Defense and Attack of Performance-Sharing Common Bus Systems

Qingqing Zhai[a], Zhi-Sheng Ye[a1], Rui Peng[b], Wenbin Wang[b,c],

[a]Department of Industrial and Systems Engineering, National University of Singapore, Singapore.

[b]Donlinks School of Economics and Management, University of Science and Technology Beijing, Beijing, China.

[c]Faculty of Business and Law, Manchester Metropolitan University, UK.

Abstract: This paper studies the defense and attack strategies for a system with a common bus performance-sharing mechanism that is subject to intentional attacks. The performance-sharing mechanism allows any surplus performance of a component to be transmitted to other components in the system via the common bus. A practical example of such a system is the power system. The system may fail due to internal causes, such as component degradation, as well as intentional attacks, such as acts of terrorism. The defender allocates its resources to maximize the system's reliability by protecting the common bus and the components. The attacker allocates its resources to minimize the system's reliability by attacking the common bus and the components. We propose a framework to model both the reliability and the defense-attack contest for a general common bus system. Based on this framework, we investigate the optimal defense and attack strategies for a system with identical components in a two-stage min-max game.

Keywords: game theory, common bus, performance sharing, defense and attack.

Notations

n	Number of components in the system
C_i	Nominal capacity of component i, $i = 1, \ldots, n$
D_i	Local demand for component i $(D_i \leq C_i)$

[1] Corresponding author. Email: yez@nus.edu.sg. Phone: (65)6601 2303.

S	Maximum transmission capacity of the common bus
p_i^I	Failure probability of component i due to internal causes
p_i^O	Failure probability of component i due to intentional attacks
e_i	Defense effort on component i from the defender
E_i	Attack effort on component i from the attacker
p_{bus}^I	Failure probability of the common bus due to internal causes
p_{bus}^O	Failure probability of the common bus due to intentional attacks
e_{bus}	Defense effort on the common bus
E_{bus}	Attack effort on the common bus
$F(e,E)$	Contest function
a_i	Expenses of unit effort for protecting component i
A_i	Expenses of unit effort for attacking component i
a_{bus}	Expenses of unit effort for protecting the common bus
A_{bus}	Expenses of unit effort for attacking the common bus
r	Budget of the defender, $\sum_{i=1}^{n} e_i a_i + e_{bus} a_{bus} \leq r$
R	Budget of the attacker, $\sum_{i=1}^{n} E_i A_i + E_{bus} A_{bus} \leq R$
x	Proportion of the defender's budget allocated to protect the common bus in the common bus system with identical components
y	Number of protected components in the common bus system with identical components

X Proportion of the attacker’s budget allocated to attack the common bus in the common bus system with identical components

Y Number of attacked components in the common bus system with identical components

1. Introduction

Infrastructure systems, such as power systems and distributed computing systems, provide essential services for daily life in the modern society. Many infrastructure systems contain components that are connected via a common bus, where the demand (or the workload) on the system can be appropriately distributed to each component (Kong & Ye, 2016; Ye, Revie & Walls, 2014). In addition, any surplus performance of a component can be shared with other components in the system via the common bus. Through such performance sharing, system reliability can be considerably improved and performance deficiency can be reduced (Levitin, 2011). The common bus can be the software, hardware and operators that distribute the demand. For example, Fig. 1 shows the power system in a region consisting of power stations and the grid connecting them. In this system, a power station has to first satisfy the local demand and can then transmit any surplus electricity to other power stations through the power grid. Therefore, the power grid is the common bus in this system.

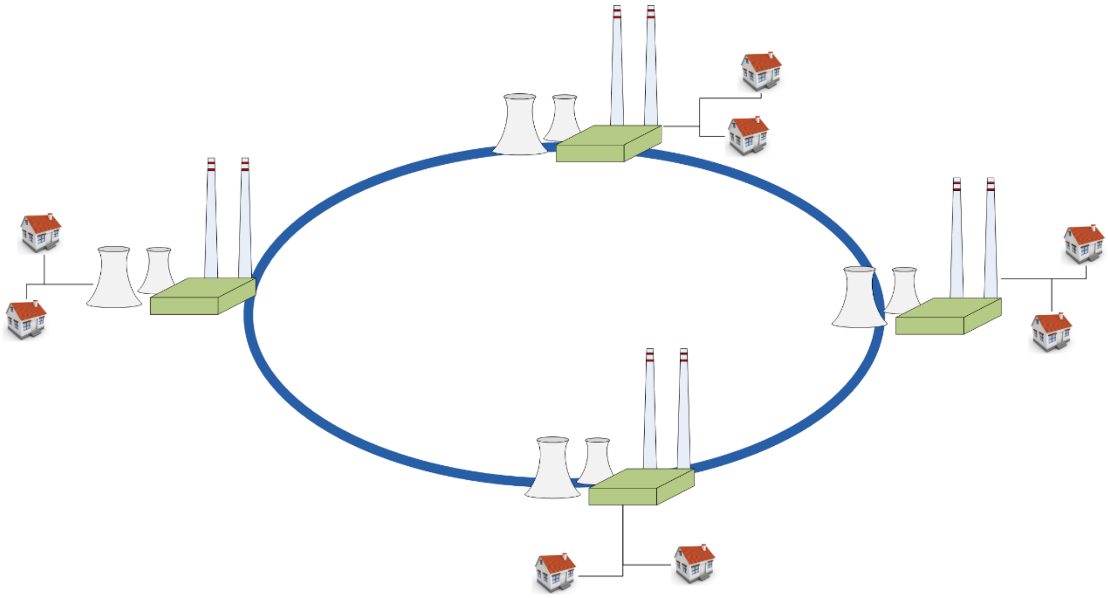


Fig. 1 The power system with a performance-sharing common bus.

Lisnianski and Ding (2009) considered the reliability of a common bus system with two multi-state components, where surplus performance can be transmitted from the reserve component to the main component. Levitin (2011) proposed a more general multi-state common bus performance-sharing model by considering real-world applications, such as meshed power distribution systems with a developed reconfiguration ability, highly interconnected data transmission systems, and grid computing systems where surplus performance can be transmitted in any direction. Following Levitin (2011), the reliability of such common bus performance-sharing systems has drawn the attention of many researchers (Peng, Liu & Xie, 2016; Xiao & Peng, 2014; Xiao, Shi, Ding & Peng, 2016; Yu, Yang & Mo, 2014). It is well recognized that a system will fail due to internal causes and external impacts. Existing studies focus primarily on the reliability of common bus systems subject to internal failures or unintentional external impacts (Xiao et al., 2016); however, in some situations, attackers intentionally carry out external impacts. Unlike unintentional impacts, the intentional attacker can choose their attack strategy according to the system's protection strategy. Intentional attacks, such as acts of terrorism, pose a significant threat to the system's survivability, and have received considerable attention after the attack on the World Trade Towers on Sep 11, 2001 (Bier & Abhichandani, 2002).

Early works on intentional attacks focus on solving the defender's optimization problem, thereby increasing the system's survival probability. Kunreuther and Heal (2003), Hausken

(2006), Zhuang, Bier and Gupta (2007), and Deck, Foster and Song (2015) studied the protection of interdependent systems, where each component is protected by one defender. In contrast, some studies assume that one defender protects the whole system, such as in Bier, Nagaraj and Abhichandani (2005), Azaiez and Bier (2007), Peng, Guo, Levitin, Mo and Wang (2014), and Paulson, Linkov and Keisler (2016). Recently, more studies account for both the defense and attack strategies. Many studies model the contest as a two-stage min-max game (Azaiez & Bier, 2007; Hausken & Zhuang, 2012; Ramirez-Marquez, Rocco, & Levitin, 2009; Zhang & Ramirez-Marquez, 2013). In a two-stage min-max game involving one defender and one attacker, the defender moves first and distributes its resources to minimize the expected system loss by assuming that the attacker will use the most harmful attack strategy. When the attacker then moves, it has full knowledge about the defensive resource allocation, based on which it optimally allocates its attack resources to maximize the expected damage to the system. Some other studies model the contest as a simultaneous game where the attacker has no information on the defensive investments, such as in Dighe, Zhuang and Bier (2009), Zhang, Ramirez-Marquez and Wang (2015), and Zhuang, Bier and Alagoz (2010). In this scenario, the Nash equilibrium approach can be used to solve the defense and attack strategies (Nikoofal & Zhuang, 2015).

In the common bus system, if the common bus is functioning then the surplus performance can be transmitted to places suffering from performance deficiency. Hence, it can be viewed as a redundant system. In contrast, if the common bus fails due to internal causes or is destroyed by intentional attacks, the system is reliable only if all of its components satisfy the local demand (Levitin, 2011). Hence, it can be viewed as a series system. Therefore, the common bus system is a complex system that generalizes series systems and parallel systems. The protection of series systems and parallel systems against intentional attacks has been studied extensively, such as in Bier and Abhichandani (2002), Bier et al. (2005), and Hausken (2008b). Levitin (2007) considered the defense of a series-parallel system with protection cases while Hausken (2008a) studied the protection and attack strategies of series-parallel and parallel-series systems. Levitin and Hausken (2008) studied the optimal resource allocation between protecting the components and deploying separated redundant components against intentional attacks. From the system level, the common bus acts like an overarching protection layer

(Hausken & Levitin, 2012), where the system is more prone to failure after the common bus fails. However, in the case of overarching protection, the attacker can only attack the individual components after penetrating the overarching protection layer: see Haphuriwat and Bier (2011), Hausken (2013, 2014), Levitin and Hausken (2012), and Levitin, Hausken and Dai (2014) for one-layer overarching protection, and Golalikhani and Zhuang (2011) for multiple-layer overarching protection. In contrast, the attacker can attack the components without destroying the common bus, and the system can also fail even when the common bus still functions. Hence, the defense and attack of the common bus system is particularly different from existing studies. Such systems abound in real-world applications and play important roles in daily life. It is of practical importance to study the defense and attack of such systems.

The remainder of the paper is organized as follows. Section 2 gives a detailed description of the common bus system and states the model assumptions. Section 3 presents a general modeling framework for the defense and attack of the common bus system that is under intentional attacks. In Section 4, we study the defense and attack of a particular common bus system with identical components. Section 5 analyzes the impact of some parameters in the model on the optimal defense and attack strategies. Conclusions are given in Section 6.

2. System description and assumptions

2.1 The common bus system

Consider a system consisting of n components and one performance-sharing common bus that connects these n components. The components and the common bus are assumed to be binary, i.e., they are either operational or have completely failed.

Component $i (i = 1, \ldots, n)$ has a nominal capacity C_i in the operational state (e.g., the electrical power for a power station) and has to meet a local demand D_i ($D_i \leq C_i$, e.g., the local electricity demand). Clearly, there would be a surplus capacity $(C_i - D_i)$ when component i is operational and a performance deficiency D_i when component i fails. Due to the common bus, surplus capacity can be transmitted to those components suffering from performance deficiency. A practical assumption is that the performance-sharing capacity of the common bus is not unlimited: there is a maximum capacity S. Thus, the performance shared via the common bus is at its minimum among:

- the total surplus performance $\sum_{i=1}^{n} \max\{0, c_i - D_i\}$,
- the total performance deficiency $\sum_{i=1}^{n} \max\{0, D_i - c_i\}$,
- and the common bus capacity S.

Here, c_i is the actual capacity of component i, taking the value of C_i when the component is operational and 0 otherwise.

If any local demand cannot be satisfied, a loss will be incurred (Bier & Kosanoglu, 2015). Following Levitin (2011), we focus on the probability that all local demand is being satisfied, and deem that the system fails whenever any local demand is not met.

2.2 Defense-attack contest

In the system, a component or the common bus may fail due to internal causes or intentional attacks. Internal causes and intentional attacks are assumed to be independent of one another. In either case, the component or the common bus cannot operate properly and their actual capacity is 0. We assume component i (the common bus) would fail due to internal causes with probability p_i^I (p_{bus}^I), and would be destroyed by intentional attacks with probability

$$p_i^O = F(e_i, E_i) \ (p_{bus}^O = F(e_{bus}, E_{bus})),$$

where e_* and E_* are the respective defense and attack efforts. $F(\cdot,\cdot)$ is the contest success function, satisfying the practical assumptions that: (i) $F(e, E)$ is a non-increasing function of e and a non-decreasing function of E; and (ii) $F(e, 0) = 0$ and $F(0, E) = 1, \forall E > 0$. This means that a component would not be destroyed if the attacker does not attack the component, and the component would definitely be destroyed if it were attacked when unprotected. Hence, with a specific contest function, the destruction probability of a component or the common bus depends on the resources that the defender and the attacker allocate to it.

A commonly used contest function of the ratio form is

$$F(e, E) = \frac{E^{\lambda_0}}{e^{\lambda_0} + E^{\lambda_0}}, \tag{1}$$

which originates from the rent seeking theory (Tullock, 1980). Here, $\lambda_0 \geq 0$ is the contest intensity coefficient. A large λ_0 indicates that, with slightly more effort, any one of the competitors can easily take the upper hand. When $\lambda_0 = 0$, $F(e, E) = 1/2$ as long as $e > 0$ and $E > 0$; therefore, the competitors can win the contest with equal probability regardless of their effort. On the other hand, $F(e, E) \rightarrow 1_{(E>e)}$ for $\lambda_0 \rightarrow +\infty$, indicating that the "winner takes all". Many studies use such a contest function to model the defense-attack contest (Hausken & Bier, 2011; Levitin & Hausken, 2009; Mo, Xie & Levitin, 2015), and one may refer to Skaperdas (1996) and Hausken (2005) for more theoretical discussions.

In the defense-attack contest, the expense of a unit effort (e.g., in dollars) for attacking and defending the component i are A_i and a_i, respectively, and the expense of attacking and defending the common bus are A_{bus} and a_{bus}, respectively. We assume that the total available budgets for the attacker and the defender are R and r, respectively. Both the attacker and the defender are strategic. The attacker can allocate its resources into attacking the common bus and the components, while the defender can allocate its resources into protecting them. The attacker intends to maximize the probability of destroying the system, while the defender tries to maximize the system's reliability.

3. General contest modeling for the common bus system

In this section, we propose a modeling framework for a common bus system under intentional attack. As described in Section 2, the surplus capacity of one component may be transmitted to other components whose local demand cannot be satisfied. However, when the components have different capacities and are subject to different local demands, the performance-sharing between components can become complicated. In this case, identifying scenarios that can lead to a system failure is a complex combinatory problem. Hence, we propose to use a universal generation function (UGF)-based approach to efficiently determine the system reliability (Levitin, 2005; Ushakov, 1987).

The UGF method is an effective and universal tool for solving combinatory problems. A UGF represents the probability mass function (pmf) of a discrete random variable X:

$$\Pr\{X = x_k\} = p_k, k = 1, \dots, K$$

by a polynomial $u(z) = \sum_{k=1}^{K} p_k\, z^{x_k}$. Resorting to the corresponding UGF, many combinatory problems involving the random variable can be solved. For example, consider the pmf of the sum of two discrete random variables X and Y, $(X + Y)$. Suppose the UGFs of X and Y are $u_X(z) = \sum_{k=1}^{K} p_k\, z^{x_k}$ and $u_Y(z) = \sum_{l=1}^{L} q_l\, z^{y_l}$, respectively. Then, by applying a multiplication operation to $u_X(z)$ and $u_Y(z)$, we can obtain the UGF of the random variable $(X + Y)$:

$$u_X(z)u_Y(z) = \sum_{k=1}^{K}\sum_{l=1}^{L} p_k q_l\, z^{x_k + y_l}.$$

From the UGF, the pmf of $(X + Y)$ can be readily obtained. For more details and applications of the UGF technique, see Levitin (2005).

To derive the system reliability using UGF, we first consider a single component i. As the component may fail due to both internal causes and intentional attacks, the total failure probability is

$$P_i = 1 - \left(1 - p_i^I\right)\left(1 - p_i^O\right) = p_i^I + p_i^O - p_i^I p_i^O.$$

Corresponding to the operational and the failed state of component i, there is a surplus performance $C_i - D_i$ and a deficiency D_i. Then, we can use a bivariate UGF to represent the pmf of component i as

$$u_i(z_1, z_2) = (1 - P_i) z_1^{C_i - D_i} z_2^0 + P_i z_1^0 z_2^{D_i}, \tag{2}$$

where the exponents of z_1 and z_2 represent the performance surplus and performance deficiency, respectively. Clearly, the performance surplus and deficiency at each state (i.e., operational or failed) of component i are linked to the corresponding occurrence probability using the UGF.

Then, the system UGF accounting for the total system performance surplus and deficiency is obtained as the product of all component UGFs:

$$U(z_1, z_2) = \prod_{i=1}^{n} u_i(z_1, z_2) = \sum_{j=1}^{J} \gamma_j z_1^{w_{j,1}} z_2^{w_{j,2}}, \tag{3}$$

where $w_{j,1}$ represents the total system performance surplus, $w_{j,2}$ represents the total system deficiency, γ_j is the corresponding occurrence probability, and J is the number of terms after collecting like terms. For instance, for a system consisting of two components, we can obtain the system UGF as

$$U(z_1, z_2) = u_1(z_1, z_2)u_2(z_1, z_2)$$
$$= (1 - P_1)(1 - P_2)z_1^{C_1+C_2-D_1-D_2}z_2^0 + (1 - P_1)P_2 z_1^{C_1-D_1}z_2^{D_2} + P_1(1 - P_2)z_1^{C_2-D_2}z_2^{D_2}$$
$$+ P_1 P_2 z_1^0 z_2^{D_1+D_2}.$$

Then, from the system UGF $U(z_1, z_2)$, we can infer that

- with probability $(1 - P_1)(1 - P_2)$, the system has surplus capacity $(C_1 + C_2 - D_1 - D_2)$ and performance deficiency 0;
- with probability $(1 - P_1)P_2$, the system has surplus capacity $(C_1 - D_1)$ and performance deficiency D_2;
- with probability $P_1(1 - P_2)$, the system has surplus capacity $(C_2 - D_2)$ and performance deficiency D_1;
- and with probability $P_1 P_2$, the system has surplus capacity 0 and performance deficiency $D_1 + D_2$.

Thus, we can obtain all possible operation scenarios and their corresponding occurrence probabilities according to the system UGF. Given that the common bus is operating, the conditional system reliability equals the sum of the occurrence probabilities that the total performance deficiency $w_{j,2}$ is smaller than the minimum between the total surplus capacity $w_{j,1}$ and the common bus capacity S:

$$R_1 = \sum_{j=1}^{J} 1_{\min\{w_{j,1}, S\} \geq w_{j,2}} \gamma_j. \tag{4}$$

However, if the common bus fails, no performance sharing is possible among the system. In this instance, any component failure would result in an unmet local demand and thus a system failure. The conditional system reliability in this case is $\prod_{i=1}^{n}(1 - P_i)$. Unconditionally, the overall system reliability is

$$R_S = P_{bus} \prod_{i=1}^{n}(1 - P_i) + (1 - P_{bus})R_1. \tag{5}$$

From the defense-attack contest perspective, the system reliability is a function of the resource allocation of both the defender and the attacker:

$$R_S = R_S(e_1, \ldots, e_n, e_{bus}, E_1, \ldots, E_n, E_{bus}).$$

The defender has to properly allocate its resources to maximize the system reliability:

$$\max_{e_1,\ldots,e_n,e_{bus}} R_S \text{, s.t.} \sum_{i=1}^{n} a_i e_i + a_{bus} e_{bus} \leq r, e_i \geq 0, e_{bus} \geq 0. \quad (6)$$

In contrast, the attacker seeks to minimize the system reliability:

$$\min_{E_1,\ldots,E_n,E_{bus}} R_S \text{, s.t.} \sum_{i=1}^{n} A_i E_i + A_{bus} E_{bus} \leq R, E_i \geq 0, E_{bus} \geq 0. \quad (7)$$

It can be easily verified that R_S is a non-decreasing function of $e_i, i = 1, \ldots, n$ and e_{bus}, and a non-increasing function of $E_i, i = 1, \ldots, n$ and E_{bus}. Hence, the optimal policy for both the attacker and the defender will be achieved at the boundary of the constraints, i.e., the defender would spend their entire budget on protecting the system while the attacker would spend their entire budget on attacking it. It can be proven that both problems are of convex optimization, given that the contest function $F(e, E)$ is convex about e and concave about E (see Appendix A). Then, the optimal policies in the general case can be easily found by solving the above optimization problems. When the objectives in Eq. (6) and (7) are not convex, the problems can be solved by heuristic optimization methods such as the genetic algorithm (Ye, Li & Xie, 2010).

The type of game between the defender and the attacker is determined by whether the attacker knows the resource allocation of the defender. If the attacker has no knowledge of the defensive resource allocation, then the optimal defense and attack strategy can be solved by the Nash equilibrium approach (Nikoofal & Zhuang, 2015). In this case, the optimal defense and attack strategies satisfy

- Defender: $R_S(e_1^*, \ldots, e_n^*, e_{bus}^*, E_1^*, \ldots, E_n^*, E_{bus}^*)$
  $\geq R_S(e_1, \ldots, e_n, e_{bus}, E_1^*, \ldots, E_n^*, E_{bus}^*), \forall e_1, \ldots, e_n, e_{bus},$
- Attacker: $R_S(e_1^*, \ldots, e_n^*, e_{bus,}^* E_1^*, \ldots, E_n^*, E_{bus}^*)$
  $\leq R_S(e_1^*, \ldots, e_n^*, e_{bus}^*, E_1, \ldots, E_n, E_{bus}), \forall E_1, \ldots, E_n, E_{bus}.$

In contrast, if the attacker has full knowledge of the defensive resource allocation, then the contest can be modeled by a two-stage min-max game. The optimal defense strategy is

$$(e_1^*, \ldots, e_n^*, e_{bus}^*) = \arg \max_{e_1,\ldots,e_n,e_{bus}} \left(\min_{E_1,\ldots,E_n,E_{bus}} R_S(e_1, \ldots, e_n, e_{bus}, E_1, \ldots, E_n, E_{bus}) \right),$$

while the optimal attack strategy with $(e_1^*, \dots, e_n^*, e_{bus}^*)$ given above is

$$(E_1^*, \dots, E_n^*, E_{bus}^*) = \arg \min_{E_1, \dots, E_n, E_{bus}} R_S(e_1^*, \dots, e_n^*, e_{bus}^*, E_1, \dots, E_n, E_{bus}).$$

From a defense point of view, it seems safe to assume that the attacker can know the defense strategy. In the following, we consider a special common bus system with identical components and investigate the optimal defense and attack strategies under a two-stage min-max game.

4. Contest on common bus system with identical components

4.1 System reliability modeling

Suppose the components are identical, i.e., $C_i = C$ (capacity), $a_i = a$, $A_i = A$ (expenses of unit defense and attack effort, respectively) and $p_i^I = p^I$ (failure probability due to internal causes) for all $i = 1, \dots, n$, and the demands for all the components are also the same, i.e., $D_i = D$ for $i = 1, \dots, n$. Then, if the defender decides to protect some components, it should spend the same effort on these components. Nevertheless, the defender may choose to leave some components unprotected to concentrate its effort elsewhere. Similarly, the attacker can choose to attack a subset of the components and/or the common bus.

As previously mentioned, the optimal strategy is achieved when the defender/attacker spends its entire budget in the contest. Hence, we assume that the defender spends part of its budget xr $(x \in [0,1))$ on protecting the common bus and evenly distributes the remaining $(1-x)r$ among y selected components. Therefore, the defense effort on each component is $(1-x)r/(ya)$ for the y protected components. The attacker spends part of its resources XR $(X \in [0,1))$ on attacking the common bus and the rest $(1-X)R$ on attacking the components. We assume the attacker does not know exactly which components are protected, and it randomly chooses Y components to attack. Hence, the attack effort on each attacked component is $(1-X)R/(YA)$. For each component in the system, there are four possible situations: (i) protected and attacked; (ii) unprotected but attacked; (iii) protected but not attacked; (iv) unprotected and not attacked. The component destruction probabilities under the first two situations are $F\big((1-x)r/(ya), (1-X)R/(YA)\big)$ and 1, respectively, while the destruction probabilities for the latter two cases are 0 and can be merged as "not attacked".

Note that a component would definitely be destroyed if it is attacked but not protected. Hence, when the common bus is destroyed, the system can only survive if the attacked components are among the protected components. The system reliability attributed to this case is

$$R_{S,2}=\begin{cases}P_{bus}\cdot\frac{\binom{y}{Y}}{\binom{n}{Y}}(1-P)^{Y}, Y\le y,\\ 0, Y>y,\end{cases} \tag{8}$$

where $P_{bus}=p_{bus}^{I}+(1-p_{bus}^{I})F(xr/a_{bus},XR/A_{bus})$ and $P=p^{I}+(1-p^{I})F\big((1-x)r/(ya),(1-X)R/(YA)\big)$.

If the common bus is not destroyed, then surplus performance can be transmitted to components suffering from performance deficiency. If $(n-k)$ components fail and k components survive, then the total performance surplus is $k(C-D)$ and the total performance deficiency is $(n-k)D$. Accounting for the limited transmission capacity of the common bus, the system can survive only if the following inequality holds:

$$(n-k)D\le\min\{k(C-D),S\}\Leftrightarrow k\ge\max\left\{n-\frac{S}{D},\frac{nD}{C}\right\}. \tag{9}$$

Let $K=\lceil\max\{n-S/D,nD/C\}\rceil$, the smallest integer greater than or equal to $\max\{n-S/D,nD/C\}$. Then the system should have at least K components operating simultaneously to ensure the system's operation. In other words, the system is a K-out-of-n redundant system given that the common bus does not fail. The system reliability attributed to this case is

$$R_{S,1}=(1-P_{bus})\times\sum_{l=\max\{0,Y-y\}}^{\min\{Y,n-K,n-y\}}\frac{\binom{n-y}{l}\binom{y}{Y-l}}{\binom{n}{Y}}\sum_{m=0}^{\min\{Y-l,n-K-l\}}\binom{Y-l}{m}P^{m}(1-P)^{Y-l-m}. \tag{10}$$

Here, the attacker chooses Y components to attack, where l out of Y may be the unprotected components and these components would definitely fail under attack. As there are $(n-y)$ unprotected components, we have $l\le n-y$ and $Y-l\le y\Rightarrow l\ge Y-y$. Also note that if $l>n-K$, there would be more than $n-K$ component failures, and thus the system will be destroyed. Therefore, $l\le n-K$. Among the $Y-l$ protected and attacked components, m out of them may fail with probability $\binom{Y-l}{m}P_1^{m}(1-P_1)^{Y-l-m}$. An illustration for the case when the common bus does not fail is given in Fig. 2.

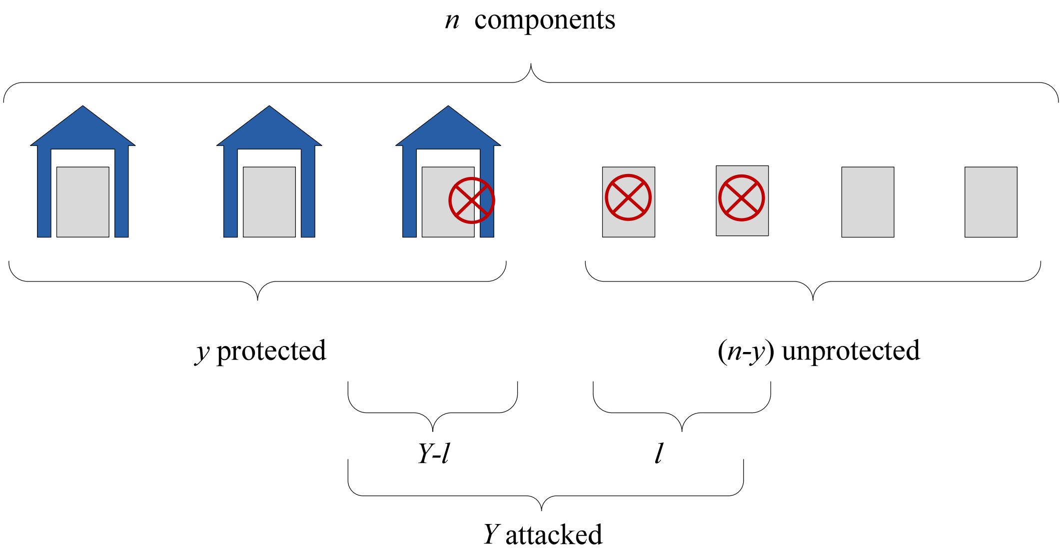


Fig. 2 Defense and attack of the system components when the common bus is operating.

To sum up, the system reliability is

$$R_S = R_{S,1} + R_{S,2} = (1 - P_{bus}) \times \sum_{l=\max\{0,Y-y\}}^{\min\{Y,n-K,n-y\}} \frac{\binom{n-y}{l}\binom{y}{Y-l}}{\binom{n}{Y}} \sum_{m=0}^{\min\{Y-l,n-K-l\}} \binom{Y-l}{m} P^m (1-P)^{Y-l-m} + 1_{Y\le y} P_{bus} \cdot \frac{\binom{y}{Y}}{\binom{n}{Y}} (1-P)^Y. \quad (11)$$

4.2 Optimal defense and attack strategies

We consider the contest between the defender and the attacker in a two-stage min-max game framework (Levitin & Hausken, 2010). The defender deploys its defense strategy first, and the attacker then follows by attacking the protected system. It is assumed that both the defender and the attacker have full knowledge of the contest (i.e., all the parameters of the system and the contest function). When the attacker moves in the second stage, it knows the defensive resource allocation between the common bus and the components x and the number of protected components y. Note that the attacker may not have full knowledge about x and y in reality, but it is conservative for the defender to assume that the attacker can anticipate the defense strategy and implement the most harmful attack (Peng, Levitin, Xie & Ng, 2011). The optimal defense and attack strategies are derived recursively. Specifically, the attacker seeks to minimize the system reliability by properly choosing X and Y, which depend on the defender's strategy x and y:

$$(X^*, Y^*) = \arg\min_{X,Y} R_S(X, Y; x, y). \tag{12}$$

By substituting the optimal X^* and Y^* into R_S, the defender can find the optimal x^* and y^* that minimize the maximum possible destruction from the attacker:

$$(x^*, y^*) = \arg\max_{x,y} R_S(X^*(x, y), Y^*(x, y), x, y). \tag{13}$$

In this contest, the defender should protect at least K components, i.e., $y \geq K$; otherwise, the attacker can always choose to attack all the n components and more than $n - K$ components would be destroyed. Hence, the system reliability degenerates to

$$R_S = (1 - P_{bus}) \times \sum_{l=\max\{0,Y-y\}}^{\min\{Y,n-y\}} \frac{\binom{n-y}{l}\binom{y}{Y-l}}{\binom{n}{Y}} \sum_{m=0}^{\min\{Y-l,n-K-l\}} \binom{Y-l}{m} P^m (1-P)^{Y-l-m} + 1_{Y\leq y} P_{bus} \cdot \frac{\binom{y}{Y}}{\binom{n}{Y}} (1-P)^Y. \tag{14}$$

Consider an example with $n = 8$, $K = 4$, $R/A = r/a = 1$, $A_{bus} = A$, $a_{bus} = a$, $p^I = p^I_{bus} = 0$. Here, the optimal number of protected components for the defender should not be smaller than $K = 4$. Applying the ratio contest function $F(e, E) = E^{\lambda_0}/(e^{\lambda_0} + E^{\lambda_0})$ with $\lambda_0 = 1$, we find the optimal attack strategy (Y^*, X^*) for different combinations of (x, y). It shows that Y^* is always 8, i.e., the attacker would attack all the components. The system reliability in this case is

$$R_S = (1 - P_{bus}) \sum_{m=0}^{y-4} \binom{y}{m} P^m (1-P)^{y-m} + 1_{y\geq 8} P_{bus} (1-P)^Y.$$

The variation of X^* (the optimal proportion of the resources allocated to attack the common bus) with x for different Y is shown in Fig. 3. For the case $y < 8$ where some components are left unprotected, X^* is a non-increasing function of x. This indicates that the attacker reduces its investment in attacking the common bus when the defender increases its effort in protecting the common bus. As the defensive investment in protecting the components decreases, it becomes easier for the attacker to disable the system by destroying more than 4 components rather than destroying the common bus. X^* is close to 1 when x is small for $y =$

5,6,7, i.e., the attacker spends almost all of its resources on attacking the common bus. This is because the attacker can destroy the whole system with negligible effort by destroying the unprotected components once the common bus is destroyed. When x is smaller than a threshold, X^* increases with y because the defensive resource is diluted on a single component and the attacker can destroy the same component with less effort. Therefore, it will move its focus to the common bus. When $y = 8$, i.e., all the components are protected, the optimal X^* first increases with x and then decreases to zero when x exceeds a threshold. This is because the contest becomes fair when all components are protected. When x increases, the attacker first has to cope with the increased defensive investment of the common bus. When x exceeds a certain proportion (around 0.23 in this case), the attacker reduces its effort in attacking the common bus and seeks to destroy more components instead. When x is sufficiently large ($x > 0.55$), the attacker gives up the contest over the common bus and focuses on destroying the components.

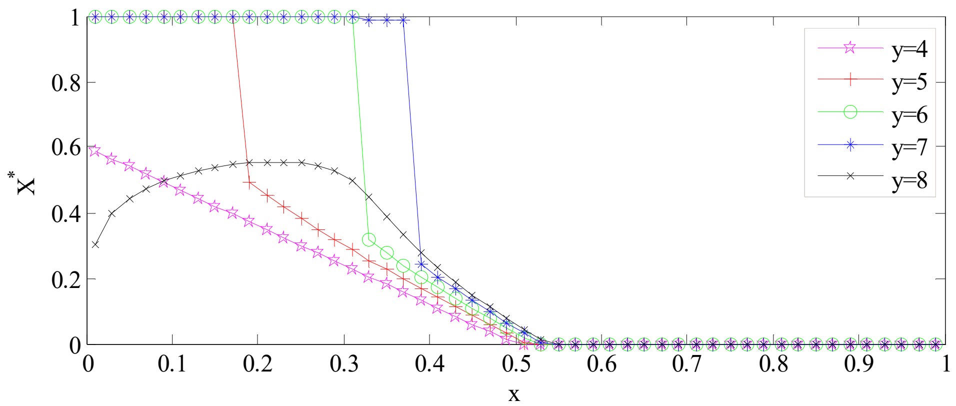


Fig. 3 Optimal proportion of resources for attacking the common bus, X^*, for different x and y.

The variation of $R_S^*(x, y)$ (the minimum system reliability when the attacker takes the most harmful strategy) versus x for different y is given in Fig. 4. For all y, $R_S^*(x, y)$ first increases and then decreases after a peak is reached with respect to x. When $y < 8$, the system reliability increases with y in general for a fixed x, indicating that the defender benefits from protecting more components. Note that $R_S^*(x, y)$ can be the same for different y when x is relatively small. This is because the attacker spends almost all its resources on attacking the common bus and uses negligible effort in attacking the 8 components (referring to Fig. 3). As there are unprotected components, the system would fail if the common bus fails, and the survival probability of the common bus determines the system reliability. Note that $R_S^*(x,8) > R_S^*(x,y)$ for $y<8$, indicating that protecting all 8 components is always optimal for the defender. In particular, the optimal defense strategy is $(x^*,y^*)=(0.36,8)$, where the defender spends 36% of its resources on protecting the common bus and the remaining 64% on protecting the 8 components. Corresponding to this defense strategy, the optimal attack strategy is $(X^*,Y^*)=(0.36,8)$, i.e., the attacker spends 36% of its resources on attacking the common bus and the remaining 64% on attacking the 8 components. The system survival probability under this defense-attack contest is 0.32.

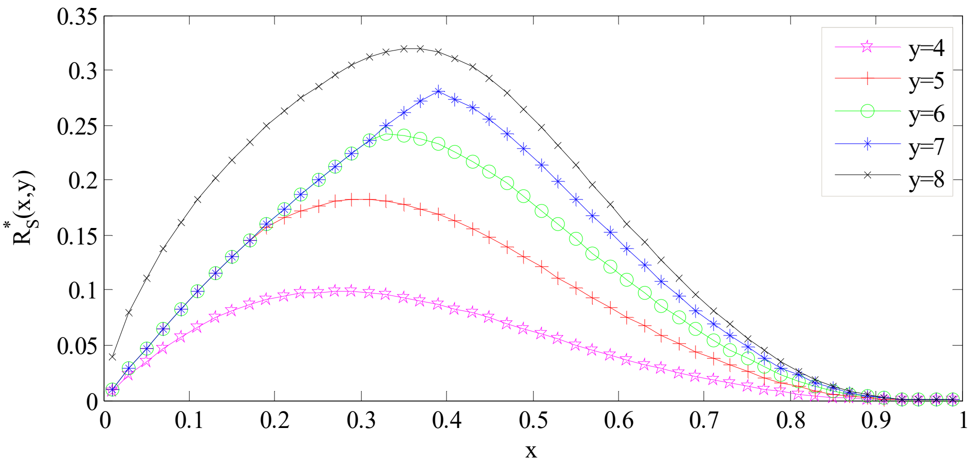


Fig. 4 Optimal (minimum) system reliability for the attacker for different x and y.

4.3 Optimal number of attacked and protected components

When the defender chooses to protect all the components, i.e., $y=n$, then we can obtain the system reliability from Eq. (14) as

$$R_S = (1-P_{bus}) \sum_{m=0}^{\min\{Y,n-K\}} \binom{Y}{m} P_Y^m (1-P_Y)^{Y-m} + P_{bus}\cdot(1-P_Y)^Y. \quad (15)$$

Here, the subscript "Y" of P_Y is to indicate that P_Y is a function of Y. Let $H_1(Y) = \sum_{m=0}^{\min\{Y,n-K\}} \binom{Y}{m} P_Y^m (1-P_Y)^{Y-m}$. Then, $H_1(Y)=1$ for $Y<n-K$. For $Y \geq n-K$, we have

$$H_1(Y) = \sum_{m=0}^{n-K} \binom{Y}{m} P_Y^m (1-P_Y)^{Y-m}.$$

Therefore,

$$H_1(Y+1) - H_1(Y)$$

$$= \sum_{m=0}^{n-K} \binom{Y+1}{m} P_{Y+1}^m (1-P_{Y+1})^{Y+1-m} - \sum_{m=0}^{n-K} \binom{Y}{m} P_Y^m (1-P_Y)^{Y-m}$$

$$= \sum_{m=0}^{n-K} \binom{Y}{m} P_{Y+1}^m (1-P_{Y+1})^{Y+1-m} + \sum_{m=1}^{n-K} \binom{Y}{m-1} P_{Y+1}^m (1-P_{Y+1})^{Y+1-m}$$

$$- \sum_{m=0}^{n-K} \binom{Y}{m} P_Y^m (1-P_Y)^{Y-m}$$

$$= \sum_{m=0}^{n-K} \binom{Y}{m} P_{Y+1}^m (1-P_{Y+1})^{Y-m} - P_{Y+1} \binom{Y}{n-K} P_{Y+1}^{n-K} (1-P_{Y+1})^{Y-n+K}$$

$$- \sum_{m=0}^{n-K} \binom{Y}{m} P_Y^m (1-P_Y)^{Y-m}.$$

As the derivative of $\sum_{m=0}^{n-K} \binom{Y}{m} P^m (1-P)^{Y-m}$ with respect to P is $-Y \binom{Y-1}{n-K} P^{n-K} (1-P)^{Y-n+K-1}$, we have the following approximation according to the mean value theorem:

$$H_1(Y+1) - H_1(Y)$$

$$= -Y \binom{Y-1}{n-K} \tilde{P}^{n-K} \left(1-\tilde{P}\right)^{Y-n+K-1} (P_{Y+1} - P_Y) - P_{Y+1} \binom{Y}{n-K} P_{Y+1}^{n-K} (1-P_{Y+1})^{Y-n+K}$$

$$\approx \binom{Y}{n-K} P_{Y+1}^{n-K} (1-P_{Y+1})^{Y-n+K-1} [(Y-n+K)(P_Y - P_{Y+1}) - (P_{Y+1} - P_{Y+1}^2)],$$

where $\tilde{P} \in (P_{Y+1}, P_Y)$ (note that $P_{Y+1} < P_Y$ because of the dilution of the attack effort). In this case,

$$P_Y = p^I + (1-p^I) \frac{\left(\frac{(1-X)R}{YA}\right)^{\lambda_0}}{\left(\frac{(1-X)R}{YA}\right)^{\lambda_0} + \left(\frac{(1-x)r}{na}\right)^{\lambda_0}} = p^I + (1-p^I) \frac{\rho}{\rho + Y^{\lambda_0}}$$

and $\frac{dP_Y}{dY} = -(1-p^I) \frac{\rho \lambda_0 Y^{\lambda_0 - 1}}{\left(\rho + Y^{\lambda_0}\right)^2}$, where $\rho = \left(\frac{na(1-X)R}{A(1-x)r}\right)^{\lambda_0}$. Therefore,

$$(Y-n+K)(P_Y - P_{Y+1}) - (P_{Y+1} - P_{Y+1}^2)$$

$$= (1-p^I)(Y-n+K) \frac{\rho \lambda_0 \tilde{Y}^{\lambda_0 - 1}}{\left(\rho + \tilde{Y}^{\lambda_0}\right)^2} - (1-p^I) \frac{(Y+1)^{\lambda_0}}{\rho + (Y+1)^{\lambda_0}} \left(p^I + (1-p^I) \frac{\rho}{\rho + (Y+1)^{\lambda_0}}\right)$$

$$\leq (1-p^I)(Y-n+K) \frac{\rho \lambda_0 \tilde{Y}^{\lambda_0 - 1}}{\left(\rho + \tilde{Y}^{\lambda_0}\right)^2} - (1-p^I) \frac{\rho (Y+1)^{\lambda_0}}{\left(\rho + (Y+1)^{\lambda_0}\right)^2}$$

$$\approx (1-p^I)(Y-n+K) \frac{\rho \lambda_0 (Y+1)^{\lambda_0 - 1}}{\left(\rho + (Y+1)^{\lambda_0}\right)^2} - (1-p^I) \frac{\rho (Y+1)^{\lambda_0}}{\left(\rho + (Y+1)^{\lambda_0}\right)^2}$$

$$= (1-p^I)(Y-n+K)\frac{\rho(Y+1)^{\lambda_0-1}}{\left(\rho+(Y+1)^{\lambda_0}\right)^2}\left[\lambda_0-\left(1+\frac{n-K+1}{Y-n+K}\right)\right],$$

where $\tilde{Y} \in [Y, Y+1]$. When Y $(Y \geq n-K)$ is large and λ_0 is small (i.e., the approximation analysis holds and $\lambda_0 < 1+\frac{n-K+1}{Y-n+K}$), we would have $H_1(Y+1) < H_1(Y)$. If $(1-P_Y)^Y$ is also a decreasing function of Y (which is the case for $\lambda_0 \leq 1$, as shown in Appendix B), then R_S will also be a decreasing function of Y. In this case, the optimal Y^* will be achieved at n.

Conversely, when the attacker fixes the number of attacked components to $Y = n$, we have

$$R_S = (1-P_{bus})\sum_{m=0}^{y-K}\binom{y}{m}P_y^m\left(1-P_y\right)^{y-m} + 1_{y\geq n}P_{bus}\left(1-P_y\right)^n. \tag{16}$$

Let $H_2(y) = \sum_{m=0}^{y-K}\binom{y}{m}P_y^m\left(1-P_y\right)^{y-m}$. Analogously, we have

$$H_2(y+1) - H_2(y)$$
$$= \left(P_{y+1}-P_{y+1}^2\right)\binom{y}{K-1}P_{y+1}^{y-K}\left(1-P_{y+1}\right)^{K-1} - y\binom{y-1}{y-K}\hat{P}^{y-K}\left(1-\hat{P}\right)^{K-1}\left(P_{y+1}-P_y\right)$$
$$\approx \binom{y}{K-1}P_{y+1}^{y-K}\left(1-P_{y+1}\right)^{K-1}\left[\left(P_{y+1}-P_{y+1}^2\right)-(y-K+1)\left(P_{y+1}-P_y\right)\right],$$

where $\hat{P} \in \left(P_y, P_{y+1}\right)$ (note that $P_y < P_{y+1}$ because of the dilution of the defense effort). We can similarly derive that

$$\left(P_{y+1}-P_{y+1}^2\right)-(y-K+1)\left(P_{y+1}-P_y\right)$$
$$\geq (1-p^I)\frac{\gamma(y+1)^{\lambda_0}}{\left((y+1)^{\lambda_0}+\gamma\right)^2} - (1-p^I)(y-K+1)\frac{\gamma\lambda_0\hat{y}^{\lambda_0-1}}{\left(\hat{y}^{\lambda_0}+\gamma\right)^2}$$
$$\approx (1-p^I)\frac{\gamma(y+1)^{\lambda_0}}{\left((y+1)^{\lambda_0}+\gamma\right)^2} - (1-p^I)(y-K+1)\frac{\gamma\lambda_0(y+1)^{\lambda_0-1}}{\left((y+1)^{\lambda_0}+\gamma\right)^2}$$
$$= (1-p^I)(y-K+1)\frac{\gamma(y+1)^{\lambda_0-1}}{\left((y+1)^{\lambda_0}+\gamma\right)^2}\left[\left(1+\frac{K}{y-K+1}\right)-\lambda_0\right],$$

where $\gamma = \left(\frac{nA(1-x)r}{a(1-X)R}\right)^{\lambda_0}$. When y $(y \geq K)$ is large and the contest intensity λ_0 is small (i.e., the approximation analysis holds and $\lambda_0 < 1+\frac{K}{y-K+1}$), we would have $H_2(y) < H_2(y+1)$. Clearly, $1_{y\geq n}P_{bus}\left(1-P_y\right)^n$ is a non-decreasing function of y. This means that R_S is an increasing function of y. Therefore, the optimal y^* in this case is n.

Combining the analysis above, we infer that whenever the defender/attacker decides to distribute its resources evenly among all the components, an optimal choice for its competitor is to distribute its resources evenly among all the components as well, given that the above assumptions are satisfied. Then, the system reliability is a function of x and X only:

$$R_S = R_S(x, X) = (1 - P_{bus}) \sum_{m=0}^{n-K} \binom{n}{m} P^m (1-P)^{n-m} + P_{bus}(1-P)^n. \tag{17}$$

4.4 Defense and attack under different contest functions

The contest function $F(e, E)$ characterizes the destruction probability attributed to the defender and the attacker. With different contest functions, the contest between the defender and the attacker may be distinct. This leads to different defense and attack strategies.

In this section, we compare the exponential contest function $F(e, E) = 1 - \exp\left\{-\frac{\lambda_1 E}{e}\right\}$ in Nikoofal and Zhuang (2015) with the ratio contest function in the defense and attack of the common bus system, where $\lambda_1 = \ln 2$ so that $F(e, E) = \frac{1}{2}$ for $e = E$. A comparison of the two contest functions is illustrated in Fig. 5.

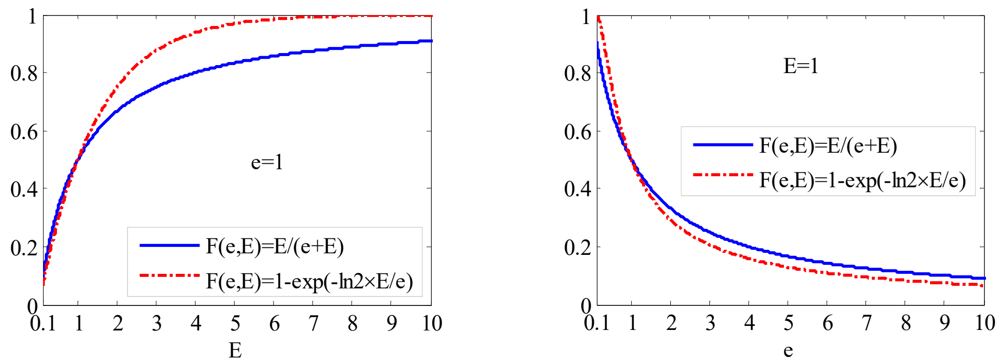


Fig. 5 Comparison of different contest functions.

With the exponential contest function and the same other parameters for the system, we obtain the optimal attack strategy of the attacker under different defense strategies. Fig. 6 illustrates the optimal number of components that the attacker should attack for different x and y. It shows that, except for a quite small x ($x = 0.01$), it is always optimal for the attacker to attack all 8 components. In fact, when x is 0.01, it makes negligible difference for the attacker to attack $Y > y$ components, as the system would definitely be destroyed as long as the common bus and at least one component are destroyed. Therefore, the system destruction probability is determined by the contest over the common bus. This is also revealed in Fig. 7, where the attacker spends almost all of its resources on attacking the common bus. Hence, attacking all the components is always an optimal strategy for the attacker.

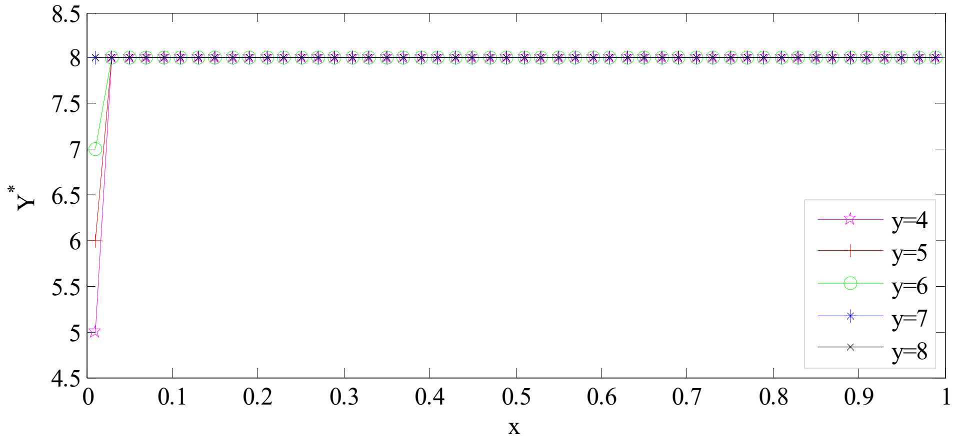


Fig. 6 Optimal number of components to attack for the attacker for different x and y.

Fig. 7 shows the optimal proportion of the resource allocated to attack the common bus, X^*, for different x and y. In contrast to the ratio contest function shown in Fig. 3, there is a sharp drop of the optimal X^* when x exceeds a certain threshold for all y. For $y = 4,5,6,7$, X^* drops from approximately 1 to 0 when x exceeds a threshold. This indicates that the attacker spends all its effort on destroying the common bus when the defender's effort on the common bus is low, and switches to attacking the components when the defender's effort on the common bus increases to a certain level. For $y = 8$, where all the components are protected, the attacker first increases its investment in attacking the common bus to cope with the increased x, and then gives up attacking the common bus and focuses on attacking the 8 components after x exceeds a threshold. The different behavior of X^* with respect to x can be explained by comparing the exponential and the ratio contest functions. From Fig. 5, it can be noted that the attacker finds it easier to get the upper hand if it spends more than the defender, and finds it easier to be defeated if it spends less than the defender under the exponential contest function than under the ratio contest function. Hence, it is much easier for the attacker to take extreme choices in the contest under the exponential contest function. This explains the sharp change of X^* with respect to x.

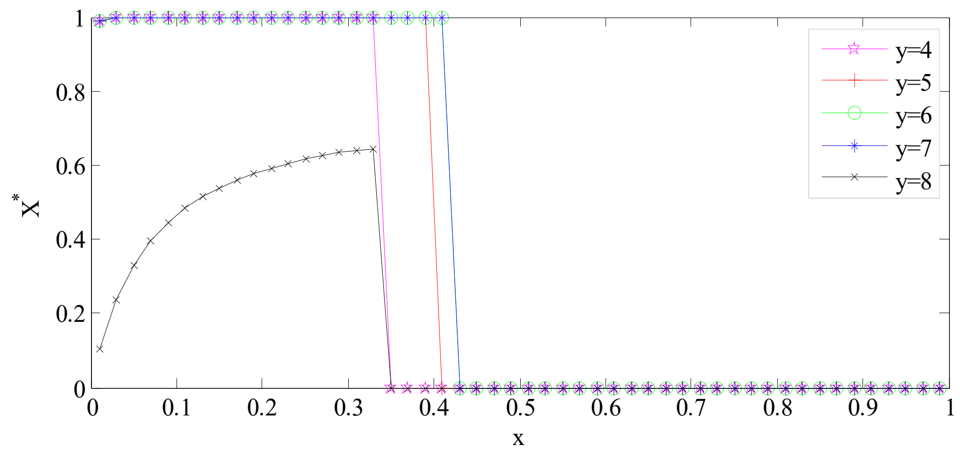


Fig. 7 Optimal proportion of resources for attacking the common bus, X^*, for different x and y.

The system reliability when the attacker optimally chooses its attack strategy is given in Fig. 8. The overall trend of $R_S^*(x, y)$ with respect to x is similar to that under the ratio contest function, but is less gentle due to the difference between the two contest functions, as explained. The optimal strategy for the defender is $(x^*, y^*) = (0.34, 8)$, and the corresponding system reliability is 0.2875. In contrast to the ratio contest function, protecting all 8 components is not always optimal for the defender in this case, especially when x is large. For a large x, the defender has less resources to protect the components. Therefore, it chooses to concentrate its protection effort on fewer components.

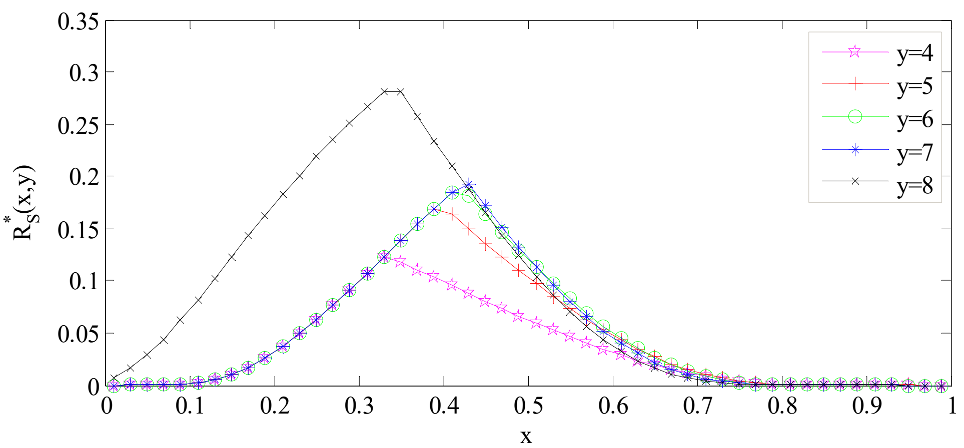


Fig. 8 Optimal (minimal) system reliability for the attacker for different x and y.

5. Influential factors in the contest

This section shows the influence of different parameters on the optimal defense and attack strategies shown in Section 4. In particular, we focus on the impacts of the relative robustness of the common bus, the contest intensity and the redundancy level of the system.

5.1 Relative robustness of the common bus and the components

Given fixed resources, the defender can spare more resources on protecting the components if the common bus is robust. Conversely, the defender has to spend more resources on protecting the common bus if it is prone to failure. This section investigates the influence of the internal-cause failure probability of the component p, the internal-cause failure probability of the common bus p_{bus} and the relative expense of the unit attacking effort for the common bus A_{bus}/a_{bus} on the optimal defense and attack strategies.

Again, consider the system with $n = 8$, $K = 4$, $R/A = r/a = 1$, $A = 1$, $a_{bus} = a$, and with the contest function $F(e, E) = E/(e + E)$. As $A = 1$, A_{bus} quantifies the relative efficiency of attacking the common bus; in turn, it reflects the robustness of the common bus against intentional attacks. We try five different parameter settings: (i) $p^I = p^I_{bus} = 0$; (ii) $p^I = 0$, $p^I_{bus} = 0.25$; (iii) $p^I = 0.25$, $p^I_{bus} = 0$; (iv) $p^I = 0.25$, $p^I_{bus} = 0.25$; and (v) $p^I = 0.5$, $p^I_{bus} = 0.25$ for $A_{bus} \in (0.1,10)$, and derive the corresponding $(y^*, Y^*, x^*, X^*, R^*_S)$. For all these considered parameter combinations, we obtain $y^* = 8$ and $Y^* = 8$, which is not surprising when referring to the analysis in Section 4.3: it is always optimal for the defender to protect all the components and the attacker to attack all the components.

The variation of x^* (the optimal proportion of the resources allocated to protect the common bus) with respect to A_{bus} is illustrated in Fig. 9. With the increase of A_{bus}, the defender spends less on protecting the common bus as the attacker becomes less competitive in the contest over the common bus. Therefore, the defender can get an upper hand with less resources and spend more on protecting the components. For a fixed A_{bus}, x^* decreases as p^I increases, implying that the defender should spend more on protecting the components if the components are more prone to failure. The impact of p^I_{bus} on x^* is not significant, though in general x^* will decrease with respect to p_{bus}^I.

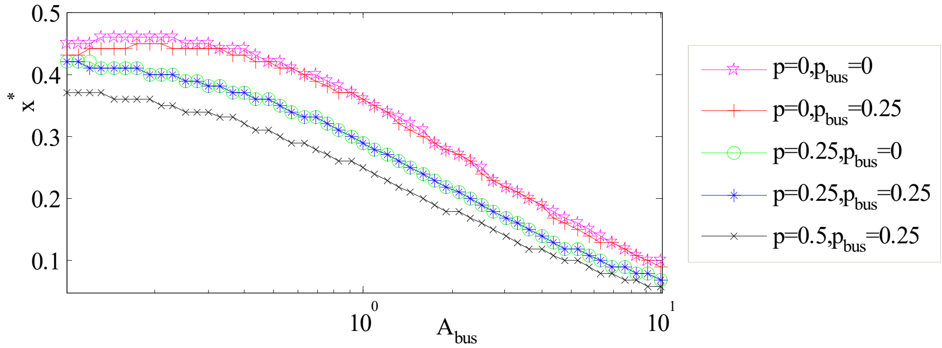


Fig. 9 Variation of the optimal x^* with respect to A_{bus} for different p^I and p_{bus}^I.

Fig. 10 shows the variation of X^* with respect to A_{bus}. Generally, X^* decreases with respect to A_{bus}, but it exhibits more significant fluctuation compared with x^*, especially for large A_{bus}. For a larger A_{bus}, it would be less efficient for the attacker to attack the common bus. Hence, it can neither increase X to gain an upper hand over the contest on the common bus, nor decrease X to cope with the increased defensive effort on the components. As a result, it struggles to balance the gains made from attacking the common bus and the components, leading to an unstable X^*.

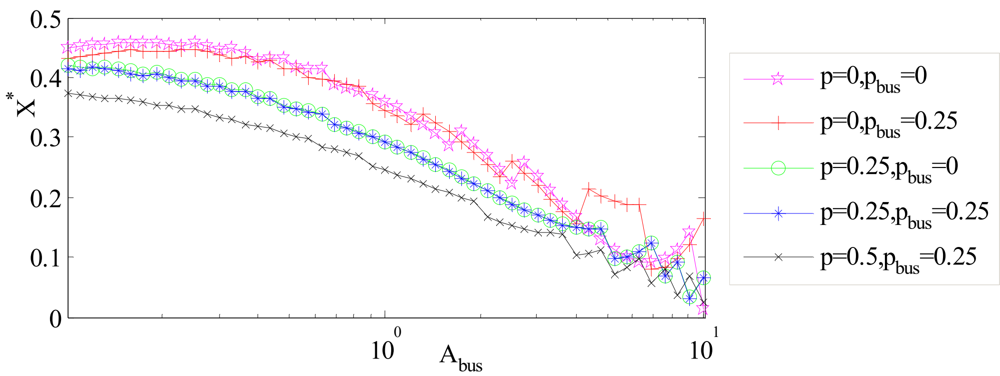


Fig. 10 Variation of the optimal X^* with respect to A_{bus} for different p^I and p_{bus}^I.

Fig. 11 shows the variation of R_S^* with respect to A_{bus}. The system reliability R_S^* decreases monotonically with respect to p^I and p_{bus}^I, and increases monotonically with respect to A_{bus}. However, the improvement of R_S^* becomes less significant after A_{bus} exceeds a certain level. In this case, the defender can easily get the upper hand in the contest over the common bus, and both the defender and the attacker shift their attention to the contest over the components. Similar situations occur when A_{bus} is very small, resulting in an S-shaped R_S^* with respect to A_{bus}.

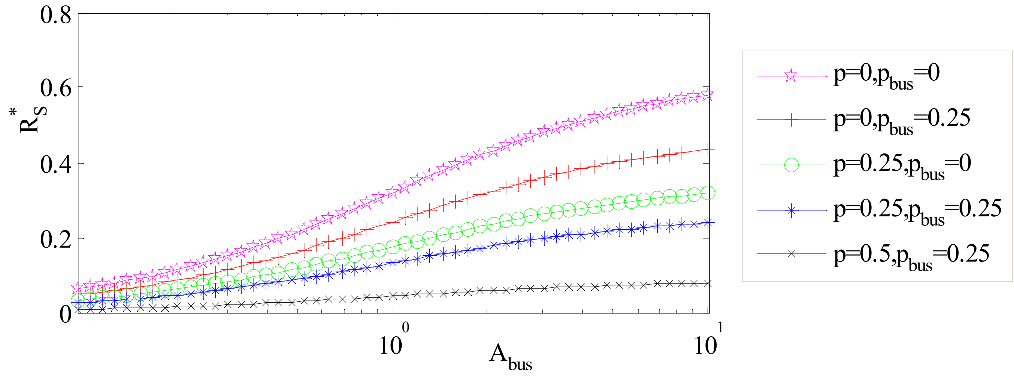
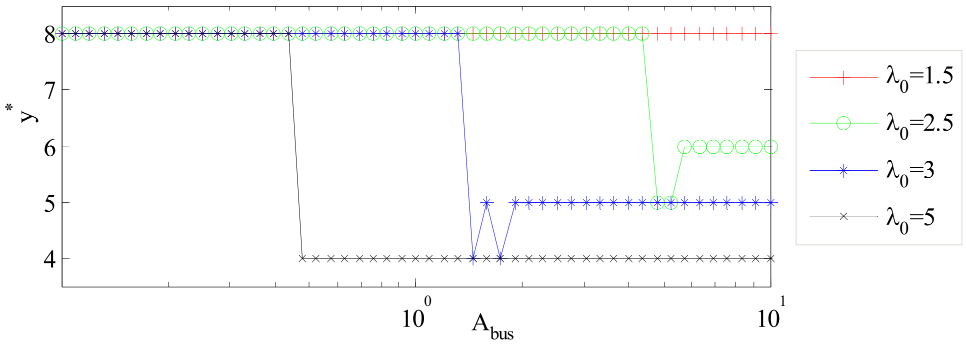


Fig. 11 Variation of R_S^* with respect to A_{bus} for different p^I and p_{bus}^I.

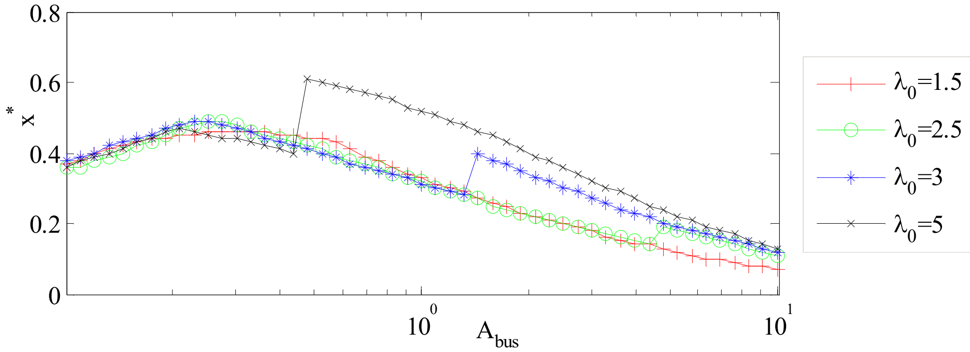
5.2 Contest intensity

As previously mentioned, the destruction probabilities of the common bus and the components vary mildly for a small contest intensity, especially when the two competitors spend comparative resources. In contrast, when the contest intensity increases, one competitor may easily get the upper hand by spending slightly more resources, and the optimal defense and attack strategies may vary significantly. With the same parameter setting, this section studies the influence of the contest intensity.

Unlike in the low contest intensity cases, the defender has to concentrate its effort on protecting fewer components with the increase of λ_0, especially when A_{bus} is large, as shown in Fig. 12 (a). On one hand, the defender gains an advantage over the attacker in the contest over the common bus when A_{bus} increases. Therefore, it can spare more resources on protecting the components. This explains the trend that x^* decreases as A_{bus} increases. On the other hand, the defender would choose to protect fewer components so that it can increase the investment on the common bus while maintaining the survivability of the protected components. This explains the drop of y^* in Fig. 12 (a) and the jump of x^* in Fig. 12 (b). Nevertheless, the defender will not protect fewer than $K = 4$ components.



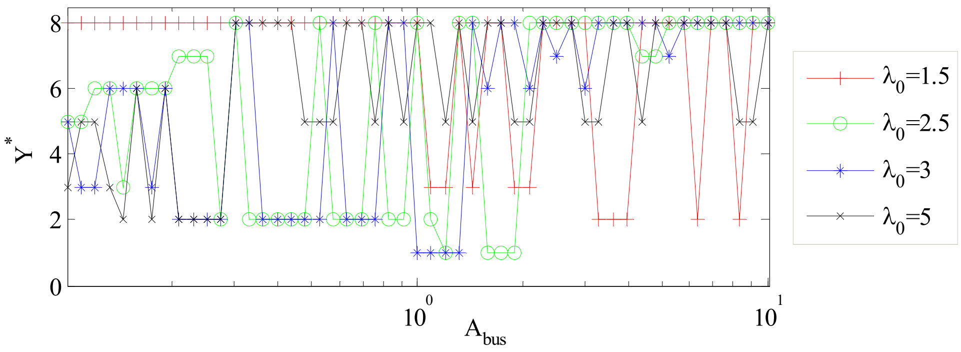
(a) Optimal number of protected components y^*.



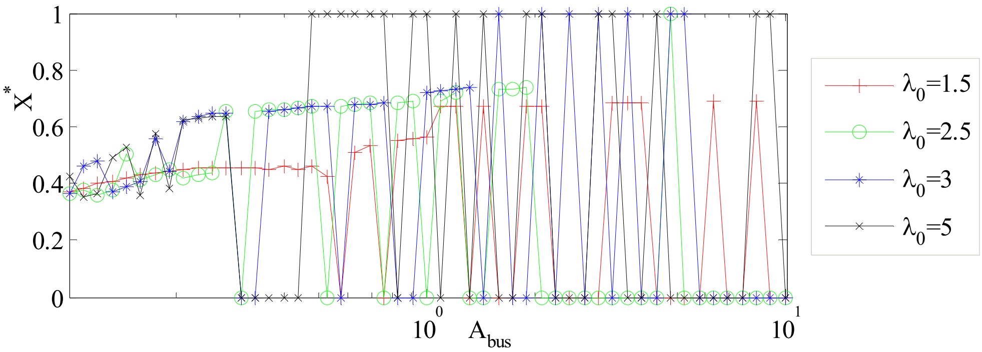
(b) Optimal proportion of resources allocated to protect the common bus x^*.

Fig. 12 Variation of the optimal defense strategy (y^*, x^*) with respect to A_{bus} for different λ_0.

Compared with the defense strategy, the variation of the attack strategy is more complicated, as shown in Fig. 13. For small λ_0 ($\lambda_0 = 1.5$), the attack strategy changes mildly when A_{bus} is small but fluctuates significantly when A_{bus} becomes large. Nevertheless, both Y^* and X^* fluctuate more significantly for $\lambda_0 = 1.5$ compared with the case $\lambda_0 = 1$ (referring to the previous section). As the contest intensity increases ($\lambda_0 = 2.5, 3, 5$), the attack strategy becomes more sensitive to A_{bus}, even when A_{bus} is small. Particularly, for a large A_{bus} when the defender leaves some components unprotected, the attacker would either spend almost all of its resources on attacking the common bus or all its resources on attacking the components. Hence, the contest intensity λ_0 increases the sensitivity of the optimal attack strategy to parameter A_{bus}.



(a) Optimal number of components to attack Y^*.



(b) Optimal proportion of resources allocated to attack the common bus X^*.

Fig. 13 Variation of the optimal attack strategy (Y^*, X^*) with respect to A_{bus} for different λ_0.

The variation of the system reliability is shown in Fig. 14. Apparently, when the attacker takes the upper hand in the contest over the common bus (i.e., when A_{bus} is small), the system reliability decreases as the contest intensity λ_0 increases. In contrast, the system reliability increases with the increase of λ_0 when the defender takes the upper hand in the contest over the common bus. Thus, the contest intensity λ_0 enlarges the advantage of competitors in the defense and attack contest, which is consistent with its definition.

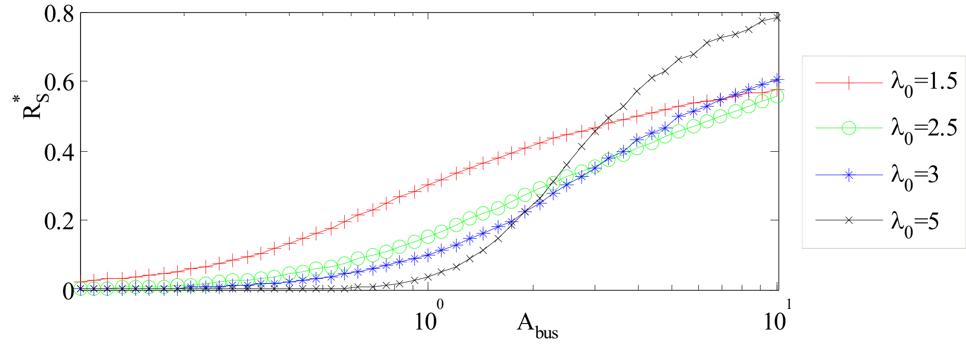
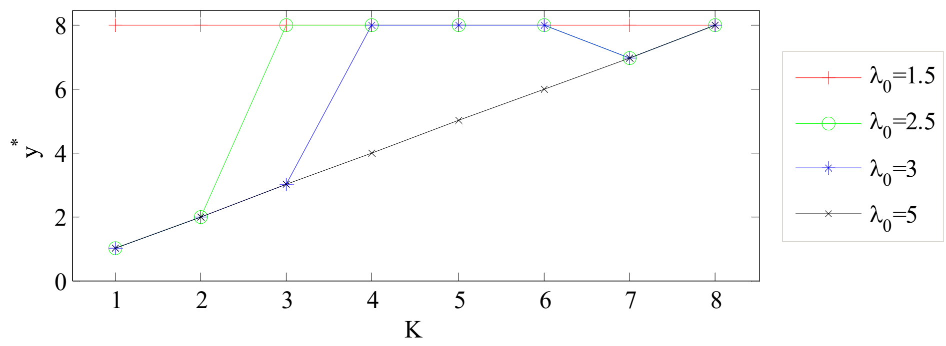


Fig. 14 Variation of R_S^* with respect to A_{bus} for different λ_0 .

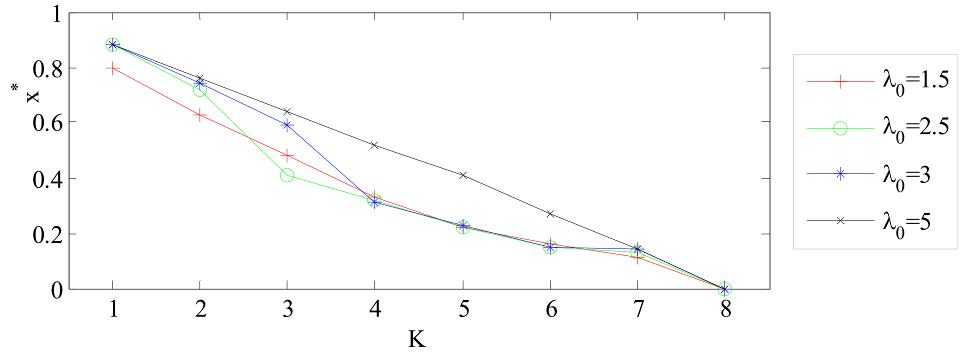
5.3 System redundancy

A significant factor that influences the system reliability is the system redundancy level. In the common bus system, the system has $(n-K)$ redundant components when the common bus functions. This section investigates the variation of the defense and attack strategies with respect to. K.

Fig. 15 shows the variation of the defense strategy with respect to K for different λ_0. For a small λ_0 ($\lambda_0 = 1.5$), the defender chooses to protect all the components. As none of the two competitors can gain a significant advantage over the other by spending slightly more resources, protecting all components can improve the survivability of the whole system. When the contest intensity λ_0 is large, the attacker can easily gain a significant advantage over the defender by spending slightly more resources. Therefore, the defender has to protect fewer components to keep the survivability of the whole system. In any case, the proportion x^* decreases with K, and decreases to 0 when $K = 8$. In this case, the performance-sharing among different components does not work (due to the limited capacity of the common bus or the limited surplus performance of each component), and there is no need to protect the common bus.



(a) Optimal number of protected components y^*.

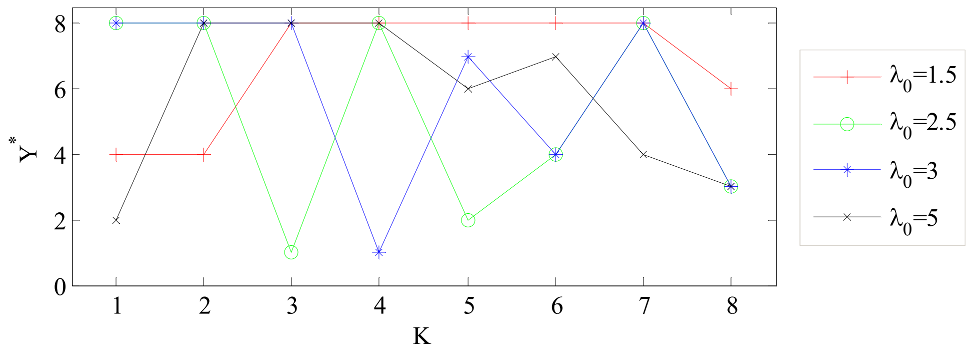


(b) Optimal proportion of resources allocated to protect the common bus x^*.

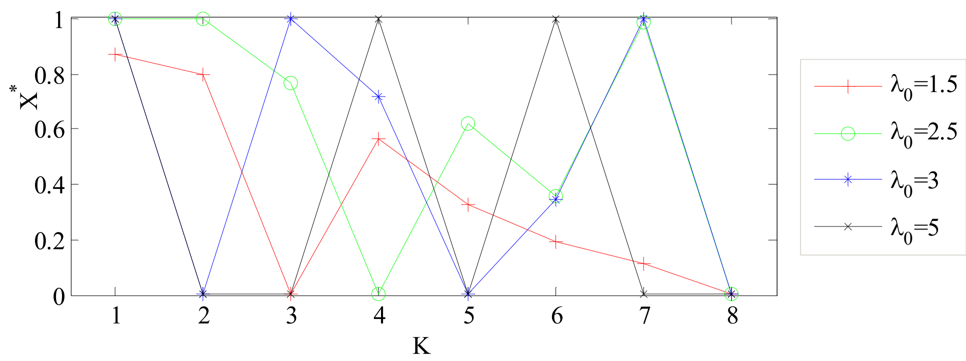
Fig. 15 Variation of the optimal defense strategy (y^*, x^*) with respect to K for different λ_0.

Fig. 16 shows the variation of the optimal attack strategy, which is more complex and intractable. It is useful to note that the attacker tends to spend either almost all of its resources or none of its resources on protecting the common bus, especially when λ_0 is large. This reveals the importance of the common bus in the contest over the whole system, and the attacker is quite sensitive to the system configurations. Nevertheless, when $K = 8$, the attacker would definitely spend all of its resources on attacking the components, as the common bus is useless in the system.

Fig. 17 illustrates the variation of R_S^* with respect to K for different λ_0. The system reliability decreases with λ_0 for fixed K, implying that the defender is at a disadvantage in the contest (referring to the discussion in the preceding section that λ_0 enlarges the advantage). Moreover, R_S^* decreases more rapidly with K for large λ_0. This reveals the importance of redundancy and the common bus in the system, especially in a fierce contest with large λ_0.



(a) Optimal number of components to attack Y^*.



(b) Optimal proportion of resources allocated to attack the common bus X^*.

Fig. 16 Variation of the optimal attack strategy (y^*, x^*) with respect to K for different λ_0.

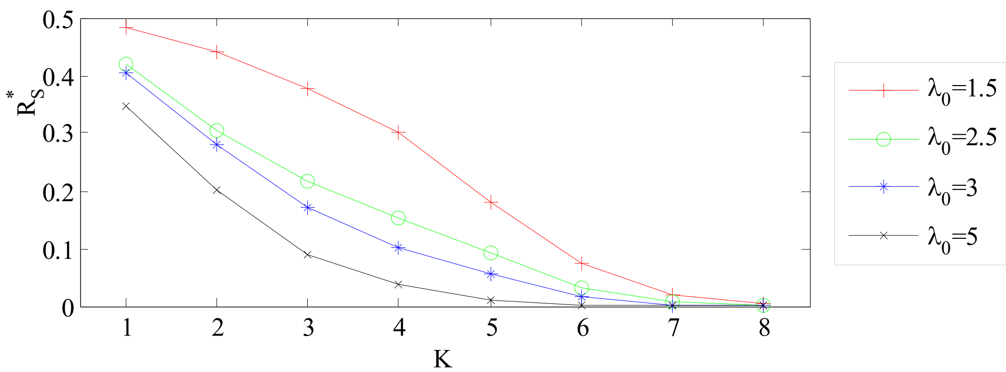


Fig. 17 Variation of R_S^* with respect to K for different λ_0.

6. Conclusions

Performance sharing among different components is common for many infrastructure systems. This paper focused on the defense and attack of the common bus performance-sharing system under intentional attacks. We investigated the optimal defense and attack strategies in a two-stage min-max game framework.

We first constructed the framework to allow us to study the optimal defense and attack strategies of general common bus systems. We then focused on a special common bus system with identical components. The optimal number of components to protect/attack was analyzed under mild assumptions, and it is optimal for the defender/attacker to protect/attack all the components when its competitor distributes its resources evenly among all the components. We revealed the impact of different contest functions on the optimal defense and attack strategies. The influences of the relative robustness of the common bus, the contest intensity, and the system redundancy level on the optimal defense and attack strategies were investigated. It was shown that the defender would spend less on the common bus when the common bus is robust or the redundancy is low for a small contest intensity. However, when the contest intensity increases, both the optimal defense and attack strategies become more sensitive to the change of the system parameters.

In this paper, it is assumed that the attacker knows the defender's resource allocation. In future research, it would be interesting to study the defense of common bus systems under other assumptions, such as where neither the attacker nor the defender knows its competitor's strategy. Another direction for future research would be to extend this research to the case where the performance sharing is possible only among a part of the components, instead of all of them.

Acknowledgments

The authors would like to thank the editor and the anonymous referees for their constructive comments, which considerably helped improve the original manuscript. This work was partially supported by the NSFC under Grant 71231001, 71301009, 71420107023, and the Fundamental Research Funds for the Central Universities under FRF-TP-15-031A3 and FRF-BR-15-001B.

Appendix A

R_1 in Eq. (4) and (5) can be rewritten as

$$R_1 = P_i G_{-i,1} + (1 - P_i) H_{-i} = P_i \left(G_{-i,1} - H_{-i}\right) + H_{-i} = P_i G_{-i} + H_{-i},$$

where $G_{-i,1}$ is the conditional system reliability given that component i fails and the common bus is operating, H_{-i} is the conditional system reliability given that both i and the common bus are operating, and $G_{-i} = G_{-i,1} - H_{-i}$. Obviously, $G_{-i,1} < H_{-i}$ and $G_{-i} < 0$. Therefore, the system reliability in Eq. (5) can be rewritten as

$$R_S = (1 - P_i) P_{bus} \prod_{j=1, j \neq i}^{n} \left(1 - P_j\right) + (1 - P_{bus})(P_i G_{-i} + H_{-i})$$

$$= P_{bus} \prod_{j=1, j \neq i}^{n} \left(1 - P_j\right) + (1 - P_{bus}) H_{-i} + P_i \left((1 - P_{bus}) G_{-i} - P_{bus} \prod_{j=1, j \neq i}^{n} \left(1 - P_j\right) \right),$$

where $(1 - P_{bus}) G_{-i} - P_{bus} \prod_{j=1, j \neq i}^{n} \left(1 - P_j\right) < 0$. As P_i is a non-increasing function of e and a non-decreasing function of E, it can be easily verified that R_S is a non-decreasing function of $e_i, i = 1, \dots, n$, and a non-increasing function of $E_i, i = 1, \dots, n$. In addition, if the contest function $F(e, E)$ is convex about e and concave about E, then R_S is also convex about e_i and concave about E_i. The same result can be derived for e_{bus} and E_{bus}. Therefore, the problems in Eq. (6) and (7) are of a convex nature. It should be mentioned that $F(e, E) = E^{\lambda_0} / (E^{\lambda_0} + e^{\lambda_0})$ is convex about e and concave about E for $\lambda_0 \leq 1$.

Appendix B

Consider $h(Y) \triangleq \ln[(1 - P_Y)^Y] = Y\left(\ln(1 - p^I) - \ln\left(\rho Y^{-\lambda_0} + 1\right)\right)$, we have

$$\frac{dh(Y)}{dY} = \ln(1 - p^I) - \ln\left(\rho Y^{-\lambda_0} + 1\right) + \frac{\lambda_0 \rho Y^{-\lambda_0}}{\rho Y^{-\lambda_0} + 1},$$

and

$$\frac{d^2 h(Y)}{dY^2} = \frac{\lambda_0 \rho Y^{-\lambda_0 - 1}}{\left(\rho Y^{-\lambda_0} + 1\right)^2} \left(\rho Y^{-\lambda_0} + 1 - \lambda_0\right).$$

Clearly, $\frac{d^2 h(Y)}{dY^2} > 0, \forall Y > 0$ for $\lambda_0 \leq 1$, and $\frac{dh(Y)}{dY} \to \ln(1 - p^I) < 0$ as $Y \to +\infty$.

Therefore, $\frac{dh(Y)}{dY} < 0, \forall Y > 0$ and both $h(Y)$ and $(1 - P_Y)^Y$ are decreasing with respect to Y for $\lambda_0 \leq 1$.

References

Azaiez, M. N., & Bier, V. M. (2007). Optimal resource allocation for security in reliability systems. *European Journal of Operational Research, 181*, 773–786.

Bier, V. M., & Abhichandani, V. (2002). Optimal allocation of resources for defense of simple series and parallel systems from determined adversaries. In *The Engineering Foundation Conference on Risk-based decision making in water resources X* (pp. 59–76). Santa Barbara, CA: American Society of Civil Engineers.

Bier, V. M., & Kosanoglu, F. (2015). Target-oriented utility theory for modeling the deterrent effects of counterterrorism. *Reliability Engineering & System Safety, 136*, 35–46.

Bier, V. M., Nagaraj, A., & Abhichandani, V. (2005). Protection of simple series and parallel systems with components of different values. *Reliability Engineering & System Safety, 87*, 315–323.

Deck, C., Foster, J., & Song, H. (2015). Defense against an opportunistic challenger: Theory and experiments. *European Journal of Operational Research, 242*, 501–513.

Dighe, N. S., Zhuang, J., & Bier, V. M. (2009). Secrecy in defensive allocations as a strategy for achieving more cost-effective attacker deterrence. *International Journal of Performability Engineering, 5*, 31–43.

Golalikhani, M., & Zhuang, J. (2011). Modeling arbitrary layers of continuous-level defenses in facing with strategic attackers. *Risk Analysis, 31*, 533–547.

Haphuriwat, N., & Bier, V. M. (2011). Trade-offs between target hardening and overarching protection. *European Journal of Operational Research, 213*, 320–328.

Hausken, K. (2005). Production and conflict models versus rent-seeking models. *Public Choice, 123*, 59–93.

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

Hausken, K. (2008a). Strategic defense and attack for reliability systems. *Reliability Engineering & System Safety, 93*, 1740–1750.

Hausken, K. (2008b). Strategic defense and attack for series and parallel reliability systems. *European Journal of Operational Research, 186*, 856–881.

Hausken, K. (2013). Combined series and parallel systems subject to individual versus overarching defense and attack. *Asia-Pacific Journal of Operational Research, 30*, 1250056.

Hausken, K. (2014). Individual versus overarching protection and attack of assets. *Central European Journal of Operations Research, 22*, 89–112.

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

Hausken, K., & Levitin, G. (2012). Review of systems defense and attack models. *International Journal of Performability Engineering, 8*, 355–366.

Hausken, K., & Zhuang, J. (2012). The timing and deterrence of terrorist attacks due to exogenous dynamics. *Journal of the Operational Research Society, 63*, 726–735.

Kong, Y., & Ye, Z. S. (2016). A cumulative-exposure-based algorithm for failure data from a load-sharing system. *IEEE Transactions on Reliability, 65*, 1001–1013.

Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and*

Uncertainty, 26, 231–249.

Levitin, G. (2005). *The universal generating function in reliability analysis and optimization*. London: Springer.

Levitin, G. (2007). Optimal defense strategy against intentional attacks. *IEEE Transactions on Reliability, 56*, 148–157.

Levitin, G. (2011). Reliability of multi-state systems with common bus performance sharing. *IIE Transactions, 43*, 518–524.

Levitin, G., & Hausken, K. (2008). Protection vs. redundancy in homogeneous parallel systems. *Reliability Engineering & System Safety, 93*, 1444–1451.

Levitin, G., & Hausken, K. (2009). False targets efficiency in defense strategy. *European Journal of Operational Research, 194*, 155–162.

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

Levitin, G., & Hausken, K. (2012). Individual versus overarching protection against strategic attacks. *Journal of the Operational Research Society, 63*, 969–981.

Levitin, G., Hausken, K., & Dai, Y. (2014). Optimal defense with variable number of overarching and individual protections. *Reliability Engineering & System Safety, 123*, 81–90.

Lisnianski, A., & Ding, Y. (2009). Redundancy analysis for repairable multi-state system by using combined stochastic processes methods and universal generating function technique. *Reliability Engineering & System Safety, 94*, 1788–1795.

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*, 200–210.

Nikoofal, M. E., & Zhuang, J. (2015). On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness. *European Journal of Operational Research, 246*, 320–330.

Paulson, E. C., Linkov, I., & Keisler, J. M. (2016). A game theoretic model for resource allocation among countermeasures with multiple attributes. *European Journal of Operational Research, 252*, 610–622.

Peng, R., Guo, L., Levitin, G., Mo, H., & Wang, W. (2014). Maintenance versus individual and overarching protections for parallel systems. *Quality Technology and Quantitative Management, 11*, 353–362.

Peng, R., Levitin, G., Xie, M., & Ng, S. H. (2011). Optimal defence of single object with imperfect false targets. *Journal of the Operational Research Society, 62*, 134–141.

Peng, R., Liu, H., & Xie, M. (2016). A study of reliability of multi-state systems with two performance sharing groups. *Quality and Reliability Engineering International*, in press.

Ramirez-Marquez, J. E., Rocco S, C. M., & Levitin, G. (2009). Optimal protection of general source-sink networks via evolutionary techniques. *Reliability Engineering & System Safety, 94*, 1676–1684.

Skaperdas, S. (1996). Contest success functions. *Economic Theory, 7*, 283–290.

Tullock, G. (1980). Efficient rent seeking. In J. M. Buchanan, R. D. Tollison & G. Tullock (Eds.), *Toward a theory of the rent-seeking society*. College Station, Texas: Texas A&M University Press.

Ushakov, I. (1987). Optimal standby problems and a universal generating function. *Soviet Journal of Computer Systems Science, 25*, 79–82.

Xiao, H., & Peng, R. (2014). Optimal allocation and maintenance of multi-state elements in series-parallel systems with common bus performance sharing. *Computers & Industrial Engineering, 72*, 143–151.

Xiao, H., Shi, D., Ding, Y., & Peng, R. (2016). Optimal loading and protection of multi-state systems considering performance sharing mechanism. *Reliability Engineering & System Safety, 149*, 88–95.

Ye, Z., Li, Z., & Xie, M. (2010). Some improvements on adaptive genetic algorithms for reliability-related applications. *Reliability Engineering & System Safety, 95*, 120–126.

Ye, Z., Revie, M., & Walls, L. (2014). A load sharing system reliability model with managed component degradation. *IEEE Transactions on Reliability, 63*, 721–730.

Yu, H., Yang, J., & Mo, H. (2014). Reliability analysis of repairable multi-state system with common bus performance sharing. *Reliability Engineering & System Safety, 132*, 90–96.

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

Zhang, C., Ramirez-Marquez, J. E., & Wang, J. (2015). Critical infrastructure protection using secrecy-A discrete simultaneous game. *European Journal of Operational Research, 242*, 212–221.

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

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