European Journal of Operational Research 000 (2016) 1–15

Contents lists available at ScienceDirect

European Journal of Operational Research

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

Production, Manufacturing and Logistics

An analytical approach to the protection planning of a rail intermodal terminal network

Hassan Sarhadi[a], David M. Tulett[a], Manish Verma[b,*]

[a] Faculty of Business Administration, Memorial University of Newfoundland, Canada
[b] DeGroote School of Business, McMaster University, Canada

ARTICLE INFO

Article history:
Received 5 January 2015
Accepted 16 July 2016
Available online xxx

Keywords:
(O) Transportation
(T) Logistics
Mixed-integer program
Fortification
Decomposition heuristic

ABSTRACT

Rail-truck intermodal transportation has experienced remarkable growth over the past three decades, and plays a vital role in the freight transportation system in North America. Hence, a crucial issue is to guarantee continuity of service and to minimize the adverse impacts following disruption, natural or man-made. We make the first attempt to develop an analytical framework that could be used by rail intermodal owners to determine the best fortification plan in order to minimize the impact of a worst-case attack. The complexity of the resulting tri-level mathematical model motivated the development of a decomposition-based heuristic solution technique, and the resulting analytical approach was used to solve and analyze problem instances generated using the realistic infrastructure of a railroad operator.

1. Introduction

Intermodal transportation, defined as the transportation of goods by a sequence of at least two different modes, continues to be one of the dominant segments of the transportation industry. This has been attributed to the competitive pressures on global supply chains (Szyliowicz, 2003), the increasing demand for new service patterns driven by ocean carriers (Stone, 1997), as well as the globalization of industry (Rondinelli & Berry, 2000). Rail-truck intermodal transportation, which exploits the accessibility advantage of trucks and the scale economies of railroads, has experienced phenomenal growth over the past three decades. The most recent statistics indicate that railroad intermodal traffic, measured in ton-miles, increased by 254 percent between 1993 and 2007 (DOT, 2010), and became the largest revenue segment for the railroad industry (AAR, 2014a; Hatch, 2014). Rail-truck combination is attractive, in part, for three reasons: first, the significant reduction in both delivery and lead-time uncertainty because of the schedule-based operation of intermodal trains (Nozick and Morlok, 1997); second, a more efficient and cost-effective overall movement ensured by combining the best attributes of the two modes (AAR, 2014b); and, third increase in fuel costs have undermined the competitiveness of long-haul trucking (Jennings & Holcomb, 2007). Furthermore, rail-truck intermodal is being promoted as the preferred transportation medium because of its role in alleviating highway congestion (Bryan, Weisbrod, & Martland, 2007), and in reducing carbon emission (Kim & Van Wee, 2014).

A significant volume of traffic transits the rail-truck intermodal transportation network, which is crucial to the economic growth of North America, and thus the associated infrastructure could be deemed *critical*, i.e., systems and assets whose destruction (or disruption) would have a crippling effect on security, economy, public health, and safety (US DHS, 2014). Disruptions could be induced by nature such as hurricane Katrina in 2005 (Mouawad, 2005), or man-made threats such as the 9/11 terrorist attacks in the United States (Scaparra & Church, 2012). One of the ways to mitigate the impact of disruption is to design supply chain infrastructure so that it operates efficiently (i.e., low cost) both normally and when a disruption occurs (Snyder, Scaparra, Daskin, & Church, 2006). Alternatively, one could ascertain the vulnerability of a critical infrastructure to failure and then develop strategies to preclude it. This paper falls under the latter domain, and proposes an analytical framework to preserve the functionality of a rail-truck intermodal transportation system given a worst-case disruption perpetuated by an intentional attack (or by natural disasters). More specifically we focus on intentional attacks on transportation system, a very real and pertinent issue reflected in the global terrorism database containing over six-thousand attacks on the transportation infrastructure, including numerous on the railroad and the highway networks (START, 2015). Furthermore, the National Counterterrorism Center, a United States government organization responsible for national and international counterterrorism efforts, notes that the proportion of accidents on transportation infrastructure has increased 34 percent since 1998 (NCTC, 2015). In an effort

* Corresponding author.
E-mail addresses: hassan.sarhadi@mun.ca (H. Sarhadi), dtulett@mun.ca (D.M. Tulett), mverma@mcmaster.ca (M. Verma).

http://dx.doi.org/10.1016/j.ejor.2016.07.036
0377-2217/

to conduct a focused investigation, we consider disruption only at the terminals and identify those crucial to the intermodal infrastructure, and then discuss different strategies to fortify them.

A tri-level defender-attacker-defender (DAD) approach is proposed, where the outermost problem belongs to the network operator with a limited budget to protect or harden some of the terminals, the middle level to the attacker with enough resources to interdict some of the un-protected terminals, and the innermost to the intermodal operator who attempts to meet demand on a reduced network. It is pertinent that intentional disruption domain received increased engagements from academics and practitioners over the last decade, starting with the work of Brown, Carlyle, Salmeron, and Wood (2005), and the subsequent contributions mostly focused on fortifying fixed facilities (such as Scaparra & Church, 2008a, 2008b). The authors made the first attempt to extend the discussion about intentional disruption of fixed facilities within a transportation context (Sarhadi, Tulett, & Verma, 2015). It is important to note that, unlike the small problem size in Sarhadi et al. (2015) that could be solved via a commercial solver, in here we are aiming to solve realistic size problem instances that challenge the capability of the existing optimization packages, and thus also propose an efficient decomposition-based solution technique. The resulting analytical framework (i.e., mixed-integer programming model and the heuristic solution technique) was used to study the rail-truck intermodal transportation system of a Class I railroad operator in North America, and the resulting analysis led to the following conclusions. First, finite resources should be spent appropriately if the post-interdiction connectivity of the rail-truck intermodal network needs to be preserved. Second, focusing on just the critical terminals will not result in optimal fortification.

The rest of the paper is organized as follows. Section 2 reviews the relevant literature, followed by the problem description and assumptions in Section 3. The analytical framework, i.e., a tri-level mixed-integer programming model and the decomposition-based solution technique, is developed in Section 4, followed by an outline of parameter estimation in Section 5. Solution and analyses of the realistic size problem instances are discussed in Section 6. Finally, conclusions, contributions and directions for future research are outlined in Section 7.

2. Literature review

Given the focus of this work on fortification and interdiction of rail-truck intermodal terminals, the relevant papers can be organized under two streams: protection and fortification planning; and, rail-truck intermodal transportation systems.

Protection and fortification planning is an enormous exercise especially given the complexity of a typical intermodal infrastructure, the interdependencies among various components (Liberatore, Scaparra, & Daskin, 2012), and the prohibitive cost. As alluded earlier, this emerging area has started receiving increased attention from researchers over the past decade, and we organize the efforts under three sub-streams: redesign of the network; protection of an existing system; and, uncertainty in protection and interdiction.

The *first* sub-stream focused on developing protection strategies by embarking on a full redesign of the network so that the system is robust to attacks. Snyder and Daskin (2005) extended the classical *p*-median and un-capacitated fixed charge location problems to account for failures of the facilities. More recently, O'Hanley and Church (2011) proposed a resilient design problem for coverage-based service systems that aims to locate a set of facilities such that the combination of initial demand coverage and the minimum coverage following a loss is maximized. Finally, Peng, Snyder, Lim, and Liu (2011) proposed a mathematical model for designing a logistics network that can perform well in pre- and post-disruption conditions.

The *second* sub-stream, seeking to avoid the huge investments associated with complete redesign of the network, focuses on protecting the pre-established systems and has witnessed most of the academic effort. A majority of the works have approached the fortification problem, within the facility location domain, as a leader-follower game (Stackelberg, 1952), in which the defender is the leader and the interdictor the follower, and are modeled as bi-level programming problems (Dempe, 2002). For expositional reasons, we review those efforts under two threads: *ascertaining criticality*; and *fortification*.

The question of ascertaining critical elements can be traced to military planning, wherein the objective was to identify the best place to disrupt or interdict an enemy's supply line. While the first peer reviewed effort was by Wollmer (1964), subsequent works have investigated the impact of interdiction of arcs in a network to minimize flow capacity (Wood, 1993) and to maximize the shortest path between a given OD pair (Israeli & Wood, 2002), and made use of a variant of the multicommodity shortest path problem to investigate the impact on revenue (Lim & Smith, 2007). Finally, Salmeron, Wood, and Baldick (2004) used a bi-level approach to identify critical components of an electrical supply system, whereas Church, Scaparra, and Middleton (2004) studied the impact of interdicting supply and emergency facilities.

The idea of finding the optimal protection plan, and not just protecting the most critical assets, has been introduced by Church and Scaparra (2007). The authors extended their median-based interdiction model by adding a layer to incorporate fortification, and then proposed solution techniques for solving the resulting bi-level programs (Scaparra & Church, 2008a, 2008b). Some recent works have considered fortification within a system of capacitated facilities (Aksen, Piyade, & Aras, 2010; Scaparra & Church, 2012). The concept of fortification against worst-case losses for infrastructure systems has been conceptually introduced in Brown et al. (2005, 2006), which uses bi-level models to represent fortification and interdiction decisions (i.e. defender-attacker framework) and tri-level models to represent fortification, interdiction, and system operating decisions, like network flow decisions (i.e., defender-attacker-defender framework). A number of applications of the proposed framework appeared in the literature such as power grid (Alguacil, Delgadillo, & Arroyo, 2014), water supply (Qiao et al., 2007), and railway infrastructure when the protection resources become available overtime (Starita & Scaparra, 2016). The last work has modeled the protection problem as a bi-level mixed integer program, and proposed two different decomposition techniques to solve them.

Finally, under the *third* sub-stream, uncertainty associated with the attacks was incorporated by attaching a probability of successful attacks on facilities (Church & Scaparra, 2007), and by making use of a probability distribution for estimating the number of facilities that could be attacked (Liberatore, Scaparra, & Daskin, 2011). Losada, Scaparra, and O'Hanley (2012) explores investment in protection measures to reduce the recovery time of the system, whereas Zhang, Zheng, Zhu, and Cai (2014) attached a probability of success measure to investigate vulnerability of a protected facility. Subsequently, the impact of imperfect information between the defender and the attacker is discussed in Zhu, Zheng, Zhang, and Cai (2013), while the need for an all hazards approach to incorporate the possibility of worst-case and random attacks simultaneously is considered in Zhuang and Bier (2007).

Rail-truck intermodal transportation systems: Although rail-truck intermodal transportation has been an active research area over the last two decades (Macharis & Bontekoning, 2004), the discussion about disruption is still in its infancy (Sarhadi et al., 2015). We invite the reader to refer to Bontekoning, Macharis, and Trip (2004) for an excellent discussion on intermodal

Please cite this article as: H. Sarhadi et al., An analytical approach to the protection planning of a rail intermodal terminal network, European Journal of Operational Research (2016), http://dx.doi.org/10.1016/j.ejor.2016.07.036