Trade-Off Between Redundancy, Protection, and Imperfect False Targets in Defending Parallel Systems

Hui Xiao and Rui Peng

Abstract A substantial amount of research over the past decades has studied the reliability of different systems, but most of them are restricted to systems with only internal failures. In practice, systems may fail due to unintentional impacts or intentional attacks. In this chapter, we first provide a comprehensive review of the research on improving system reliability. The survey shows that, for systems subject to intentional attacks, providing redundant system elements, protecting genuine elements, and deploying false targets are the three important measures to increase the system survivability. The trade-off between protecting genuine elements and deployment of imperfect false targets has been studied before, however, subject to a fixed number of genuine elements in the system. This chapter studies the trade-off between building redundant genuine elements, protection of genuine elements and deploying imperfect false targets in the defense of a capacitated parallel system. Numerical examples are carried out to illustrate the applications.

Keywords Vulnerability · Attack · Defence · False target · Protection · Parallel system

H. Xiao (✉)
Department of Management Science, School of Statistics, Southwestern University of Finance and Economics, Chengdu, China
e-mail: msxh@swufe.edu.cn

R. Peng
Donlinks School of Economics and Management, University of Science and Technology Beijing, Beijing, China
e-mail: pengrui1988@ustc.edu.cn

A. Lisnianski et al. (eds.), *Recent Advances in Multi-state Systems Reliability*, Springer Series in Reliability Engineering, DOI 10.1007/978-3-319-63423-4_12

1 Introduction

In the past two decades, reliability has received substantial attention in both industry and research [15, 17]. In order to model the complex modern systems more accurately, the traditional binary reliability theory has been extended to analyze multi-state systems that can perform their intended work at different intensities [34]. A variety of multi-state systems such as series-parallel systems [36], linear sliding window systems [18], linearly connectively connected systems [40] and multi-state network systems [48] have been studied in recent years. These reliability models have been successfully applied to analyze many real industrial systems such as power supply systems [33], maritime transportation systems [7], and high performance computing systems [50].

Most of the abovementioned research is restricted to systems with only internal failures. In practice, systems may fail due to external impacts. Examples of unintentional impacts include shocks, natural disasters, and unintentional human errors [41, 47]. Providing redundant system elements and elements protection are the two essential measures against unintentional impacts. Besides unintentional impacts, intentional attackers may circumvent the protection and choose the fragile positions to attack in order to destroy the system [42, 51]. For systems subject to intentional attacks, the defender not only need to provide redundancy and protect the genuine elements, but also can deploy some false targets in order to distract the attacker. In the literature, the false targets can be assumed to be perfect or imperfect. If the attacker cannot distinguish the false targets from the genuine elements, the false target is said to be perfect. If the false target can be detected by the attacker, the false target is imperfect. This chapter aims to analyze the trade-off among providing redundancy, investing in protection and deploying imperfect false targets. The work is closely related to some of the existing works, but differs in different aspects. Levitin and Hausken [21–23] have studied the different measures such as providing redundancy and protection, and deployment of false targets to defend parallel systems under attacks. In these works, the false targets are assumed to be perfect. In practice, false targets are usually detectable, i.e., imperfect. Thus, we study the scenario when false targets are assumed to be imperfect in this chapter. Peng et al. [38] considered the optimal number of false targets in both a parallel system and a series system assuming that the false targets are imperfect, but this paper does not consider the strategy of providing redundancy to improve the system reliability. Previous research has shown that providing redundancy is an important and useful measure to improve system reliability, therefore, this chapter proposes a model to study the optimal resource allocation in providing redundant system elements, protecting genuine system elements, and deploying false targets in the defense of capacitated parallel systems. The organization of this chapter is as follows. Section 2 conducts a comprehensive literature review on the relevant topics. Section 3 studies the defense of capacitated parallel systems with redundancy, protection, and imperfect false targets. The chapter is concluded in Sect. 4.

2 Literature Review

In the literature, approaches to minimize the system unavailability caused by internal failures include providing redundancy and finding the optimal maintenance policy [3, 44]. For example, Yeh and Fiondella [49] studied the optimal redundancy allocation for a multi-state computer network system. A correlated binomial distribution is applied to characterize the state distribution of the edges, which can exhibit multiple states. This redundancy allocation problem was solved using simulated annealing with an illustration in four practical networks. Ardakan and Hamadani [1] considered the redundancy allocation problem in a series-parallel system, where active and cold-standby strategies are simultaneously used in one subsystem. Utilizing the genetic algorithm, it determined the optimal component type, redundancy level, number of active units and cold-standby units jointly for each subsystem with the objective of maximizing the system reliability. Levitin and Amari [20] presented an approximation algorithm based on the universal generating function technique to evaluate the distribution of the time to failure for a k-out-of-n system with shared redundant elements. Besides providing redundancy, maintenance is also a frequently used measure to reduce the system internal failures. Peng et al. [40] studied the optimal preventive maintenance policy for linearly consecutively connected systems with the objective of minimizing the total maintenance cost while meeting a pre-specified system availability requirement. Xiao and Peng [46] studied the optimal element allocation and replacement interval in a series-parallel system with common bus performance sharing. Lisnianski et al. [35] considered a reliability importance evaluation for components in an aging multi-state system under minimal repair.

Besides the preventive replacement and minimal repair used in the abovementioned research, imperfect maintenance is also well studied in the literature [43]. For example, in order to model the wind turbine system in a wind farm, Ding and Tian [5] proposed an opportunistic maintenance policy that introduces different imperfect maintenance thresholds for failure turbines and working turbines. The proposed approach was shown to be effective in modeling the practical system in order to minimize the maintenance cost. Zhao et al. [52] utilized the cumulative processes theory and found the optimal imperfect maintenance policy by minimizing the expected cost rate for a used system. Pandey et al. [37] developed a selected maintenance strategy for a multi-state system with multi-state components. Different types of maintenance options such as replacement, do-nothing option, and imperfect repair were chosen to ensure that maximum system reliability could be achieved during the next mission.

Besides internal failures, systems may also fail due to external impacts. In general, the external impacts can be classified into unintentional impacts and intentional attacks. Natural disasters such as earthquakes and tsunamis are typical examples of unintentional impacts, while terrorism, warfare, intrusion, and human disruption are examples of intentional attacks [6]. In the case of external impacts, providing redundant systems elements and investing in protection are two effective

measures to improve system survivability, and the two measures have been well-studied in the literature. For example, Kunreuther and Heal [16] characterized the Nash equilibrium for an interdependent security problem to analyze the incentive of firms investing in protection against intentional attacks. Bier et al. [2] proposed general models for determining the optimal defense resource allocation assuming that the attacker will maximize either the expected damage or the success probability. Hausken [9] considered the security investment of several firms in cyber wars with external intruders. Zhuang and Bier [53] considered the defender resource allocation for countering terrorism and natural disasters. Hausken [10, 11] studied the strategic defense and attack for series and parallel systems consisting of independent components against intentional attacks. Levitin [19] considered the optimal trade-off between protection and redundancy in a homogenous parallel system subject to intentional attacks. When overarching protection is provided, the attacker can only destroy the components when the outside protection layer is penetrated. Haphuriwat and Bier [8] developed a model to allocate the resource optimally between target hardening and overarching protection and analyzed the effects that influence the trade-off between target hardening and overarching protection. Hausken [12] considered the individual and overarching protection versus attack for both defenders and attackers in both series and parallel systems. The model was extended to analyze the individual and overarching protection versus attack of assets in a simultaneous game and a two-period game [13]. Levitin et al. [32] further studied the viable number of individual protection versus overarching against strategic attack. Peng et al. [41] studied the optimal individual protection versus overarching protection versus maintenance for a parallel system subject to both internal failures and unintentional impacts. Deck et al. [4] proposed a model to analyze the scenario when the contest happens between an attacker and multiple defenders, and concluded that alliance of the defenders can reduce the defense spending and result in higher profit for defenders and attackers.

Besides providing redundant system elements and investing in protection, some researchers studied the deployment of false targets in defense of systems against intentional attacks. A historical example of using false targets (decoys) can be found in WWII and the Operation Desert Storm in 1990–1991. The objective of deploying false targets is to distract the attacker and dissipate the attack resource over greater number of targets. The defense measure of deploying false targets is most effective when the attacker cannot distinguish the false targets from genuine elements. Usually, false targets are much cheaper than genuine elements, but they are not costless. Deploying more false targets results in less resource allocated to provide redundancy and protect the genuine elements. In the literature, the study on the deploying false targets against intentional attacks has been studied in a variety of ways. Firstly, based on the assumption that the false targets can be destroyed with much less effort than the genuine elements, the attacker can distribute its attack resource in two sequential attacks so that the false targets can be eliminated as many as possible in the first attack [26, 29–31]. Secondly, the defense resource is usually distributed to provide redundancy, deploy false element and protect the genuine elements. In some scenarios, the defender can also distribute its resource to strike

preventively against the attacker [27, 28]. Thirdly, the quality of the false targets can be different in different scenarios. Some researchers assume that the false targets are perfect, i.e., the attacker cannot distinguish the false targets from the genuine elements [14, 21, 23, 24], while others consider the false targets as imperfect, i.e., the false target can be distinguished from the genuine elements by the attacker with certain probability [38, 39]. Lastly, some recent research has also considered the scenario that the attacker allocates part of the resource into intelligence activities to detect the false targets, and the defender allocates part of the resource into counter-intelligence activities [22, 25, 42].

In this chapter, the following notations will be used.

N	The number of genuine elements in the system
H	The number of false targets in the system
k	The number of false targets that are detected
Q_k	The number of objects the attacker tries to attack give k false targets are detected
P_k	The probability that k false targets are detected
x, y	The cost of a false target and a genuine element respectively
r, R	The total resource of the defender and attacker respectively
a, A	The unit cost of defending and attacking respectively
d	The detection probability of a false target
F	The system demand
g	The performance of a genuine element.

3 Defense of Parallel Systems with Redundancy, Protection, and Imperfect False Targets

Consider a parallel system that consists of N identical genuine elements. The defender can deploy imperfect false targets, provide redundancy, and protect genuine elements to minimize the expected damage that may be caused by the intentional attacks. The defender builds the system and distributes its defense resource first. The attacker takes it as given when it chooses its attack strategy. Therefore, it can be modeled as a two-period min-max game of perfect information where the defender moves in the first period, and the attacker moves in the second period. The defender decides how many false targets to deploy and how many redundant genuine elements to provide in order to minimize the expected damage caused by the attacker assuming that the attacker will always use the most harmful attack strategy.

The total resource of the attacker is a fixed value R. The unit cost of attacking an object is a constant denoted by A. We assume that attacker distributes the resource evenly among all attacked objects. All elements are assumed to be mutually independent. A single attack cannot destroy more than one object. In order to improve the system reliability, the defender can perform three different measures

using a fixed value of resource r. The defender can provide redundancy for the parallel system, and the cost of a genuine element is y. Therefore, the maximal number of genuine elements is $\lfloor r/y \rfloor$. The defender can deploy false targets at the cost of x each, and $x \ll y$. Similarly, the maximal number of false targets to deploy is $\lfloor (r - Ny)/x \rfloor$, where N is the number of genuine elements in this parallel system. The false target is imperfect, i.e., each false target can be detected by the attacker independently with probability d. The probability that k false targets are detected is denoted by p_k:

$$p_k = \binom{H}{k} d^k (1-d)^{H-k}, \tag{1}$$

where H is the total number of the false targets deployed.

The cost of a genuine element is much more than the cost of a false target. Additionally, the defender can protect the genuine elements using the remaining resource. The unit cost of protecting a genuine element is a, and the protection effort on each genuine element is assumed to be evenly distributed.

Given that N genuine elements and H false targets are placed in this system, the protection effort on each genuine element can be expressed as follows:

$$t = \frac{r - Ny - Hx}{Na}. \tag{2}$$

Suppose that $k\,(0 \le k \le H)$ false targets are detected. The attacker chooses Q_k out of $N + H - k$ objects to attack, where $1 \le Q_k \le N + H - k$. The attack effort on each attacked object is $T = R/(Q_k A)$. Therefore, the destruction probability of each element can be written using the contest function suggested by Tullock [45]:

$$v = \frac{T^m}{T^m + t^m} = \frac{R^m}{R^m + \frac{(r - Ny - Hx)^m (Q_k A)^m}{N^m a^m}} = \frac{R^m}{R^m + Q_k^m \varepsilon^m \frac{(r - Ny - Hx)^m}{N^m}}, \tag{3}$$

where $\varepsilon = A/a$, T and t are the efforts allocated to a single object by the attacker and the defender respectively. m is the parameter describing the intensity of the contest. If the no protection effort is provided, the element is destroyed with probability 1 when it is attacked since $v = 1$ if $t = 0$. The destruction probability will be always 0.5 if the intensity parameter m is zero. If $m \to \infty$, v is a step function where "winner takes all".

Given k and Q_k, the number of attacked genuine elements can vary from $\max(0, Q_k - H + k)$ to $\min(N, Q_k)$, where $\max(0, Q_k - H + k)$ refers to the scenario when all the false targets are attacked while $\min(N, Q_k)$ refers to the case when no false target is attacked. Let $\varphi(Q_k, i)$ denote the probability that among the Q_k attacked objects i of them are genuine elements. $\varphi(Q_k, i)$ can be derived using hyper-geometric distribution:

$$\varphi(Q_k, i) = \frac{\binom{N}{i}\binom{H-k}{Q_k-i}}{\binom{N+H-k}{Q_k}}. \quad (4)$$

Let $\theta(i,j)$ denote the probability that j elements out of i attacked genuine elements are destroyed. $\theta(i,j)$ can be determined based on the destruction probability function as follows:

$$\theta(i,j) = \binom{i}{j} v^j (1-v)^{i-j}. \quad (5)$$

In the parallel system, it is assumed that all genuine elements have the same functionality with performance rate g. The system demand is F. The system fails if at least $\lfloor N - F/g \rfloor + 1$ elements are destroyed by the attacker. When the system fails, the expected damage is proportional to the loss of demand probability. In this case, the risk can be obtained as follows:

$$D(Q_k, N, H) = F \cdot \sum_{i=\max(\lfloor N-F/g \rfloor + 1,\, Q_k - H + k)}^{\min(N, Q_k)} \left(\varphi(Q_k, i) \cdot \sum_{j=\lfloor N-F/g \rfloor + 1}^{i} \theta(i,j) \right). \quad (6)$$

The attacker chooses the most harmful strategy Q_k^* which maximizes $D(Q_k, N, H)$. The total risk over all possible values of k can be obtained as follows:

$$D(N,H) = \sum_{k=0}^{H} p_k \cdot D\left(Q_k^*, N, H\right) = \sum_{k=0}^{H} \left(\binom{H}{k} \cdot d_k \cdot (1-d_k) \cdot D\left(Q_k^*, N, H\right) \right). \quad (7)$$

In this two-period game, the defender moves first. Given the defender's strategy of H and N, the attacker chooses the best Q_k to maximize the damage $D(Q_k, N, H)$ when k false targets are detected. The defender knows that the attacker will maximize its damage for any value of H and N, and chooses the optimal H and N such that the expected risk $D(N,H)$ can be minimized.

For example, consider a parallel system that is made up by genuine elements to satisfy the demand of $F = 4$. The performance of each genuine element is $g = 1$. In order to protect the system, the defender can deploy false targets at the cost of $x = 0.03$ each and provide redundancy at the cost of $y = 0.1$ for a genuine element. The cost of the attacker's effort unit and defender's effort unit is assumed to be equal, i.e., $\varepsilon = 1$. The total resource of the attacker and defender are assumed to be $R = 1$ and $r = 1$ respectively.

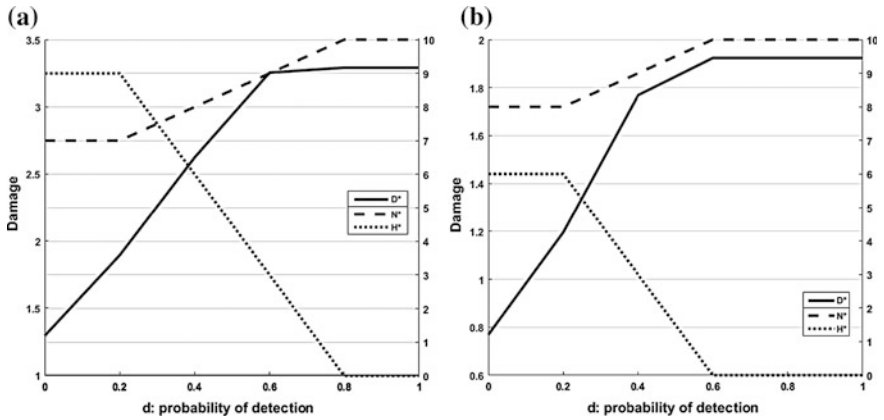

Fig. 1 Optimal number of false targets and the corresponding expected risk as a function of detection probability given intensity parameter m: (**a**) $m = 10$, (**b**) $m = 6$

Figure 1 shows the optimal redundancy, optimal number of false targets and the corresponding expected damage of this defense-attack game as a function of detection probabilities when the contest intensity parameter m is equal to 10 and 6 respectively. Figure 1 indicates that the expected damage and optimal redundancy increase when the probability of detection increases, but the optimal number of false targets decreases with increasing probability of detection. The numerical results show that it is worthy deploying false targets than providing redundancy when the detection probability is very low. When the probability of detection increases, the benefit of deploying false targets will be reduced. Furthermore, the redundancy reduces the need of false targets.

Figure 2 shows how the amount of resource owned by the attacker affects the optimal values of N, H and D. The results indicate that the expected damage increases due to the increase of resource owned by the attacker. It is also interesting to note that the optimal redundancy decreases and the optimal number of false targets increases when the attacker's resource increases. When the resource of the attacker increases, the destruction probability increases given the fixed contest intensity parameter. Therefore, the attacked GEs are more likely to be destroyed. This is why it is better to deploy more false targets so that the attack effect on each GE will be reduced.

Figure 3 shows that the expected damage is reduced when the resource of the defender increases. Naturally, increasing the resource of defense reduces the probability of destruction, therefore, the expected damage can be reduced. In Fig. 3, the optimal redundancy increases and the optimal number of false targets decreases in general when the resource of defense is increasing. It shows that increasing redundancy is better than increasing the false targets in order to minimize the expected damage if the resource of defense is unlimited.

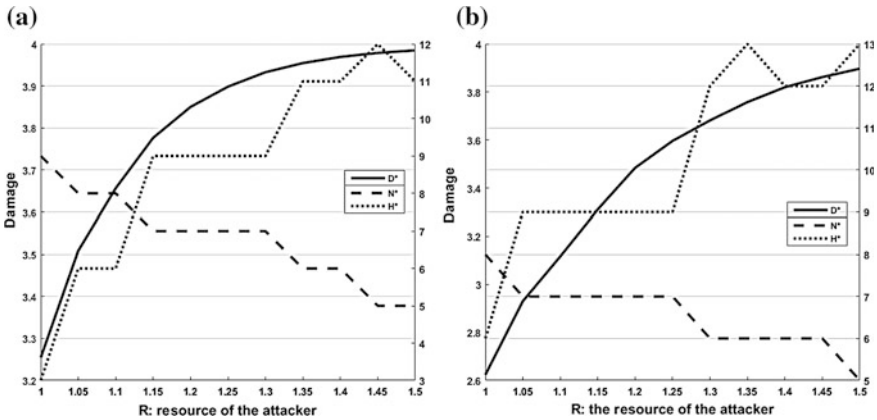

Fig. 2 Optimal number of false targets and the corresponding expected risk as a function of attacker's resource given detection probability d: (**a**) $d = 0.6$, (**b**) $d = 0.4$

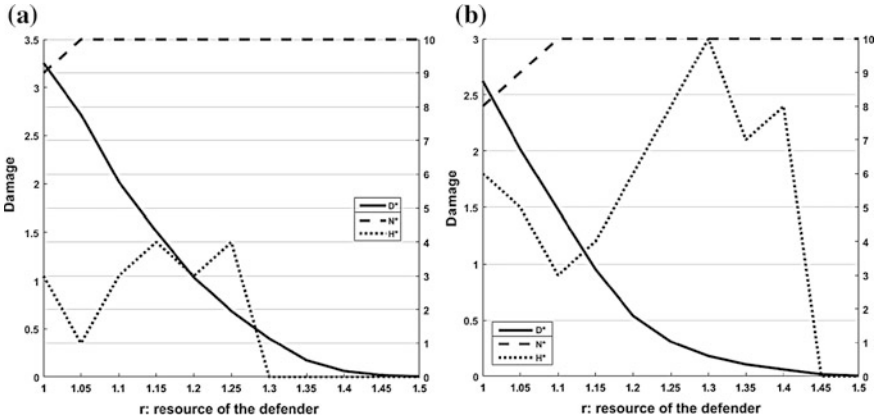

Fig. 3 Optimal number of false targets and the corresponding expected risk as a function of defender's resource when detection probability d: (**a**) $d = 0.6$, (**b**) $d = 0.4$

Figures 4 and 5 show the optimal redundancy, optimal number of false targets and the corresponding expected damage under different cost of a genuine element and different cost of a false target. Both figures indicate that the expected damage increases with increasing cost of a genuine element or a false target. When the cost of a genuine element increases, the optimal redundancy decreases and the optimal number of false targets increases. On the other hand, the optimal redundancy increases and the optimal number of false targets decreases when the cost of a false target increases.

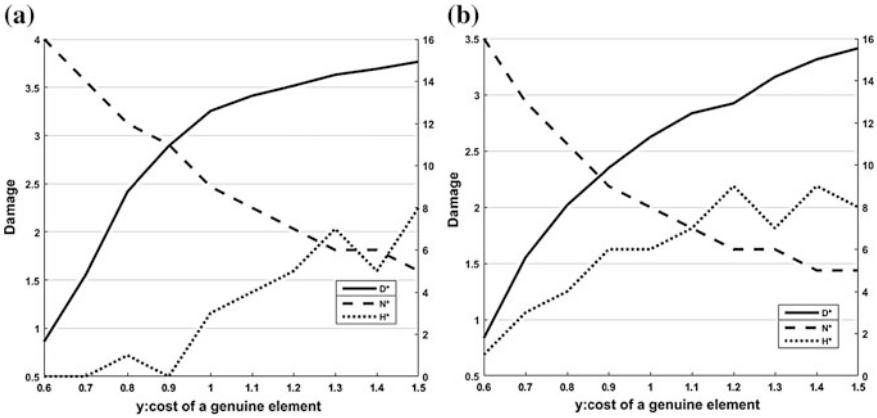

Fig. 4 Optimal number of false targets and the corresponding expected risk as a function of cost of a genuine element when detection probability d: (**a**) $d = 0.6$, (**b**) $d = 0.4$

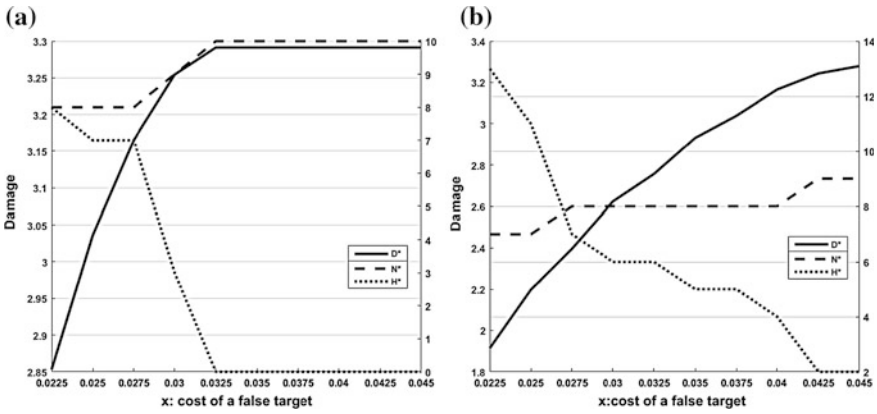

Fig. 5 Optimal number of false targets and the corresponding expected risk as a function of cost of a false target when detection probability d: (**a**) $d = 0.6$, (**b**) $d = 0.4$

4 Conclusions and Future Research

This chapter considers protecting a capacitated parallel system under intentional attacks. The defense resource can be allocated to protect the genuine element, deploy imperfect targets, and provide redundancy in order to minimize the expected damage caused by intentional attacks. Given the protection strategy of the defender, the attacker will choose the optimal number of elements to attack such that the damage can be maximized. Therefore, the defender must take consideration of the attacker's decision to optimally allocate the defense resource to minimize the total expected damage. To illustrate the attack-defense model, several numerical

experiments are conducted to analyze the effect of detection probability, the amount of resource owned by the defender and the attacker, and the cost of a genuine element and a false target. The numerical experiments indicate that the optimal number of false targets decreases when the probability of detection increases. When the detection probability become larger, it is better to allocate more resources to provide redundancy rather than deploying false targets. When the resource of the attacker becomes large, it is more worthy deploying more false targets than providing redundancy. However, more redundancy should be provided rather than deploying false targets if the resource of the defender is large. Besides, as consistent as the theoretic argument, higher cost of a genuine element results in a smaller optimal value of the redundancy, while higher cost of a false targets leads to a smaller optimal number of false targets.

This chapter uses a two-period dynamic game of perfect information to model the contest between the attacker and the defender assuming each party has full information about the other. In future, the model can be extended to consider the scenario when full information is not available. Besides, it is also important to consider the scenario when preventive strikes may be used by the defender. In this case, the problem becomes more complicated since the defender will consider the resource allocation for preventive strikes, and the attacker may consider using part of the resource to defend the preventive strike. Furthermore, it is also interesting to analyze the contest model between one defender and multiple attackers in future.

Acknowledgements The research is supported by the NSFC under grant numbers 71601158, 71671016 and 71231001, and by the Fundamental Research Funds for the Central Universities of China and FRF-BR-15-001B.

References

1. Ardakan M, Hamadani A (2014) Reliability optimization of series–parallel systems with mixed redundancy strategy in subsystems. Reliab Eng Syst Saf 130:132–139
2. Bier V, Nagaraj A, Abhichandani V (2005) Protection of simple series and parallel systems with components of different values. Reliab Eng Syst Saf 87:315–323
3. Chang C (2014) Optimum preventive maintenance policies for systems subject to random working times, replacement, and minimal repair. Comput Ind Eng 67:185–194
4. Deck C, Foster J, Song H (2015) Defense against an opportunistic challenger: theory and experiments. Eur J Oper Res 242:501–513
5. Ding F, Tian Z (2012) Opportunistic maintenance for wind farms considering multi-level imperfect maintenance thresholds. Renew Energy 45:175–182
6. Enders W, Sandler T (2006) The political economy of terrorism. Cambridge University Press, New York
7. Faghih-Roohi S, Xie M, Ng K, Yam R (2014) Dynamic availability assessment and optimal component design of multi-state weighted k-out-of-n systems. Reliab Eng Syst Saf 123:57–62
8. Haphuriwat N, Bier V (2011) Trade-offs between target hardening and overarching protection. Eur J Oper Res 213:320–328

9. Hausken K (2006) Income, interdependence, and substitution effects affecting incentives for security investment. J Acc Public Policy 25:629–665
10. Hausken K (2008) Strategic defense and attack for reliability systems. Reliab Eng Syst Saf 93:1740–1750
11. Hausken K (2008) Strategic defense and attack for series and parallel reliability systems. Eur J Oper Res 186:856–881
12. Hausken K (2013) Combined series and parallel systems subject to individual versus overarching defense and attack. Asia Pac J Oper Res 30
13. Hausken K (2014) Individual versus overarching protection and attack of assets. CEJOR 22:89–112
14. Hausken K, Levitin G (2009) Protection vs. FTs in series systems. Reliab Eng Syst Saf 94:973–981
15. Kapur K (1977) Reliability in engineering design. Wiley, New York
16. Kunreuther H, Heal G (2003) Interdependent security. J Risk Uncertainty 26:231–249
17. Kuo W, Zuo M (2002) Reliability engineering: theory and practice. Wiley, New York
18. Levitin G (2003) Linear multi-state sliding-window systems. IEEE Trans Reliab 52(2): 263–269
19. Levitin G (2007) Optimal defense strategy against intentional attacks. IEEE Trans Reliab 56:148–157
20. Levitin G, Amari S (2010) Approximation algorithm for evaluating time-to-failure distribution of k-out-of-n system with shared standby elements. Reliab Eng Syst Saf 95 (4):396–401
21. Levitin G, Hausken K (2009) False targets vs. redundancy in homogeneous parallel systems. Reliab Eng Syst Saf 94(2):588–595
22. Levitin G, Hausken K (2009) Intelligence and impact contests in systems with redundancy, false targets, and partial protection. Reliab Eng Syst Saf 94(12):1927–1941
23. Levitin G, Hausken K (2009) Redundancy vs. protection vs. false targets for systems under attack. IEEE Trans Reliab 58(1):58–68
24. Levitin G, Hausken K (2009) False targets efficiency in defense strategy. Eur J Oper Res 194 (1):155–162
25. Levitin G, Hausken K (2009) Intelligence and impact contests in systems with fake targets. Defense Secur Anal 25(2):157–173
26. Levitin G, Hausken K (2011) Is it wise to protect false targets. Reliab Eng Syst Saf 96 (12):1647–1656
27. Levitin G, Hausken K (2011) Preventive strike vs. false targets and protection in defense strategy. Reliab Eng Syst Saf 96(8):912–924
28. Levitin G, Hausken K (2012) Preventive strike vs. false targets in defense strategy. Int J Performability Eng 8(4):341–354
29. Levitin G, Hausken K (2013) is it wise to leave some false targets unprotected? Reliab Eng Syst Saf 112:176–186
30. Levitin G, Hausken K, Ben Haim H (2014) Defending systems against two sequential attacks. Mil Oper Res 19(1):19–35
31. Levitin G, Hausken K, Ben Haim H (2014) False targets in defending systems against two sequential attacks. Mil Oper Res 19(1):19–35
32. Levitin G, Hausken K, Dai Y (2014) Optimal defense with variable number of overarching and individual protections. Reliab Eng Syst Saf 123:81–90
33. Li Y, Zio E (2012) A multi-state model for the reliability assessment of a distributed generation system via universal generating function. Reliab Eng Syst Saf 106:28–36
34. Lisnianski A, Levitin G (2003) Multi-state system reliability: assessment, optimization and applications. World Scientific, Singapore
35. Lisnianski A, Frenkel I, Khvatskin L (2015) On Birnbaum importance assessment for aging multi-state system under minimal repair by using the L-z-transform method. Reliab Eng Syst Saf 142:258–266

36. Nourelfath M, Yalaoui F (2012) Integrated load distribution and production planning in series-parallel multi-state systems with failure rate depending on load. Reliab Eng Syst Saf 106:38–145
37. Pandey M, Zuo M, Moghaddass R (2013) Selective maintenance modeling for a multistate system with multistate components under imperfect maintenance. IIE Trans 45(11): 1221–1234
38. Peng R, Levitin G, Xie M, Ng S (2010) Defending simple series and parallel systems with imperfect false targets. Reliab Eng Syst Saf 95:679–688
39. Peng R, Levitin G, Xie M, Ng S (2011) Optimal defense of single object with imperfect false targets. J Oper Res Soc 62(1):134–141
40. Peng R, Xie M, Ng S, Levitin G (2012) Element maintenance and allocation for linear consecutively connected systems. IIE Trans 44(11):964–973
41. Peng R, Guo L, Levitin G, Mo H, Wang W (2014) Maintenance versus individual and overarching protections for parallel systems. Qual Technol Quant Manage 11(3):353–362
42. Peng R, Zhai Q, Levitin G (2016) Defending a single object against an attacker trying to detect a subset of false targets. Reliab Eng Syst Saf 149:137–147
43. Pham H, Wang H (1996) Imperfect maintenance. Eur J Oper Res 94(3):425–438
44. Taghipour S, Kassaei M (2015) Periodic inspection optimization of a k-out-of-n load-sharing system. IEEE Trans Reliab 64(3):1116–1127
45. Tullock G (1980) Efficient rent seeking. In Buchanan JM, Tollison RD, Tullock G (eds) Toward a theory of the rent-seeking society. Texas A&M University Press, College Station, Texas
46. Xiao H, Peng R (2014) Optimal allocation and maintenance of multi-state elements in series–parallel systems with common bus performance sharing. Comput Ind Eng 72:143–151
47. Xiao H, Shi D, Ding Y, Peng R (2016) Optimal loading and protection of multi-state systems considering performance sharing mechanism. Reliab Eng Syst Saf 149:88–95
48. Yeh W (2014) Multistate network reliability evaluation under the maintenance cost constraint. Int J Prod Econ 88(1):73–83
49. Yeh C, Fiondella L (2017) Optimal redundancy allocation to maximize multi-state computer network reliability subject to correlated failures. Reliab Eng Syst Saf 166:138–150
50. Yu H, Yang J, Mo H (2014) Reliability analysis of repairable multi-state system with common bus performance sharing. Reliab Eng Syst Saf 132:90–96
51. Zhai Q, Ye Z, Peng R, Wang W (2016) Defense and attack of performance-sharing common bus systems. Eur J Oper Res 256(3):962–975
52. Zhao X, Nakagawa T, Qian C (2012) Optimal imperfect preventive maintenance policies for a used system. Int J Syst Sci 43(9):1632–1641
53. Zhuang J, Bier V (2007) Balancing terrorism and natural disasters—defensive strategy with endogenous attacker effort. Oper Res 55(5):976–981