R_{ij}^*, i \in \{A, B\}, j = 1, 2, 3, 6$ are not assigned any
 307 values, and similarly hereinafter. It is interesting to point out that in Table 2, the optimal
 308 attack strategies require the attacker to spend all resource into A_4, B_4, A_5 , and B_5 ,
 309 respectively. In fact, when the defender evenly distributes the resource into all nodes,
 310 the optimal strategies for the attacker is to allocate all resource evenly into four nodes:
 311 A_4, B_4, A_5 , and B_5 and the corresponding CPV for both players will go to $V_d = -73.5$
 312 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
 313 and B_3-B_6 , the network will be destructed, as shown in Figure 1. Moreover, the failures

314 of A_4 and B_4 will lead to the failure of A_4 and B_4 , which divides the original network
 315 into two parts with each part combining two interdependent pairs of nodes. Any further
 316 node failure will result in the destruction of the network, which makes the whole
 317 network more vulnerable than before.

318

319 **4. Optimal Defense Strategies**

320 For the defender who moves first, the optimal defense strategies go to the case
 321 where the CPV of the defender is maximized. Since the attacker can observe the action
 322 of the defender, it will always take the strategy that benefits itself most. Thus, the
 323 defender should compare the CPVs under all possible combinations of defense
 324 strategies and choose the largest one among them. That is,
 325 $(r_{A_j}^*, r_{B_j}^*) = \arg \max(V_d(R_{A_j}^*, R_{B_j}^*)).$

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

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

342 Hence, the optimal defense strategy, the responsive attack strategy and their

343 corresponding CPVs are performed in Table 3.

344 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

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

354 There are two additional cases that deserve mentioning: the attacker moves first,
355 and both players move simultaneously. For the former scenario, the attacker and the
356 defender in backward induction should be exchanged, as well as their decision variables.
357 The defender first chooses the optimal strategy to maximize its CPV, i.e.,
358 $(r_{A_j}^*, r_{B_j}^*) = \arg \max(V_d(R_{A_j}, R_{B_j}))$. The attacker then compares all possible outcomes and
359 chooses the dominating strategy, i.e., $(R_{A_j}^*, R_{B_j}^*) = \arg \max(V_a(r_{A_j}^*, r_{B_j}^*))$. The specific
360 calculating approach is exactly the same as the case where the defender moves first. As
361 for the latter scenario, there will be no need for the application of backward induction.
362 For each player, it independently chooses its strategy through maximizing its CPV. In
363 general, one can obtain the optimal attack and defense strategies through repetitively
364 going through Section 3, introducing the attacker's and the defender's decision
365 variables, respectively. The reader is referred to Hausken et al. (2009) and Hausken
366 (2011) for more details on the simultaneous game.

367

368 **5. Impact of Risk Preferences**

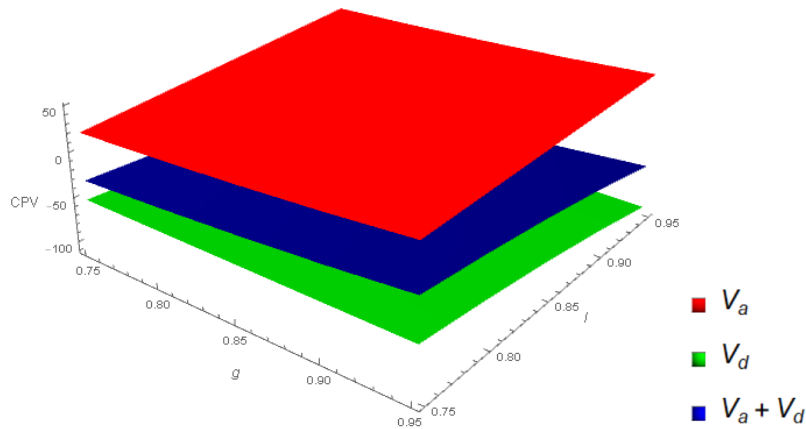
369 For the sake of distinguishing our proposed CPT model from the traditional
370 Tullock model, we concentrate on the analysis of risk preferences in this section. We
371 also conduct sensitivity analysis on the resource held by the defender and the attacker
372 as well as the unit cost of each player.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

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

393 We continue our analysis through concentrating on two different risk behaviors:
394 risk-seeking or risk-averse. When $0 < g < 1$, the value function exhibits risk aversion
395 over gains and when $0 < l < 1$, the function favors risk seeking over risk losses. In fact,

396 the CPV is influenced by the risk preferences, which makes the changes on the
 397 attacker's risk parameters may not only alter the attacker's CPV but also
 398 correspondingly change the optimal attack strategies. As the defender should anticipate
 399 the optimal attack strategy when choosing its defense strategies, the optimal defense
 400 strategies will change accordingly. Therefore, to analyze the influence of risk
 401 preferences on the attack-defense game, we now alter the parameters of g, l and λ ,
 402 respectively, to analyze the behavior of each party under the case where the players
 403 become more risk-averse, risk seeking or more sensitive to losses than gains.

404 In the online Appendix 1, we prove the optimality of optimal attack strategies and
 405 the invariance of the summation of CPV of both players. Therefore, we directly show
 406 that the optimal attack strategies when the defender evenly allocate the resource are
 407 $r_{i4} = 3$ and $r_{i5} = 3$. The CPV of each player are presented in Figure 3 and the
 408 summation of CPVs under the alteration of g and l are performed in Figure 4.



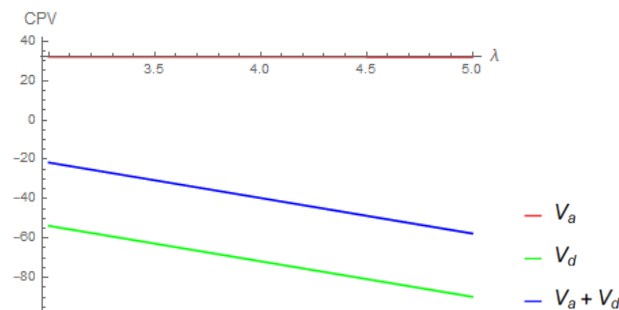
409
 410 Figure 3 CPVs of Both Players under Different Risk Preferences

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

416 It is easy to understand the relationship between CPV and the risk parameters from
 417 the equations. We can therefore conclude that: when the defender evenly distributes the

418 resource into all nodes, the attacker should choose the most conservative method in
 419 order to maximize the CPV. Note that we do not discuss the influence of risk preferences
 420 on the CPV of the defender here since we have already fixed the defending strategy.
 421 From the blue plane shown in Figure 3, when both players become more risk-averse,
 422 then the CPV of defender increases faster than the decrease of the CPV of the attacker.
 423 In reality, when the attacker cares more about the risk, then the strategy will become
 424 more conservative than before and thus increase the social welfare. Interestingly, we
 425 find that the attacker has the incentive to become risk-averse, which may finally
 426 increase the social welfare. This is counterintuitive since the reliability model applied
 427 in previous literature demonstrates that the attacker's radical strategies will lead to a
 428 lose-lose situation. In contrast, for the interdependent network, the design of attacking
 429 strategy is more challenging than the normal system without interdependency since the
 430 resource should be divided. In effect, a more risk-averse attacker and its conservative
 431 strategy increases the summation of CPV.

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



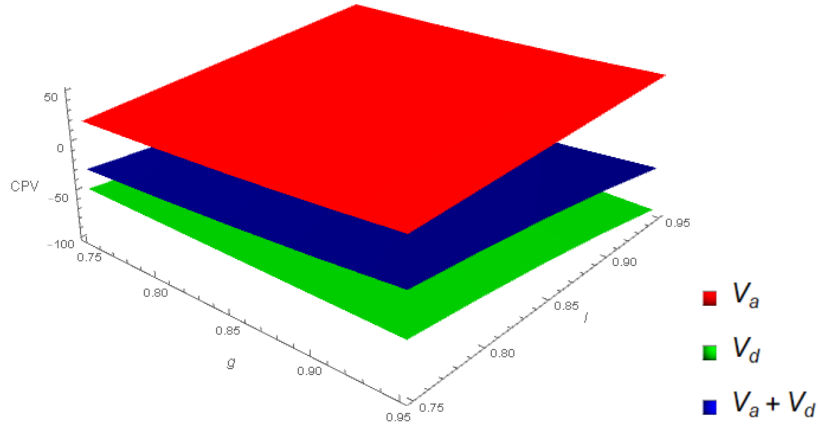
433 Figure 4 CPVs under the Alteration of λ

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

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

441 Interestingly, we find the same optimal attack and defense strategy as shown in
 442 Table 3 under the alteration of the risk preferences, for instance, no matter whether both

443 players become more risk-averse or risk-seeking, the optimal strategy for both players
 444 remain the same. Therefore, we now directly perform the CPV for both players when
 445 the defender is dynamic allocating its resource in Figure 5.



446
 447 Figure 5 CPVs of Both Players under Different Risk Preferences

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

452 Since the attacker will always choose the strategy to maximize its CPV after
 453 observing the action of the defender, then for the attacker, cases 1, 7, 8, or 12 will never
 454 occur. Therefore, the terms conclude parameter l in the expression of the attacker's
 455 CPV will be eliminated, making the CPV only depends on g . Similar, since the
 456 strategy of the defender will be countered by the attacker, the network will fall in case
 457 13 with no doubt. Thus, the CPV of the defender will only depend on l .

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

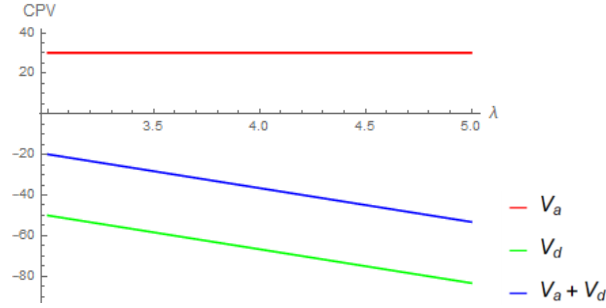


Figure 6 CPVs under the Alteration of λ

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

486 methods have been proposed.

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

495 To calculate the robustness of a complex system, one cannot theoretically derive
496 the dominating strategies for all players (see the game theoretical approach in Li et al.
497 (2019)). But it is possible to numerically investigate the optimal strategy based on the
498 design of algorithms and simulation. Additionally, quantum computer and quantum
499 computation are gaining extreme popularity these years. The construction of quantum
500 system accelerates the computational efficiency and benefits all fields, i.e., machine
501 learning and large-scale calculation. With the introduction of quantum computer, even
502 for complex systems with amounts of node, BDD can produce accurate results in an
503 acceptable time duration.

504

505 **7. Conclusions and Future Works**

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

514 Our future work will consider a possible extension of the case where both players
515 in the attack-defense game own unlimited resource. Then they should only optimize the

516 allocation and some close-formed solution may be obtained. Besides, our future
517 research will incorporate the use of false targets of the defender to increase the
518 survivability of each node in the networks. Additionally, as we mentioned in Section 4,
519 our future work will also incorporate two different scenarios: the attacker moves first,
520 and both players move simultaneously, and compare the result with our proposed model.
521 Finally, one can consider the calculation efficiency optimization. Simulation methods,
522 heuristic algorithms, and data reorganization are all potentially useful in employing
523 BDD to solve a large-scale complex system.

524

525 **Acknowledgment**

526 The research was supported by the NSFC under grant numbers 71671016 and
527 71832011.

528

529 **Reference**

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

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

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

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

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

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

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

- 546 *Statistical Mechanics and its Applications*, 436, 865-877.
- 547 Hardy, G., Lucet, C., & Limnios, N. 2007. K-terminal network reliability measures with
548 binary decision diagrams. *IEEE Transactions on Reliability*, 56(3), 506-515.
- 549 Hausken, K. 2006. Income, interdependence, and substitution effects affecting
550 incentives for security investment. *Journal of Accounting and Public Policy*, 25(6),
551 629-665.
- 552 Hausken, K. 2011, Strategic Defense and Attack of Series Systems when Agents Move
553 Sequentially, *IIE Transactions*, 43(7), 483-504.
- 554 Hausken, K. 2017a. Defense and attack of complex and dependent systems. *Reliability*
555 *Engineering & System Safety*, 95(1), 29-42.
- 556 Hausken, K. 2017b. Defense and Attack for Interdependent Systems. *European Journal*
557 *of Operational Research*, 256(2), 582-591.
- 558 Hausken, K. 2019. Defence and attack of complex interdependent systems. *Journal of*
559 *the Operational Research Society*, 70(3), 364-376.
- 560 Hausken, K., & Bier, V. M. 2011. Defending against multiple different attackers.
561 *European Journal of Operational Research*, 211(2), 370-384.
- 562 Hausken, K., Bier, V. and Zhuang, J. 2009, Defending Against Terrorism, Natural
563 Disaster, and All Hazards, in Bier, V.M. and Azaiez, M.N. (eds.), *Game Theoretic*
564 *Risk Analysis of Security Threats*, Springer, New York, 65-97.
- 565 Hausken, K., & Zhuang, J. 2011. Governments' and terrorists' defense and attack in a t-
566 period game. *Decision Analysis*, 8(1), 46-70.
- 567 Johansson, J., & Hassel, H. 2010. An approach for modelling interdependent
568 infrastructures in the context of vulnerability analysis. *Reliability Engineering &*
569 *System Safety*, 95(12), 1335-1344.
- 570 Kunreuther, H., & Heal, G. 2003. Interdependent security. *Journal of risk and*
571 *uncertainty*, 26(2-3), 231-249.
- 572 Levitin, G., & Hausken, K. 2009. Redundancy vs. protection in defending parallel
573 systems against unintentional and intentional impacts. *IEEE Transactions on*
574 *Reliability*, 58(4), 679-690.
- 575 Levitin, G., & Hausken, K. 2010. Defence and attack of systems with variable attacker

576 system structure detection probability. *Journal of the Operational Research*
577 *Society*, 61(1), 124-133.

578 Li, Y., Deng, Y., Xiao, Y., & Wu, J. 2019. Attack and Defense Strategies in Complex
579 Networks Based on Game Theory. *Journal of Systems Science and Complexity*,
580 32(6), 1630-1640.

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

584 Li, Y. P., Tan, S. Y., Deng, Y., & Wu, J. 2018. Attacker-defender game from a network
585 science perspective. *Chaos: An Interdisciplinary Journal of Nonlinear Science*,
586 28(5), 051102.

587 Liu, Y., Fan, Z. P., & Zhang, Y. 2014. Risk decision analysis in emergency response: a
588 method based on cumulative prospect theory. *Computers & Operations Research*,
589 42(2), 75-82.

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

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

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

599 Nganje, W., Bier, V., Han, H., & Zack, L. 2008. Models of interdependent security along
600 the milk supply chain. *American Journal of Agricultural Economics*, 90(5), 1265-
601 1271.

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

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

606 364-374.

607 Peng, R., Zhai, Q. Q., & Levitin, G. 2016. Defending a single object against an attacker
608 trying to detect a subset of false targets. *Reliability Engineering & System Safety*,
609 149, 137-147.

610 Polyn, S. M., Natu, V. S., Cohen, J. D., & Norman, K. A. 2005. Category-specific
611 cortical activity precedes retrieval during memory search. *Science*, 310(5756),
612 1963-1966.

613 Šenkeřík, R., Zelinka, I., Pluhacek, M., Viktorin, A., Janostik, J., & Oplatkova, Z. K.
614 2018. Randomization and Complex Networks for Meta-Heuristic Algorithms. In
615 Evolutionary Algorithms, Swarm Dynamics and Complex Networks (pp. 177-194).
616 Springer, Berlin, Heidelberg.

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

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

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

622 Wu, B., Tang, A., & Wu, J. 2016. Modeling cascading failures in interdependent
623 infrastructures under terrorist attacks. *Reliability Engineering & System Safety*,
624 147, 1-8.

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

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

630 Zhai, Q., Ye, Z. S., Peng, R., & Wang, W. 2016. Defense and attack of performance-
631 sharing common bus systems. *European Journal of Operational Research*, 256(3),
632 962-975.

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

- 636 Zhuang, J., Bier, V. M., & Gupta, A. 2007. Subsidies in interdependent security with
637 heterogeneous discount rates. *The Engineering Economist*, 52(1), 1-19.
- 638 Zio, E., & Sansavini, G. 2011. Modeling interdependent network systems for
639 identifying cascade-safe operating margins. *IEEE Transactions on Reliability*,
640 60(1), 94-101.