European Journal of Operational Research 256 (2017) 962–975

Contents lists available at ScienceDirect

European Journal of Operational Research

journal homepage: www.elsevier.com/locate/ejor

Innovative Applications of O.R.

Defense and attack of performance-sharing common bus systems

Qingqing Zhai[a,1], Zhi-Sheng Ye[a,*], 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, Manchester, UK

ARTICLE INFO

Article history:
Received 27 October 2015
Accepted 27 June 2016
Available online 15 July 2016

Keywords:
Game theory
Common bus
Performance sharing
Defense and attack

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.

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.

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, in press; 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. Hausken (2006), Kunreuther and Heal (2003), 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

[*] Corresponding author. Tel.: +65 6601 2303.
E-mail addresses: zhaiqing59@126.com (Q. Zhai), iseyez@nus.edu.sg (Z.-S. Ye).
[1] Tel.: +65 94678450.

http://dx.doi.org/10.1016/j.ejor.2016.06.059

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 ($D_i \le C_i$)
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, $\sum_{i=1}^{n} e_i a_i + e_{bus} a_{bus} \le r$
R	Budget of the attacker, $\sum_{i=1}^{n} E_i A_i + E_{bus} A_{bus} \le R$
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

studies assume that one defender protects the whole system, such as in Azaiez and Bier (2007), Bier, Nagaraj, and Abhichandani (2005), 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, M., & 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,

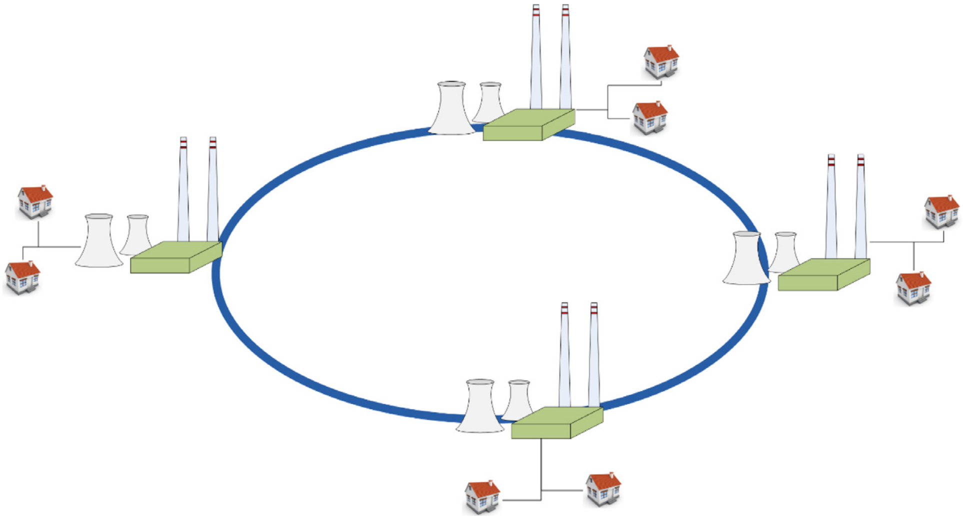

Fig. 1. The power system with a performance-sharing common bus.