

A defender-attacker-defender approach to the optimal fortification of a rail intermodal terminal network

Hassan Sarhadi · David M. Tulett · Manish Verma

Received: 29 August 2014 / Accepted: 9 November 2014 / Published online: 22 November 2014
© Springer Science+Business Media New York 2014

Abstract A crucial issue in modern supply chains is to guarantee continuity and efficiency in the event of natural and man-made threats. This task is challenging, especially given the finite resources and the complexity of the transportation infrastructure. We make use of a defender-attacker-defender framework to determine the optimal strategy for fortifying a given number of rail-truck intermodal terminals, such that the losses (or inefficiencies) resulting from an intentional attack is minimized. The proposed tri-level optimization model, used to study a realistic size case study from published literature, is solved using three distinct solution techniques. Finally, we present some managerial insights and directions of future research.

Keywords Intermodal transportation · Intentional attacks · Fortification · Mixed-integer programming · Leader-follower · Heuristic

Introduction

Intermodal transportation, which capitalizes on the synergy between the strengths of more than one transport mode, has experienced phenomenal growth over the past two decades. 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 as well as the globalization of industry (Rondinelli and Berry 2000). Rail-truck intermodal transportation, which combines the accessibility advantage of road networks

H. Sarhadi · D. M. Tulett
Faculty of Business Administration, Memorial University, St John's, Canada

H. Sarhadi
e-mail: hassan.sarhadi@mun.ca

D. M. Tulett
e-mail: dtulett@mun.ca

M. Verma (✉)
DeGroote School of Business, McMaster University, Hamilton, Canada
e-mail: mverma@mcmaster.ca

with scale economies associated with railroads, is attractive to shippers for two 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); and, *second* a more efficient and cost-effective overall movement ensured by combining the best attributes of the two modes (AAR 2010). The most recent statistics indicate that rail-truck intermodal traffic, measured in ton-miles, increased by 254 % between 1993 and 2007 (US DOT 2010), and became the largest revenue segment for the railroad industry (Hatch 2014).

It should be evident that intermodal transportation plays a vital role in the economic growth of North America, and hence 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 Katrina and Rita in 2005 that could cripple the nation's oil refining capacity (Mouawad 2005), or man-made threats such as the 9/11 terrorist attacks in the United States (Scaparra and Church 2012). One of the ways to mitigate the impact of disruption is to design supply chain infrastructure, including dramatic and expensive changes to the initial system configuration, so that it operates efficiently (i.e., at low cost) both normally and when a disruption occurs (Snyder et al. 2006). Alternatively, one could attempt to improve the reliability of existing infrastructure by using fortification models to identify optimal strategies for allocating limited resources. This paper makes use of the latter technique to preserve the functionality of the rail-truck intermodal transportation system. More specifically, we consider disruption only at the intermodal terminals and formulate it as a tri-level problem, in which the defender (i.e., network owner) has a limited budget to protect or harden some of the terminals, an attacker has enough resources to interdict some of the un-protected terminals, and finally the defender (i.e., the intermodal operators) attempts to meet demand on a reduced intermodal network.

The rest of the paper is organized as follows. [Literature review](#) section reviews the relevant literature, followed by the problem description and assumptions in [Problem description](#) section. The tri-level mixed-integer programming model developed in [Defender-attacker-defender framework](#) section is applied to a realistic size problem instance in [Case study](#) section, which is solved using three distinct solution techniques and then analyzed to provide insights. Conclusions, contributions and directions of future research are outlined in [Conclusion](#) section.

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 It should be evident that fortification planning is an enormous exercise especially given the complexity of a typical intermodal infrastructure, the interdependencies among various components (Liberatore et al. 2012), and the prohibitive cost. This exciting area has started receiving increased attention from researchers, whose efforts are summarized next.

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 modeled as bi-level programming problems (Dempe 2002). Furthermore, it is assumed that the attacker is going to make the most disruptive decision, and hence worst-case scenarios are modeled (Scaparra and Church 2008a). To ease the complexity of the bi-level programming problems, Church and Scaparra (2007) and Scaparra and Church (2008b) proposed single-level formulations, and an explicit enumeration technique for solving the problems. Uncertainty associated with the attacks has been incorporated by attaching a probability of successful attacks on facilities (Church and Scaparra 2007), and by making use of a probability distribution for estimating the number of facilities that could be attacked (Liberatore et al. 2011). While the concept of investing protection measures to reduce the recovery time of the system has been investigated in Losada et al. (2012), fortification within a system of capacitated facilities has been recently investigated by Scaparra and Church (2012).

Peer-reviewed works on the disruption of a networked system, on the other hand, have primarily focused on the analysis of risk (i.e., identifying the most critical components of a system) through the development of interdiction models. The effect of interdiction on the maximum flow through a network is studied by Wood (1993), while Lim and Smith (2007) made use of a variant of multicommodity shortest path problem to investigate the impact on revenue from arc interdictions. The concept of fortification against worst-case losses for network models has been discussed in Brown et al. (2005, 2006), wherein a tri-level optimization model to represent fortification, interdiction, and network flow decisions (i.e., defender-attacker-defender) was developed. Finally, a number of applications making use of this framework appeared in the literature such as power grid (Salmeron et al. 2004; Alguacil et al. 2014), and water supply (Qiao et al. 2007).

Rail-truck intermodal transportation systems Although rail-truck intermodal transportation has been an active research area over the past two decades (Macharis and Bontekoning 2004), the discussion about disruption is still in its infancy. To the best of our knowledge, there is no peer-reviewed work that deals with intentional attacks within the rail-truck intermodal transportation setting. We invite the reader to refer to Bontekoning et al. (2004) for an excellent discussion on intermodal transportation, and SteadieSeifi et al. (2014) for the state of the art review.

To sum, the posed problem makes use of a defender-attacker-defender framework to investigate the optimal protection strategy for rail-truck intermodal terminals, and thus draws from the works of Scaparra and Church (2012) and Brown et al. (2005, 2006).

Problem description

In this section, we provide a formal statement of the problem, emphasize its complexity, and then state the modeling assumptions.

The protection planning of rail-truck intermodal transportation problem entails interaction amongst three players, i.e., network owner, the interdictor, and the network

operator –wherein each is in a different hierarchy (Fig. 1). At the highest level, the network owner tries to minimize the cost of using the system by fortifying a limited number of intermodal terminals. Note that this is possible only if the owner knows the cost of the worst-case attack by the interdictor, and hence the latter’s problem is a part of the former’s. Next, the interdictor wants to maximize the cost of using the system by attacking a limited number of (unprotected) terminals, which is achieved through complete information about the network operator’s problem. Finally, following interdiction, the network operator has to meet customer demand using the available intermodal terminals and (reduced) train services.

For expositional reasons, we note that a rail-truck intermodal transportation system comprises three processes: (i) inbound drayage, (ii) rail-haul, and (iii) outbound drayage. Thus, the network operator endeavours to find the minimum-cost way to satisfy customer demand, given the connections between the *available* intermodal terminals and shippers/receivers, and the pre-defined intermodal trains. In an effort to ensure feasible solutions (i.e., demand is satisfied), direct trucking is permitted between each shipper-receiver. Note that the central question about allocating limited resources such that post-disruption functionality of the intermodal infrastructure is preserved is fairly complex, in large part due to the interaction amongst the three players.

In an effort to explain the complexity of the problem, we reproduce a portion of the intermodal service chain network introduced in Verma et al. (2012), which is represented via a geographical information system (GIS) model using ArcView (ESRI 2008). Figure 2 depicts the 18 intermodal terminals, which are the access points for 399 demand pairs (i.e., shipper-receiver). These terminals are connected by a total of 62 types of intermodal train services differentiated by route and intermediate stops, i.e., 31 trains of *regular* type, and another 31 of *express* type that is 25 % faster. Finally, the network owner has resources to fortify a limited number of terminals, the interdictor has resources of destroy/ disrupt a limited number of (un-protected) terminals, and the network operator has to meet demand using the reduced intermodal network.

We now turn to our modeling assumptions: *first*, a protected terminal cannot be interdicted; *second*, each intermodal terminal has finite traffic handling capacity; *third*, delivery dates are specified when placing the order, and a penalty is incurred for late deliveries; *fourth*, there is no congestion at the terminals; *fifth*, if an intermediate terminal associated with an intermodal train service is interdicted, the train can still serve the remaining terminals on its route; and *sixth*, an interdicted terminal cannot be used as either origin or destination for any shipment.

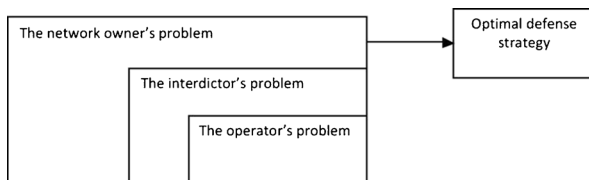


Fig. 1 Hierarchical structure for the protection planning



Fig. 2 Intermodal rail services (source: Verma et al. 2012)

Defender-attacker-defender framework

In this section, we provide the a tri-level mathematical formulation for the managerial problem and then discuss the estimation of the basic parameters of the model in [Estimation of parameters](#) section.

Mathematical model

Our notation and the model (**P**) is provided below.

Sets

- I Set of shippers, indexed by i
- J Set of receivers, indexed by j
- M_{ij} Set of intermodal paths between shipper i and receiver j , indexed by m
- K Set of intermodal terminals in the network, indexed by k
- M_{ij}^k Set of intermodal paths between shipper i and receiver j which uses intermodal terminal k
- V Set of intermodal train services defined on the network, indexed by v
- R^v Set of service legs for train service v , indexed by r
- $S^{r,v}$ Set of intermodal paths using service leg r of train service v

Variables

- x_{ij}^m Number of containers using intermodal path m between shipper i and receiver j
- xt_{ij} Number of containers using direct trucking service between shipper i and receiver j
- n^v Number of trains of type v

$$z_k = \begin{cases} 1 & \text{if terminal } k \text{ is protected} \\ 0 & \text{otherwise} \end{cases}$$

$$y_k = \begin{cases} 1 & \text{if terminal } k \text{ is interdicted} \\ 0 & \text{otherwise} \end{cases}$$

Parameters

- w Maximum number of terminals that the network owner can protect
- q Maximum number of terminals that the interdictor can disrupt
- c_{ij}^m Cost of transporting one container from shipper i to receiver j on intermodal path m
- ct_{ij} Cost of sending a container using truck on the shortest path from shipper i to receiver j
- t_{ij}^m Expected travel time from shipper i to receiver j on intermodal path m
- t_{ij} Delivery time using truck on the shortest path from shipper i to receiver j
- l_{ij} Delivery due date promised by shipper i to receiver j
- d_{ij} Number of containers demanded by receiver j from shipper i
- pc_{ij} Penalty cost per container per unit time to be paid by shipper i to receiver j
- b^v Capacity of train service v
- fc^v Fixed cost of operating train service v
- u_k Capacity of intermodal terminal k

(P)

$$\text{Min}_z C(z) \tag{1}$$

subject to:

$$\sum_{k \in K} z_k \leq w \tag{2}$$

$$z_k \in \{0, 1\} \quad \forall k \in K \tag{3}$$

where,

$$C(z) = \text{Max}_y C(y) \tag{4}$$

subject to:

$$\sum_{k \in K} y_k \leq q \tag{5}$$

$$y_k \in \{0, 1\} \quad \forall k \in K \tag{6}$$

$$y_k + z_k \leq 1 \quad \forall k \in K \tag{7}$$

where,

$$C(y) = \text{Min} \left[\sum_{i \in I} \sum_{j \in J} \sum_{m \in M_{ij}} c_{ij}^m x_{ij}^m + \sum_{i \in I} \sum_{j \in J} ct_{ij} x_{t_{ij}} \right. \tag{8}$$

$$+ \sum_{i \in I} \sum_{j \in J} \sum_{\substack{m \in M_{ij} \\ t_{ij}^m > l_{ij}}} (t_{ij}^m - l_{ij}) pc_{ij} x_{ij}^m + \sum_{i \in I} \sum_{\substack{j \in J \\ t_{ij} > l_{ij}}} \\ \left. (t_{ij} - l_{ij}) pc_{ij} x_{t_{ij}} + \sum_{v \in V} f c^v n^v \right]$$

subject to:

$$\sum_{m \in M_{ij}} x_{ij}^m + x_{t_{ij}} = d_{ij} \quad \forall i \in I, \forall j \in J \tag{9}$$

$$\sum_{i \in I} \sum_{j \in J} \sum_{m \in M_{ij} \cap M_{ij}^k} x_{ij}^m \leq u_k \quad \forall k \in K \tag{10}$$

$$\sum_{i \in I} \sum_{j \in J} \sum_{m \in M_{ij} \cap S^{r,v}} x_{ij}^m \leq b^v n^v \quad \forall v \in V, r \in R^v \tag{11}$$

$$x_{ij}^m \leq \varnothing (1 - y_k) \quad \forall i \in I, \forall j \in J, \forall k \in K, \forall m \in M_{ij} \cap M_{ij}^k \tag{12}$$

$$n^v \geq 0, \text{ integer} \quad \forall v \in V \tag{13}$$

$$x_{ij}^m \geq 0, \text{ integer} \quad \forall i \in I, \forall j \in J, \forall m \in M_{ij} \tag{14}$$

$$x_{t_{ij}} \geq 0, \text{ integer} \quad \forall i \in I, \forall j \in J \tag{15}$$

\varnothing is a larger positive integer

(P) depict the tri-level optimization model that could be used to make protection planning decision. The *outer* level problem belongs to the network owner whose objective is to minimize total cost by fortifying a given number of intermodal terminals. Constraints sets (3) enforce the binary nature of the terminal fortification decision. The *middle* level problem belongs to the interdictor who intends to maximize the total cost of using the system. Constraints sets (5) depict the finite resources available for interdiction or disruption of intermodal terminals, whereas (6) represents the binary nature of the interdiction decisions. Constraints sets (7) combine the decisions of the network owner and the interdictor by prohibiting the disruption of fortified terminals.

Finally, the *inner* level problem belongs to the network operator who intends to minimize the total cost of using the system. Note that this is a variant of the multi-commodity flow problem with capacity, delivery time, and penalty cost considerations. The objective function, i.e., (8), will capture the overall cost of moving shipments using the rail-truck intermodal option, any direct trucking service if applicable, the penalty costs for late deliveries, and the fixed cost of running different intermodal trains in the network. Constraints sets (9) ensure the demand is satisfied either using the intermodal option or through direct truck service. Constraints sets (10) enforce the capacity at various terminals in the network. Constraints sets (11) determine the number of intermodal trains of a specific type needed in the network. Constraints sets (12) link the interdicator's problem with the network operators, and states that the interdicted terminals cannot be a part of different intermodal paths to meet demand. Note that \emptyset is a large positive integer. Finally, the sign restrictions are imposed through constraints sets (13) to (15).

Estimation of parameters

Cost In the United States, trucks can travel at a maximum speed of 50 miles/h, but due to lights and traffic an average speed of 40 miles/h is assumed (Verma and Verter 2010). Normally drayage is charged in terms of the amount of time the crew (driver-truck) is engaged, and an estimate of \$300/hour including the estimated hourly fuel cost is used. A penalty cost of \$40 per hour per container was used. As indicated there are two types of intermodal train services viz. *regular* and *express*. Average intermodal train speed was calculated using the Railroad Performance Measure website (RPM 2014), and was estimated to be 27.7 miles/h for *regular*, and 36.8 miles/h for *express* service. Consistent with the published works, we estimated a rate of \$0.875/mile for *regular* and \$1.164/mile for *express* service. The hourly fixed cost of running a *regular* intermodal train is \$500 per hour, which takes into consideration the hourly rates for a driver, an engineer, a brakeman, and an engine, which are \$100, \$100, \$100, and \$200, respectively. The *express* service is 50 % more expensive at \$750 per hour (Verma 2012).

Due dates Three different due dates have been defined: *long*, *regular*, and *short*. The distance (d in miles) between each shipper and each receiver was estimated in ArcView GIS (ESRI 2008). Next, the travel time (in hours) was computed as $d/40$, where the denominator indicates the speed of trucks. Finally, constants of 10, 15 and 20 were added to the travel time to, respectively, get the *short*, *regular* and *long* delivery due dates for each shipper-receiver pair.

Demand levels and terminal capacity The inner problem belonging to the network operator was solved in CPLEX 12.1.0 (IBM 2014) on the dataset used in Verma et al. (2012), and the solution was decoded to estimate the traffic volume through each intermodal terminal. It was estimated that the terminal utilization was 80 %, and hence the terminal capacity is 1.25 times (i.e., 1 divided by 0.8) the traffic volume through each terminal, and the demand level was deemed *medium*. Finally, we assumed that *high* demand level would account for 95 % of terminal capacity and hence multiplied the *medium* demand by 1.1875 (i.e., 95 over 80), whereas *low* demand would result from 65 % terminal capacity.

Case study

(*P*) was applied to solve the realistic size case study outlined in [Problem description](#) section, and depicted in Fig. 2. All resulting mathematical models were solved using CPLEX 12.1.0 (IBM 2014). For expositional reasons, we abbreviate the names of the terminals as indicated in Table 1. Finally, we assume that the network owner has enough resources to protect two terminals, and that the interdictor has capability to disrupt two terminals. Though evident, it is assumed that the fortification is permanent and therefore the relevant terminals cannot be interdicted subsequently. To recall, we are attempting to find the best protection strategy for the network owner.

Solution algorithms

In this section, we will first comment on the computational burden if all scenarios need to be generated, and then outline two efficient algorithms that achieve the same result. For expositional reasons, we will make use of the setting wherein demand is *low* and delivery due date is *short* to demonstrate the algorithm; we will compare the solutions resulting from the other eight scenarios in [Numerical analysis](#) section.

(*P*) can be solved using [three](#) techniques: complete enumeration; implicit enumeration proposed in Scaparra and Church (2008a); and, a traffic-based heuristic.

Complete enumeration proceeds by determining an exhaustive combination for defending and interdicting two terminals, which for our problem instance amounts into $(18\ 2) * (16\ 2) = 18360$ possible defense and attack strategies. For each defense and attack strategy, the network operator's problem is solved assuming that the terminals attacked under this strategy have been disrupted. For each given defense strategy, the effect of all the ensuing attack strategies will be compared. The worst-case disruption following each defense strategy yields the total cost associated with the adoption of that defense strategy. The defense strategy with the lowest associated cost will be selected as the best defense strategy. Applying this procedure to the current case study will result in protection of intermodal terminals in Philadelphia and in Atlanta. The CPU time for this problem setting was 902.14 s, and it ranged from 241.1 to 2063.18 s for the other eight scenarios.

It is easy to see that the complete enumeration technique will become rather cumbersome if more than two terminals have to be considered for fortification and

Table 1 Terminal legends

Terminals	Legend	Terminals	Legend	Terminals	Legend
Atlanta	Atl	Charlotte	Cha	Chicago	Chi
Cleveland	Cle	Cincinnati	Cin	Columbus	Col
Detroit	Det	Fort Wayne	FoW	Indianapolis	Ind
Jacksonville	Jac	Knoxville	Kno	Macon	Mac
New York	NY	Norfolk	Nor	Philadelphia	Phi
Pittsburgh	Pit	Richmond	Ric	Roanoke	Roa

interdiction. For example, the number of strategies requiring evaluation for “three terminals” example would be 371,280. Thus, there is a need for a more efficient solution technique.

Implicit enumeration Under this scheme, first, the list of the worst-case disruptions has been provided by examining all of the attack strategies. An exhaustive combination for interdicting two terminals for our problem instance will be translated into $\binom{18}{2} = 153$ possible attacks. Then, for each attack strategy, the network operator’s problem is solved assuming that the terminals listed under this strategy have been out of service. The resulting solution gives us the total cost associated with each attack strategy, and the worst-case disruption would result from the strategy with the highest cost. The corresponding strategy called for the interdiction of intermodal terminals in Philadelphia and in Atlanta. This information will be passed to the implicit enumeration scheme proposed in Scaparra and Church (2008a), which was coded in C# and the entire search took 76.5 s. This solution algorithm is using a considerably reduced search space collectively containing only the defense strategies that will prevent the worst-case disruption. We next provide detail on how this enumeration scheme works.

As indicated above, the worst-case disruption entails interdiction of terminals in Philadelphia (*Phi*) and Atlanta (*Atl*). Hence, fortifying either or both these terminals would preclude the worst-case disruption. The implicit enumeration scheme starts at the root node, i.e., 1, by finding the worst-case disruption without fortification (i.e., *Phi* and *Atl*). Set **O**, at each node, lists the terminals at least one of which must be protected to prevent the worst-case. For instance, at node 1, terminal *Phi* could either be fortified or not.

If *Phi* were not fortified, then the terminal at *Atl* would have to be considered for fortification (i.e., node 2). If even *Atl* is not fortified, then set **O** is empty thereby implying that none of the other fortifications can prevent the worst-case disruption, and the resulting node is fathomed (i.e., grey shade). On the other hand, if *Atl* is fortified, then the worst-case disruption is prevented, and the elements for set **O** must be updated by solving the interdiction problem with latest information (i.e., *Atl* is fortified). Thus, the updated set **O** contains *NY* and *Phi* as elements representing the most disruptive interdiction given that *Atl* is fortified. At node 3, only one fortification resource is left; we continue the search process by selecting *NY*. If *NY* is not fortified, it is possible that it is disrupted together with *Phi* thereby resulting in a fathomed node. But if it is fortified, then the interdiction problem is solved given that *NY* and *Atl* are fortified. The updated set **O** contains *Atl* and *Ric*, both of which would be interdicted thereby resulting in a cost of around \$12.2mn (i.e., dark shade).

If *Phi* were fortified, the interdiction problem is solved thereby resulting in terminals *Ind* and *Atl* in the updated set **O**. Arbitrarily selecting *Ind*, if it is fortified then the protection resources have been exhausted, and the resulting interdiction problem yields *Cha* and *Atl* terminals as the most disruptive. At the same time, no further branching is possible and the associated cost is around \$12.1mn. But if *Ind* is not fortified, then the updated set **O** only contains *Atl*. If *Atl* is not fortified, then it will be attacked together with *Ind* thereby being fathomed. On the other hand, if *Atl* is fortified, then the interdiction problem is solved again to yield *Chi* and *Ind* as the most disruptive terminals, and the associated cost is around \$11.9mn.

The CPU time for the remaining eight scenarios ranged from 16.3 to 336.24 s, which is quite good. We note that, given the definition of criticality for our problem instance, it is possible to arrive at the same solution more quickly by combining information about the traffic flow through each terminal and (an adapted version of) the implicit enumeration of Scaparra and Church (2008a).

Proposed traffic-based heuristic The proposed heuristic works in two steps. *First*, the capacitated multi-commodity flow problem for the network operator is solved (i.e., the inner level problem in **(P)**). The resulting solution is decoded and the traffic volume through each terminal is estimated thereby generating a list, in descending order, of throughput terminal traffic. Since there are enough resources to protect two terminals, fortifying the top two candidates on the list would make the worst-case disruption impossible.

In the *second* step, just like Scaparra and Church (2008a), the identity of the two terminals was supplied as input at the root node 1 in Fig. 3. If *Phi* were fortified, then we would update set **O** by including the third terminal from the list generated in step one. For instance, at node 4 in Fig. 3, *Ind* would be selected from the list without solving the interdiction problem as in Scaparra and Church (2008a). If *Ind* is fortified then the protection resources are exhausted, and we select the fourth terminal on the list generated in step one, i.e., *Cha*, which would be interdicted along with *Atl*. The process continues as outlined in Fig. 3, except that we have done away with the need to solve the interdicator’s problem at each node and simply consult the list generated in step one. This luxury has a positive bearing on the computational time, which for the given

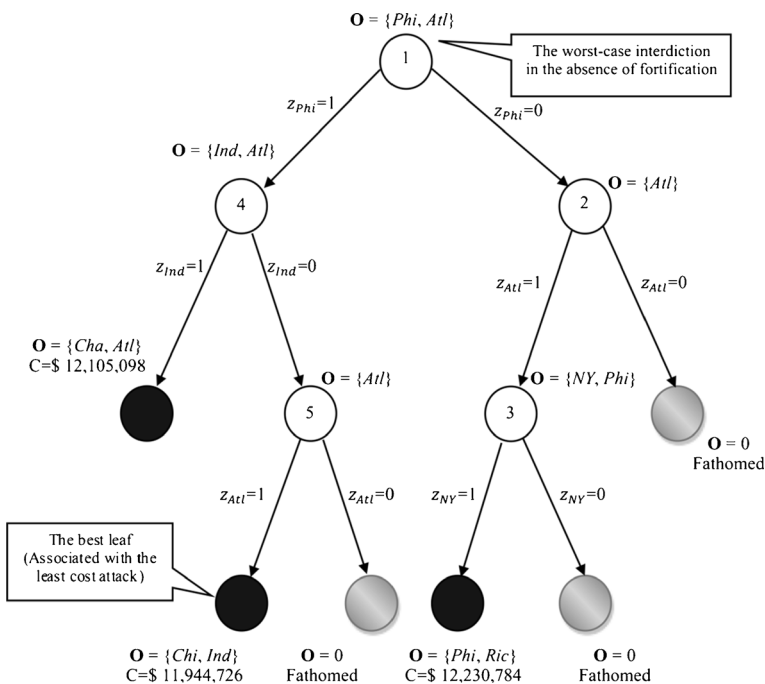


Fig. 3 Tree search (adapted from: Scaparra and Church 2008a)

problem instance was 37.86 s compared to 76.5 s using the enumeration technique of Scaparra and Church (2008a).

It is important to reiterate that the proposed traffic-based heuristic worked well for the small problem instances, but may not for much larger instances. We are currently working on a decomposition based solution technique for much larger situations, i.e., enough resources to fortify and interdict more than two terminals.

To conclude, the proposed heuristic is quicker than the other two solution techniques. Table 2 reports the relevant figures, where **BC** refers to the Base-Case, **CE** to complete enumeration, **IE** to the implicit enumeration scheme of Scaparra and Church (2008a), and **Heuristic** to the proposed traffic-based heuristic.

Numerical analysis

In this subsection, we will first provide a snapshot of the solution for the nine scenarios developed using the due date and demand level combinations as outlined in [Estimation of parameters](#) section, and then comment on terminal utilization and network connectivity.

Analysis

Following the enumeration, the resulting costs for all the leaf nodes (i.e., dark shade) were compared to conclude that the optimum strategy is to fortify *Phi* and *Atl*, which means that the interdictor would disrupt *Chi* and *Ind* and the system cost will be \$11,944,726. Table 3 summarizes the results for the nine scenarios (and twenty-seven problem instances), with the first block depicting the highlights with *short* due date and *low* demand level.

It is clear from all the nine scenarios that fortification improves the performance of the transportation system, thereby resulting in lower costs vis-à-vis no protection. In fact, for the *short* due date setting, the performance improvement ranges from 7 % for

Table 2 Snapshot of computation time

Due date	Demand level	CPU time (seconds)			
		BC	CE	IE	Heuristic
Short	Low	5.81	902.14	76.50	37.86
	Medium	7.90	1313.36	142.87	48.12
	High	1.48	260.48	17.91	9.32
Regular	Low	7.82	1362.13	123.33	49.52
	Medium	1.15	285.51	32.57	6.90
	High	1.11	243.00	16.30	7.23
Long	Low	25.31	2063.18	336.24	149.87
	Medium	1.08	241.10	26.54	7.14
	High	9.66	859.00	96.80	55.72

Table 3 Snapshot of the nine scenarios

Due date	Demand level	Cases	OFV (\$ mns)	Percent of traffic		Intermodal trains	
				Intermodal	Truck	Regular	Express
Short	Low	Base case	9.93	100	0	25	12
		W/out fort	12.84	46.22	53.78	16	6
		With fort	11.94	66.07	33.93	19	5
	Medium	Base case	10.99	100	0	26	10
		W/out fort	14.34	44.05	54.95	17	6
		With fort	13.26	66.19	33.81	19	5
	High	Base case	13.61	100	0	36	14
		W/out fort	17.80	43.18	56.82	15	8
		With fort	16.15	59.81	40.19	19	11
Regular	Low	Base case	9.67	100	0	36	0
		W/out fort	12.71	46.23	53.77	22	0
		With fort	11.78	66.08	33.92	24	0
	Medium	Base case	10.70	100	0	36	0
		W/out fort	14.20	43.05	54.95	23	0
		With fort	13.07	66.18	33.82	25	0
	High	Base case	13.26	100	0	48	3
		W/out fort	17.65	43.18	56.82	27	0
		With fort	16.18	63.82	34.18	32	1
Long	Low	Base case	9.60	100	0	36	0
		W/out fort	12.67	46.23	53.77	22	0
		With fort	11.73	66.08	33.92	24	0
	Medium	Base case	10.62	100	0	36	0
		W/out fort	14.16	45.05	54.95	24	0
		With fort	13.02	66.19	33.81	25	0
	High	Base case	13.17	100	0	48	0
		W/out fort	17.60	43.18	56.82	27	0
		With fort	16.12	65.82	34.18	33	0

low to 9.2 % for *high* demand levels. In other words, fortification has reduced the adverse effect of interdiction in each setting. It was noticed that the improvement was higher for scenarios where due dates were *short* and demand *high* versus *long* due date and *low* demand. Finally, express train service was used only with short due dates because of the pressure to deliver before the specified time (and the penalty cost).

Capacity and network connectivity

It should be clear that since interdiction of terminals render them unusable, relevant traffic would have to re-routed using alternative terminals thereby impacting their

utilization. Since each terminal in the network has a finite capacity, it may not always be possible to reassign traffic to the next closest available terminal. In other situations, an interdiction may result in shippers and/or receivers losing their connectivity to the intermodal network, and in such cases demand would have to be met using direct trucking service. In this subsection, we analyze terminal capacity utilization and connectivity (or lack of) for the twenty-seven problem instances under the nine scenarios (Table 4).

Within each scenario, the *Base Case* has the highest average capacity utilization resulting from the connectedness of all shippers/ receivers and the proper working of all terminals, which also implies no direct truck service. Within each scenario interdiction without fortification (i.e., *W/out Fort*) has the lowest capacity utilization since 23 % of the customers have lost connectivity with the

Table 4 Capacity utilization & connectivity

Due date	Demand level	Cases	Avg. Cap. Utz.	Number of terminals (utilization)						% loss
				Upto25	Upto50	Upto65	Upto80	Upto90	Upto100	
Short	Low	Base case	72 %	0	0	1	14	3	0	0
		W/out fort	53 %	4	6	4	2	0	2	23
		With fort	60 %	3	3	3	7	2	0	19
	Medium	Base case	80 %	0	0	0	11	7	0	0
		W/out fort	57 %	4	3	6	2	1	2	23
		With fort	66 %	2	3	4	4	4	1	19
	High	Base case	95 %	0	0	0	0	0	18	0
		W/out fort	66 %	4	2	3	5	1	3	23
		With fort	81 %	2	0	5	2	1	8	3
Regular	Low	Base case	72 %	0	0	2	14	1	1	0
		W/out fort	52 %	4	7	4	1	0	2	23
		With fort	62 %	3	3	3	6	2	1	19
	Medium	Base case	79 %	0	0	0	10	7	1	0
		W/out fort	55 %	4	3	8	0	1	2	23
		With fort	68 %	2	3	4	5	1	3	19
	High	Base case	96 %	0	0	0	0	2	16	0
		W/out fort	63 %	3	4	2	6	0	3	23
		With fort	81 %	2	2	3	2	1	8	19
Long	Low	Base case	71 %	0	0	5	10	2	1	0
		W/out fort	52 %	4	6	5	1	0	2	23
		With fort	62 %	3	3	4	5	2	1	19
	Medium	Base case	79 %	0	0	2	8	7	1	0
		W/out fort	55 %	4	3	8	0	1	2	23
		With fort	67 %	2	3	5	3	3	2	19
	High	Base case	96 %	0	0	0	0	1	17	0
		W/out fort	63 %	4	3	7	1	0	3	23
		With fort	81 %	2	2	3	2	1	8	19

intermodal network, and have to make use of the direct trucking service to move shipments. It was noticed that interdiction with fortification (i.e., *With Fort*) yielded better capacity utilization than the without settings because the worst-case disruptions have been rendered impossible, and relatively fewer customers lose connectivity to the intermodal network. In eight of the nine scenarios, 19 % of traffic loses connectivity stemming from the fortification of *Phi* and *Atl*, and the interdiction of *Chi* and *Ind*. Finally, it was observed that for a given due date level, average capacity utilization was linearly related to the demand level.

Conclusion

In this paper, we make use of the defender-attacker-defender framework to devise strategies to protect a given number of rail-truck intermodal terminals such that the effect of disruption is minimized. A realistic size case study, based on a Class I railroad operator in the United States, was modeled as a tri-level optimization problem and solved using three distinct solution techniques, *viz.*, complete enumeration, implicit enumeration of Scaparra and Church (2008a), and a traffic-based heuristic.

In an effort to demonstrate the significance of fortification, the proposed analytical framework was used to solve twenty-seven variations of the case study, nine each for the base-case, interdiction without fortification, and interdiction with fortification. In addition, it was demonstrated that fortification has a positive bearing on the connectivity of the intermodal network –since fewer customers are forced to use the direct-trucking option thereby resulting in more cost-efficient solution for the network and higher capacity utilization of the available terminals. Finally, it was noticed that the mix of intermodal trains used to meet demand depended on the delivery due dates, with the *express* trains being mostly used for short due dates.

There are a number of future research directions. *First*, we are currently working on devising solution techniques capable of solving larger problem instances efficiently. *Second*, the tri-level model could be extended to include service-design and terminal capacity decisions. *Third*, the assumption about perfect information for both the network owner and the interdictor could be relaxed.

Acknowledgments This research was in part supported by a grant from the National Science and Engineering Research Council of Canada (OGP 312936). The third author is a member of the Interuniversity Research Centre on Enterprise Networks, Logistics and Transportation (CIRRELT), and acknowledges the research infrastructure provided by the Centre.

References

- AAR (2010) rail intermodal keeps america moving. Association of american railroads- policy and economics department. May
- Alguacil N, Delgado A, Arroyo JM (2014) A trilevel programming approach for electric grid defense planning. *Comput Oper Res* 41:282–290. doi:10.1016/j.cor.2013.06.009
- Bontekoning YM, Macharis C, Trip JJ (2004) Is a new applied transportation research field emerging?—a review of intermodal rail–truck freight transport literature. *Transp Res A Policy Pract* 38(1):1–34. doi:10.1016/j.tra.2003.06.001
- Brown G, Carlyle M, Salmeron J, Wood K (2005) Analyzing the vulnerability of critical infrastructure to attack and planning defenses. *Tutorials Oper Res EmergTheory Methods Appl*, 102–123. doi 10.1287/educ.1053.0018

- Brown G, Carlyle M, Salmerón J, Wood K (2006) Defending critical infrastructure. *Interfaces* 36(6):530–544. doi:10.1287/inte.1060.0252
- Church RL, Scaparra MP (2007) Protecting critical assets: the r-interdiction median problem with fortification. *Geogr Anal* 39(2):129–146. doi:10.1111/j.1538-4632.2007.00698.x
- Dempe S (2002) Foundations of bilevel programming. Kluwer Academic Publishers, Dordrecht
- ESRI (2008) ArcView geographical information system: an ESRI product. <http://www.esri.com>
- Hatch AB (2014) Ten years after: the second intermodal revolution. A white paper sponsored by the association of american railroads and the intermodal association of North America. January. <http://www.intermodal.org/information/research/assets/tenyrsafter.pdf>. Accessed August 21 2014
- IBM (2014) CPLEX, version 12.1.0. <http://www.ibm.org>
- Liberatore F, Scaparra MP, Daskin MS (2011) Analysis of facility protection strategies against an uncertain number of attacks: the stochastic R-interdiction median problem with fortification. *Comput Oper Res* 38(1):357–366. doi:10.1016/j.cor.2010.06.002
- Liberatore F, Scaparra MP, Daskin MS (2012) Hedging against disruptions with ripple effects in location analysis. *Omega* 40(1):21–30. doi:10.1016/j.omega.2011.03.003
- Lim C, Smith JC (2007) Algorithms for discrete and continuous multimodality flow network interdiction problems. *IEE Trans* 39(1):15–26. doi:10.1080/07408170600729192
- Losada C, Scaparra MP, O’Hanley JR (2012) Optimizing system resilience: a facility protection model with recovery time. *Eur J Oper Res* 217(3):519–530. doi:10.1016/j.ejor.2011.09.044
- Macharis C, Bontekoning YM (2004) Opportunities for OR in intermodal freight transport research: a review. *Eur J Oper Res* 153(2):400–416. doi:10.1016/S0377-2217(03)00161-9
- Mouawad J (2005). Katrina’s shock to the system. *New York Times*, September 4
- Nozick L, Morlok E (1997) A model for medium-term operations planning in an intermodal rail-truck service. *Transp Res A Policy Pract*: 31(2): 91–107. doi:10.1016/S0965-8564(96)00016-X
- Qiao J, Jeong D, Lawley M, Richard JPP, Abraham DM, Yih Y (2007) Allocating security resources to a water supply network. *IEE Trans* 39(1):95–109. doi:10.1080/07408170600865400
- Rondinelli DA, Berry MA (2000) Environmental citizenship in multinational corporations: social responsibility and sustainable development. *Eur Manag J* 18(1):70–84. doi:10.1016/S0263-2373(99)00070-5
- RPM (2014) Railroad performance measures. <http://www.railroadpm.org>. Accessed May 20, 2014
- Salmeron J, Wood K, Baldick R (2004) Analysis of electric grid security under terrorist threat. *IEEE Trans Power Syst* 19(2):905–912. doi:10.1109/TPWRS.2004.825888
- Scaparra MP, Church RL (2008a) A bilevel mixed-integer program for critical infrastructure protection planning. *Comput Oper Res* 35(6):1905–1923. doi:10.1016/j.cor.2006.09.019
- Scaparra MP, Church RL (2008b) An exact solution approach for the interdiction median problem with fortification. *Eur J Oper Res* 189(1):76–92. doi:10.1016/j.ejor.2007.05.027
- Scaparra MP, Church R (2012) Protecting supply systems to mitigate potential disaster a model to fortify capacitated facilities. *Int Reg Sci Rev* 35(2):188–210. doi:10.1177/0160017611435357
- Snyder LV, Scaparra MP, Daskin, MS, Church RL (2006) Planning for disruptions in supply chain networks. *Tutorials Oper Res*, 234–257. doi 10.1287/educ.1063.0025
- Stackelberg HV (1952) The theory of market economy. Oxford University Press, Oxford
- SteadieSeif M, Dellaert NP, Nuijten W, Van Woensel T, Raoufi R (2014) Multimodal freight transportation planning: a literature review. *Eur J Oper Res* 233(1):1–15. doi:10.1016/j.ejor.2013.06.055
- Szyliowicz JS (2003) Decision-making, intermodal transportation, and sustainable mobility: towards a new paradigm. *Int Soc Sci J* 55(176):185–197. doi:10.1111/j.1468-2451.2003.05502002.x
- US DOT (2010) Research and innovative technology administration: bureau of transportation statistics. http://www.bts.gov/publications/national_transportation_statistics. Accessed 3 December 2010
- US DHS (2014) Department of homeland security. <http://www.dhs.gov/what-critical-infrastructure>. Accessed 26 August 2014
- Verma M (2012) A fixed-penalty cost and expected consequence approach to planning and managing intermodal transportation of heterogeneous freight. *AIMS Int J Manag*, 6(2), 101–118. <http://www.aims-international.org/aimsijm/6-2>
- Verma M, Verter V (2010) A lead-time based approach for planning rail–truck intermodal transportation of dangerous goods. *Eur J Oper Res* 202(3):696–706. doi:10.1016/j.ejor.2009.06.005
- Verma M, Verter V, Zufferey N (2012) A bi-objective model for planning and managing rail-truck intermodal transportation of hazardous materials. *Transp Res E Logist Transp Rev* 48(1):132–149. doi:10.1016/j.tre.2011.06.001
- Wood RK (1993) Deterministic network interdiction. *Math Comput Model* 17(2):1–18. doi:10.1016/0895-7177(93)90236-R