Journal of Shipping and Trade

ORIGINAL ARTICLE Open Access

Evaluation of port disruption impacts in the global liner shipping network

Pablo E. Achurra-Gonzalez*, Panagiotis Angeloudis, Nils Goldbeck, Daniel J. Graham, Konstantinos Zavitsas and Marc E. J. Stettler

* Correspondence: p.achurra-gonzalez@imperial.ac.uk
Centre for Transport Studies, Department of Civil and Environmental Engineering, Skempton Building, South Kensington Campus, Imperial College London, London SW7 2BU, UK

Abstract

The global container shipping network is vital to international trade. Current techniques for its vulnerability assessment are constrained due to the lack of historical disruption data and computational limitations due to typical network sizes. We address these modelling challenges by developing a new framework, composed by a game-theoretic attacker-defender model and a cost-based container assignment model that can identify systemic vulnerabilities in the network. Given its focus on logic and structure, the proposed framework has minimal input data requirements and does not rely on the presence of extensive historical disruption data. Numerical implementations are carried in a global-scale liner network where disruptions occur in Europe's main container ports. Model outputs are used to establish performance baselines for the network and illustrate the differences in regional vulnerability levels and port criticality rankings with different disruption magnitudes and flow diversion strategies. Sensitivity analysis of these outputs identifies network components that are more susceptible to lower levels of disruption which are more common in practice and evaluates the effectiveness of component-level interventions seeking to increase the resilience of the system.

Keywords: Liner shipping, Network vulnerability, Port disruptions, Attacker-defender models, Maritime transport

Introduction

Ocean shipping is the principal mode of international freight transport, underpinning global trade. Stable access to the global network of container shipping services (liner shipping) has been shown to be a pivotal contributor to the trade competitiveness of any national economy (UNCTAD 2017).

Disruptions to the global liner shipping network can have significant implications for consumers, industries, markets, and national economies. Such disruptions (Taylor 2012) include natural disasters, political conflicts and market events, which (depending on nature, location, and severity) may affect cargo flows across the globe. Furthermore, these may affect operations in other transport infrastructure systems (roads, rail, waterways) as well as port hinterlands and dependent supply chains (Tsavdaroglou et al. 2018). It is therefore critical to quantify the vulnerability of various network components and determine preventive intervention strategies (PIANC 2017).

As discussed in the literature reviewed in section 2 of this paper, previous works on liner shipping vulnerability have mostly used pure-topological or flow-based complex networks models. Pure-topological models focus on network connectivity and use indicators such as node degree or betweenness centrality to evaluate vulnerability. However, their representation of component states is mostly binary (e.g. a connection between two ports exists or not), and therefore cannot be used to evaluate the entire spectrum of failure conditions. Furthermore, such models are unable to capture capacity-constrained aspects of liner operations, the effects of re-routing through alternative paths, and the financial gains (if any) of preventing disruptions, which is information of key interest to decision-makers.

In contrast, flow-based models do not have such shortcomings and are therefore more suitable for the study of liner shipping vulnerabilities, subject to the availability of historical disruption data that could be used to determine expectations of failure for network components. However, in liner shipping, operators often perceive that sharing historical disruption data can be detrimental to their competitiveness as their customers can interpret it as a lack of preparedness to withstand disruptions. Therefore, current industry confidentiality practices, as well as the variety of actors, processes and relationships among them, render it difficult to access or create such datasets in liner shipping.

A separate thread of research has used game-theoretic analysis to assess the vulnerability of constrained transport networks (Bell et al. 2008) without heavily relying on historical disruption data. Such techniques focus extensively on network structures while still considering network flows. While this approach has the potential to address the shortcomings of both types of models, to the best of our knowledge (section 2) there has been no study that was able to represent the capacity-constrained nature of ports while capturing call-skipping and flow rerouting processes.

As such, the objective of this study is to address the current literature gap by developing a new systemic vulnerability analysis framework for large shipping networks that does not require prior knowledge of disruption probabilities. The resulting framework can rank critical network components, quantify the impact of disruption prevention measures and determine any additional handling costs and non-delivery penalties. The remainder of this paper is structured as follows: Section 2 provides a review of relevant literature and identifies research gaps. Premise, assumptions and formulations of the constituent mathematical models are presented in Section 3. A case study involving disruptions at major European container ports and services is presented in Section 4, illustrating the scalability of the algorithm. It is followed by a discussion on how costs and criticality rankings are affected by disruptions levels and flow diversion strategies. The paper concludes with a summary of contributions, limitations, and suggestions for future work.

Background literature

Approaches to assessing transport vulnerability can vary significantly based on the type of network, disruption sources, and data available (Muriel-Villegas et al. 2016). Previous studies focused on road networks lacking transport demand data (Bell et al. 2017), subway networks under random failures (Angeloudis and Fisk 2006), country-level ocean container networks (Calatayud et al. 2017) and power grids exposed to targeted attacks

(Ouyang et al. 2014). Comprehensive reviews of previous works on vulnerability assessment for various types of transport networks, disruption sources, and the evaluation of related terms such as resilience and reliability are also available (Mattsson and Jenelius 2015; Reggiani et al. 2015; Hosseini et al. 2016).

Complex network techniques have so far been a popular choice for the analysis of liner shipping networks (Bartholdi et al. 2016; Angeloudis et al. 2007; Ducruet et al. 2010; Ducruet 2016) which in the context of vulnerability assessment can be classified into pure-topological or flow-based models. Pure-topological models focus on indicators such as connectivity, betweenness, and degree centrality to evaluate network vulnerabilities without directly considering material flows or commercial activity (examples include Calatayud et al. 2017; Ducruet and Zaidi 2012; Viljoen and Joubert 2016).

Most pure-topological approaches can only model disruptions based on complete removal of individual network components (arcs or nodes). Sullivan et al. (2010) discuss the limitations of such binary representations, especially given the prevalence of disruptive incidents that involve only partial reductions in handling capacities (e.g. March 2013 labour strike described in Qi (2015) which reduced 20% of Hong Kong port capacity). The authors further argue that disrupted networks in such models feature isolated sub-networks, which are not commonly observed in real markets, and can be quickly resolved using service amendments.

Flow-based models use mass-conservation constraints, consider operation costs and flow redistribution in the aftermath of disruptions (Ouyang et al. 2014; Paul and Maloni 2010) are often embedded in non-cooperative game theoretic (NCGT) methods that focus on scenarios were individual agents act based on self-interest with diverging or competing objectives. Such methods have been used to mitigate the absence of historical disruption probability distributions, and identify worst-case scenarios, which were in turn used for countermeasure preparation (Kanturska and Angeloudis 2013). Hollander and Prashker (2006) classified transport-related NCGT studies according to the types of actors participating in the game: (i) games between travellers, (ii) between authorities, (iii) travellers vs authorities and (iv) travellers vs demons.

Games involving demons are best suited for the analysis of disruption impacts and are oftentimes solved using attacker-defender models (ADM). One of the earliest such efforts in transport was undertaken by Bell (2000), and involved a user seeking to minimise trip costs and a tester (demon) seeking to maximise disruption costs. The proposed maximin formulation can be used to obtain optimal routing strategies for pessimistic network users and optimal disruption strategies for the demon. Estimated user trip costs serve as a quantitative measure of network vulnerability, while component attack probabilities can determine the criticality of each component for overall network performance. It is important to note that attack probabilities do not represent actual failure probabilities of network components, but rather serve as a measure of criticality with respect to the nominal operation of the network. Subsequent studies considered multiple users and demons (Bell and Cassir 2002) and explored other transport and infrastructure problem settings (e.g. Bell 2003; Bell et al. 2008; Qiao et al. 2014; Wang 2012; Kanturska and Angeloudis 2013).

Bencomo (2009) used ADMs for the evaluation of security incident impacts (e.g. earthquakes, labour strikes and terrorism) on the transportation costs of ocean containers. Their model generates payoff matrices for the game using a multi-commodity network flow model. However, it assumes that all ports are connected, which is not necessarily the case in practice, and results in rerouting arrangements that do not adhere to service arrangements. Zavitsas (2011) focused on maritime petroleum supply chains, and their vulnerability against natural disasters, accidents or malicious attacks. An ADM was used to identify critical components in the network and propose infrastructure improvements. However, as tankers travel directly between origins and destinations, the methodology is not immediately transferable to liner-shipping.

Previous work by Achurra-Gonzalez et al. (2016) focused on unsatisfied cargo demands to quantify disruption impacts and redundancy levels in the network (for cargo re-routing). The proposed technique was limited by its focus on ports and services, which precluded the study of disrupted maritime corridors (e.g. canals, straits, access channels). This was partially addressed in Achurra-Gonzalez et al. (2017), where vessel routing algorithms were used to identify such dependencies. Both studies focused on loaded containers, and do not account any repositioning processes that would preclude the misplaced accumulations of empty containers. Such processes would also be affected by disruptions and exacerbate their effects due to misplaced accumulations of empty containers.

Methodological framework

The vulnerability analysis framework presented in this paper consists of a two-stage game-theoretic attacker-defender model (ADM) between a malevolent agent (attacker) and an ocean carrier (defender). In the first stage, a cost-based container assignment model (CAM) adapted for the analysis of networks under disruptions computes the required payoff matrix for each of the player's strategies and the ADM is solved for an initial state where all evaluated network components are exposed disruptions. In the second stage, the ADM is implemented through a series of iterative network interventions that remove the most critical network component of each previous iteration. Results generate a criticality ranking of network components with a quantitative measure of the transportation cost impact of disruptions on each of them.

Cost-based container assignment model

The container assignment model (CAM) seeks to determine optimal container flows (loaded and empty) from origin ports $r \in R$ to destination port $s \in S$, across a sequence of attractive liner service legs (formed by links connecting any pair of ports within a liner service) that can reduce the overall routing costs in the system. Higher penalty values are used for full containers to prioritise cargo deliveries over empty container repositioning. The resulting assignments utilise a set of optimal paths, expressed as chains of legs belonging to one or more liner services. Legs correspond to transportation tasks (between an an origin port and their ultimate destination) whereas links represent the physical movement of vessels between ports.

Fig. 1 illustrates these concepts for a typical liner service that sequentially connects ports A, B, C and D where solid blue lines represent links and dashed red lines represent transport legs. In this example, Leg 2 represents containers loaded in Port A and

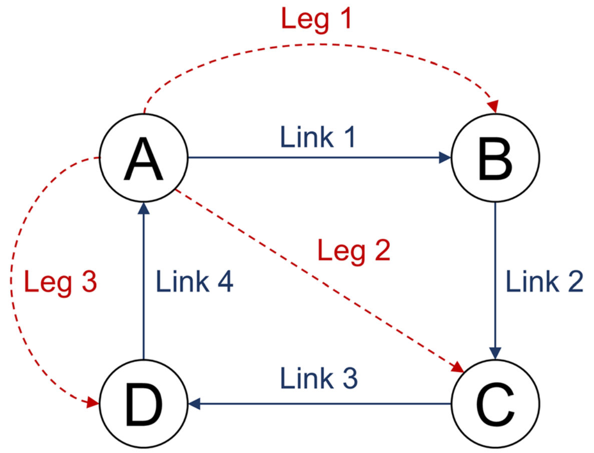


Fig. 1 Liner service links and corresponding legs

unloaded in Port C, which travel through Link 1 (A➔B) and 2 (B➔C). Since both links belong to the same liner service, the containers do not have to be transhipped at port B, which would have been the case otherwise.

Given that vessel arrival and departures at any given port $k \in K$ are assumed to be random and uncoordinated, the availability of attractive legs is proportional to the frequencies of services that can connect k to s. Therefore, the dwell times of s-bound containers at k is equal to the inverse sum of their service frequencies (Bell et al. 2011). In contrast, direct shipments do not incur dwell times. It is therefore possible and acceptable for the model to establish multiple flows for each OD pair, each with a different path. As exogenous demand matrix is used as an input, which assumes that weekly demand rates are fixed across the period surveyed – we regard to be a valid assumption for network-level vulnerability analysis.

The model assumes that loaded containers have fixed a set of daily rent, uniform loads, handling priorities, and cargo depreciation rates, while all cargo is equally prioritised. This departure from real-world practices (ocean carriers can utilise varying cost structures, shippers incur variable depreciation costs depending on cargo, and repositioning penalties apply in imbalanced trade lanes) was made to simplify data requirements in this study, but is made without loss of generality, as the model formulation is sufficiently flexible to accommodate such data. The cost structure adopted by our analysis acknowledges the effects of economies of scale, and are calculated as function of time charter (TC) rates and vessel capacities in terms of containers of twenty-foot equivalent units (TEU).

Penalty costs for containers not transported due to capacity limits or in the aftermath of disruptions are assumed to be USD 50,000 and USD 5000 for loaded and empty containers respectively. These penalty costs are calibrated to be higher than any routing costs alternative in all U_{ij} disruption scenarios (described in the attacker-defender model formulation section) to ensure that cargo flows are maximised when routing capacity is available without inflating the disruption cost outputs of our model. Our calibrated penalty costs are significantly smaller than the values used by Kjeldsen et al. (2011), who adopted a value USD 1,000,000 for any container not transported. These penalties for undelivered containers are used to capture the impact of disruptions on repositioning, which as mentioned earlier can lead to misplaced accumulation of empty containers across the network.

The notation used in our model is summarised in Table 1, which is followed by the formulation. The operators + and ++ are used to simplify two reoccurring summations: $x^f_{a+} = \sum_{s\in D} x^f_{as}$ and $w^f_{++} = \sum\limits_{r\in O} \sum_{s\in D} w^f_{rs}$.

Objective:

$$\begin{aligned} min\ Uij = &\sum_{n\in N}\sum_{a\in A} CHC_{an}\left(x^f_{a+} + x^e_{a+}\right) + \left(\sum_{a\in A} x^f_{a+} C_a + w^f_{++}\right)(CR + DV) \\ &+ \left(\sum_{a\in A} x^e_{a+} C_a + w^e_{++}\right)(CR) + \sum_{r\in O}\sum_{s\in D}\left(TD^f_{rs} - t^f_{rs}\right)PC^f \\ &+ \sum_{r\in O}\sum_{s\in D}\left(TD^e_{rs} - t^e_{rs}\right)PC^e \end{aligned} \tag{3.1}$$

Subject to:

$$\sum_{a\in A^+_k} x^f_{as} - \sum_{a\in A^-_k} x^f_{as} = B^f_k \quad \forall k\in K, s\in S \tag{3.2}$$

$$\sum_{a\in A^+_k} x^e_{as} - \sum_{a\in A^-_k} x^e_{as} = B^e_k \quad \forall k\in K, s\in S \tag{3.3}$$

$$B^f_k = \begin{cases} -\sum\limits_{s\in S} t^f_{rs}\ if\ k = r\in R \\ \sum\limits_{r\in R} t^f_{rs}\ if\ k = s\in S \\ \quad 0\ otherwise \end{cases} \tag{3.4}$$

$$B^e_k = \begin{cases} -\sum\limits_{s\in S} t^e_{rs}\ if\ k = r\in R \\ \sum\limits_{r\in R} t^e_{rs}\ if\ k = s\in S \\ \quad 0\ otherwise \end{cases} \tag{3.5}$$

$$x^f_{as} \le w^f_{ks} F_a \quad \forall a \in A^-_k, k \ne s\in K, s\in S \tag{3.6}$$

$$x^e_{as} \le w^e_{ks} F_a \quad \forall a \in A^-_k, k \ne s\in K, s\in S \tag{3.7}$$

$$LS_n \ge \sum_{a\in A}(x^f_{a+} + x^e_{a+})\tau_{aln} \quad \forall l\in L_n, n\in N \tag{3.8}$$

$$\hat{\alpha}_{jy}\hat{\delta}_{iy}MC_y \ge \sum_{a\in A}(x^f_{a+} + x^e_{a+})\tau_{aly} \quad \forall \in L_y, y\in Y, i\in I, j\in J \tag{3.9}$$

$$\hat{\alpha}_{jk}\hat{\delta}_{ik}PT_k \ge \sum_{a\in A^-_k}(x^f_{a+} + x^e_{a+}) + \sum_{a\in A^+_k}(x^f_{a+} + x^e_{a+}) \quad \forall k\in K, i\in I, j\in J \tag{3.10}$$

$$t^f_{rs} \le TD^f_{rs} \quad \forall r\in R, s\in S \tag{3.11}$$

$$t^e_{rs} \le TD^e_{rs} \quad \forall r\in R, s\in S \tag{3.12}$$

$$x^f_{as}, x^e_{as} \ge 0 \quad \forall a\in A, s\in S \tag{3.13}$$

The model seeks to minimise the sum of network routing costs U_{ij} when cargo flow is diverted from component i by the defender and component j is disrupted by the

Table 1 CAM and ADM notation

Sets		Subsets		Indices	
A	All legs	A_k^+	Legs entering port k	a	Legs
K	All ports	A_k^-	Legs leaving port k	k	Ports
S	Destination ports	A_n	Legs on service n	y	Corridors
R	Origin ports	L_y	Links on corridor y	l	Links
Y	All corridors	L_n	Links on service n	n	Liner services
L	All links			r	Origin ports
N	All liner services			s	Destination ports
J	Disrupted components			j	Disruption strategies
I	Defended components			i	Defence strategies
				f	Loaded containers
				e	Empty containers
Parameters					
B_k^f	Net flow of loaded containers at each port k				
B_k^e	Net flow of empty containers at each port k				
C_a	Sailing time on leg a, including loading and unloading times at ports (e.g. days)				
CHC_{an}	Container handling cost per loaded container on leg a using liner service n				
CR	Rental cost per unit time per loaded or empty containers				
TD_{rs}^f	Demand for loaded containers to be transported from origin r to destination s in the defined planning horizon				
TD_{rs}^e	Demand for empty containers to be transported from origin r to destination s in the defined planning horizon				
DV	Depreciation cost per unit time per loaded container (inventory cost)				
τ_{aln}	1 if leg a uses link l on liner service n, and 0 otherwise				
τ_{aly}	1 if leg a uses link l on maritime corridor y, and 0 otherwise				
F_a	Frequency of sailings on leg a				
PT_k	Throughput capacity of port k				
LS_n	Throughput capacity of liner service n				
MC_y	Throughput capacity of maritime corridor y				
δ_i	Defender flow diversion percentage in strategy i (please refer to Attacker-defender model section)				
α_j	Attacker disruption percentage in strategy j (please refer to Attacker-defender model section)				
$\hat{\delta}_i$	Defender capacity multiplier for network components with flow diversion in strategy i				
$\hat{\alpha}_j$	Attacker capacity multiplier for disrupted network components in strategy j				
PC^f	Penalty cost for loaded containers not transported				
PC^e	Penalty cost for empty containers not transported				
Decision variables					
t_{rs}^f	Serviced demand of loaded containers shipped from origin r to destination s				
t_{rs}^e	Serviced demand of empty containers shipped from origin r to destination s				
x_{as}^f	Flow of loaded containers on leg a en route to destination s				
x_{as}^e	Flow of empty containers on leg a en route to destination s				
w_{ks}^f	Expected dwell time at port k for all loaded containers en-route to destination s				
w_{ks}^e	Expected dwell time at port k for all empty containers en-route to destination s				
p_i	Probability defender diverts flows from component i				
q_j	Probability attacker disrupts component j				
v	Value of the game for the defender (routing costs)				
z	Value of the game for the attacker (disruption costs)				

attacker (3.1). These costs cover container handling, inventory, and rental fees generated from the assignment of container flows to legs and penalty costs for containers not transported.

Constraints (3.2) through (3.5) enforce flow conservation. Constraints (3.6) and (3.7) ensure that the dwell time of loaded and empty containers is not less than the inverse of the combined liner service frequencies for the corresponding route. The capacity constraint for each liner service is defined in (3.8). Constraints for maritime corridor capacity (e.g. canals, access channels and straits) are defined in (3.9) where $\hat{\alpha}_j$ and $\hat{\delta}_i$ define the percentage of available functional capacity in attacker strategy *j* and defender strategy *i* respectively. Similarly, port throughput constraints are defined in (3.10). Constraints (3.11) and (3.12) ensure that the total number of full and empty containers does not exceed the demand specified in OD matrices. Where capacity falls below the total demand, the model can decide not to fulfil a portion of the demand, subject to penalties. Finally, (3.13) ensures that all flow variables are non-negative.

Where weekly port call frequencies exist, we assume that there exist enough allocated vessels to ensure maintain weekly call frequencies (as is common practice on major routes). For services that do not operate on a weekly basis, we use the effective route capacity LS_n formula:

$$LS_n = \left(\frac{\sum\limits_{h \in H_n} NC_{hn}}{TH_n}\right)\left(\frac{SMF}{F_n}\right) \ \forall n \in N \tag{3.14}$$

Where

$n \in N$	Set of liner services in the network
$h \in H_n$	Set of container vessels deployed in liner service $n \in N$
F_n	Port call frequency of liner service $n \in N$
NC_{hn}	Nominal capacity (TEU) of a container vessel $h \in H_n$ deployed in liner service $n \in N$
TH_n	Total number of vessels deployed in liner service $n \in N$
SMF	Standardised model service frequency (e.g. weekly, monthly, annual)

In the above, *SMF* is expressed as the actual number of days for the desired time window in which the liner service capacities will be standardised.

Attacker-defender model

In our attacker-defender model (ADM) formulation, the attacker represents an abstract entity that encompasses potential sources of targeted disruption that may affect a liner shipping network. These include, but are not limited to labour strikes, intentional port access closure political conflicts, cyber- or terrorist attacks. The attacker's objective is to disrupt critical components and maximise disruption costs to the defender.

For the purposes of this study, we assume that the defender is a global ocean carrier or alliance seeking to serve transport demands at the lowest possible routing cost. Ocean carriers in today's liner shipping industry can influence operations at some components of their network (e.g. ports owned by the same holding company) to increase security measures that would reduce the incidence of some disruptions. However, most ocean carriers do not have such influence across all components of their network and are therefore exposed to disruptions at components that they cannot protect.

As such, the ocean carrier modelled as the defender in our ADM is assumed to be incapable of protecting network components. Instead, it is only capable diverting cargo flows away from critical component the attacker may disrupt to minimise its routing costs. Thus, the defender's objective is to identify any critical components that the attacker would be likely to disrupt and divert container flows in a way that minimises disruption-related rerouting and penalty costs.

Our ADM is, therefore, a zero-sum game played simultaneously, with both players having access to perfect information on the abilities of their opponent but no knowledge of their adopted strategy. The required payoff matrix is generated using the CAM model, executed for all combinations of available strategies. For the purposes of this study, we assume that the attacker can disrupt only one network component at any time, but is afforded the option to attack more components in further rounds. Similarly, the defender undertakes a single preventative activity on each stage. This aspect of the framework is explained further in Section 3.3.

The disruption scenarios are built on the premise that the attacker can only disrupt the same set of components that the defender may choose to divert flow from. Each scenario U_{ij}, where i is the component from which the defender diverts cargo and j is the component disrupted by the attacker. With the assumptions stated above and m being the total number of elements in the sets $I = J$, the following two cases are possible for each scenario:

1) Case $i = j$: The attacker and defender choose the same component to disrupt or defend, and there remain $m - 1$ components in the network that are not affected by disruption or flow diversion.
2) Case $i \neq j$: The attacker and defender choose different components to disrupt or defend, and there remain $m - 2$ unaffected components.

Using the network routing costs U_{ij} for all scenarios, we construct an m-by-n payoff matrix, with values calculated by distinct CAM iterations. The minimum number of iterations required to complete the payoff matrix depends upon the defender flow diversion percentage δ_i and the attacker capacity disruption percentage α_j as defined in the following two cases:

1) Case $\alpha_j = \delta_i$: If the attacker disruption percentage α_j is equal to the defender flow diversion percentage δ_i, then $U_{ij} = U_{ji}$. Since the matrix is symmetric, the minimum number of required CAM iterations is equal to $(m + 1)m/2$.
2) Case $\alpha_j \neq \delta_i$: If the attacker disruption percentage α_j is not equal to the defender flow diversion percentage δ_i, then $U_{ij} \neq U_{ji}$. Therefore, the minimum number of required CAM iterations increases exponentially according to m^2 corresponding to the total number of elements in the payoff matrix.

For the defender, we define the scalar $\hat{\delta}_i = 1{-}\delta_i$ as the functional capacity for network components with flow diversion in strategy i. Similarly, for the attacker, $\hat{\alpha}_j = 1 - \alpha_j$ defines the functional capacity for network components affected by disruptions in attacker strategy j. Using the above definitions, we develop the following maximin formulation for the attacker-defender model:

Objective:

$$\max_{q_j}\left(\min_{p_i}\sum_{i\in I}\sum_{j\in J}p_i U_{ij}q_j\right) \tag{3.15}$$

Subject to:

$$\sum_{j\in J}q_j = 1 \tag{3.16}$$

$$\sum_{i\in I}p_i = 1 \tag{3.17}$$

$$q_j, p_i \geq 0 \ \ \forall i\in I, j\in J \tag{3.18}$$

The objective (3.15) is for the attacker to maximise the expected disruption cost while the defender minimises the expected disruption cost. Constraints (3.16) through (3.18) ensure valid mixed strategies where each player assigns a probability to each component in $I = J$ such that the sum of probabilities equals to one. The model is solved using a linear formulation with the introduction of a variable z that represents network disruption costs:

Objective:

$$\max z \tag{3.19}$$

Subject to:

$$\sum_{j\in J}U_{ij}q_j \geq z \ \ \forall i\in I \tag{3.20}$$

$$\sum_{j\in J}q_j = 1 \tag{3.21}$$

$$q_j \geq 0 \ \ \forall j\in J \tag{3.22}$$

The resulting objective (3.19) represents the attacker's intention to maximise z. Setting z on the right-hand side of the inequality constraints (3.20) ensures that the optimal strategy of the defender is taken into account because the payoff for the attacker cannot exceed the smallest expected disruption costs considering all possible moves of the defender. To derive the optimisation problem of the defender, we introduce a variable v to represent total routing costs, alongside a minimisation objective (3.23):

Objective:

$$\min v \tag{3.23}$$

Subject to:

$$\sum_{i\in I}U_{ij}p_i \leq v \ \ \forall j\in J \tag{3.24}$$

$$\sum_{i\in I}p_i = 1 \tag{3.25}$$

$$p_i \geq 0 \ \ \forall i\in I \tag{3.26}$$

The model formulation for attacker strategies is the dual of the defender strategy model and vice versa. Therefore, the optimal solution would satisfy $z = v$ and the solution would be a Nash equilibrium with mixed strategies. Here, the attacker's strategy represents the worst case attack probabilities assuming that these are anticipated by the defender (Kanturska and Angeloudis 2013). In other words, higher component attack probabilities would have a more adverse effect to the networks. On the other hand, the equilibrium strategy of the defender indicates the safest path choice frequency. As expected for maritime supply chain networks, this path choice frequency often involves the use of more than one path.

As demonstrated in previous ADM implementations, disruption costs can be expected irrespective of the routing paths selected by the defender. Therefore, the value of the game also represents a measure of the overall vulnerability of the transport network. On the other hand, the value of the game for the defender indicates the worst-case routing costs. The routing strategy selected by the defender guarantees that regardless of attack strategies, the total routing costs will not be higher than the value of the game.

Model integration

The ADM and CAM models are combined in a two-stage framework that evaluates a series of iterative network interventions to generate a criticality ranking of network components. This framework hereinafter referred to as ADCAM, follows from Sullivan et al. (2010), who investigated the use of sequential approaches to assess the relative importance of disrupted components as part of a solution procedure. This approach does not focus on the investigation of specific impacts of a single disruptive action but the performance of the system against known or unknown sources of disruption.

The overall workflow of our proposed framework stages and the interactions between the two models are illustrated in Fig. 2. The pseudocode for the framework implementation is presented in Fig. 3. In the first stage, iterations of the CAM for U_{ij} scenarios defined by the player's strategies populate the required payoff matrix of the ADM (pseudo code lines 14 through 21). The ADM is then solved for an initial iteration t where all evaluated network components are exposed disruptions. The most critical network component (MC) is identified in line 24 as the arc or node with the highest attack probability (max of vector q) from solving the current ADM iteration t.

In the second stage, the most critical network component at iteration t is removed from the set of components that can be disrupted by the attacker in iteration $t + 1$. Therefore, the algorithm proceeds to remove the current MC from the payoff matrix in lines 27 and 28 of the pseudocode before solving the next ADM iteration. The iterations end when all network components are removed from the attacker's disruptable set. The outputs of the integrated framework include a series of network disruption costs Z^{*} ranging from a worst-case disruption scenario (where the most vulnerable component is disrupted) to the best-case scenario (where the attacker is only able to disrupt the component with minimum network impact). Also provided are network component rankings with respect to the attack probabilities in the network.

The iterative removal of components in the second stage of our proposed framework is not part of the defence strategy of the ocean carrier but an algorithmic step necessary to generate a criticality ranking of the network components. Without this iterative removal of network components, quantitative vulnerability methods such as

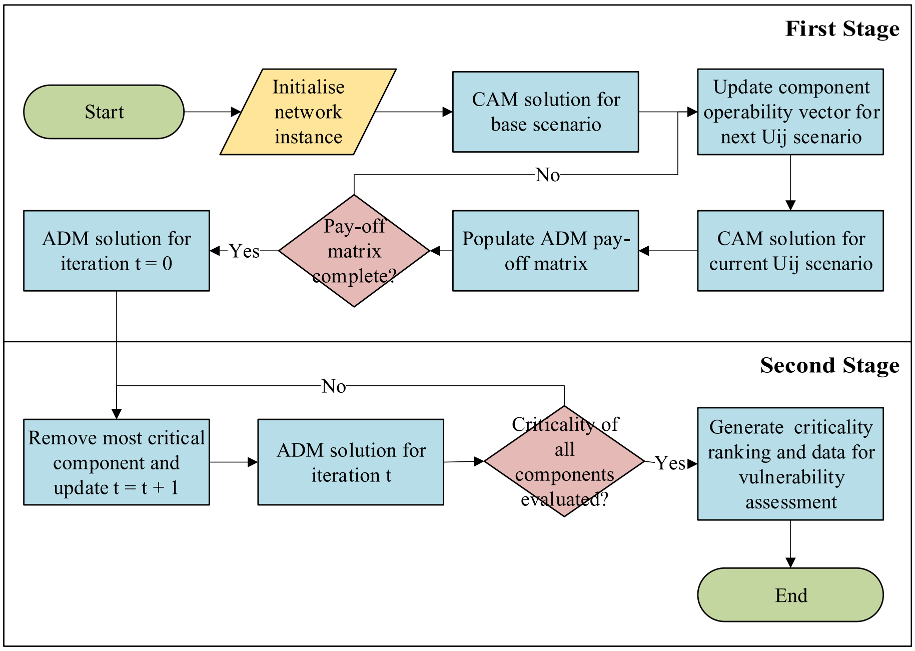

First Stage
Start
Initialise network instance
CAM solution for base scenario
Update component operability vector for next Uij scenario
No
ADM solution for iteration t = 0
Yes
Pay-off matrix complete?
Populate ADM pay-off matrix
CAM solution for current Uij scenario
Second Stage
No
Remove most critical component and update t = t + 1
ADM solution for iteration t
Criticality of all components evaluated?
Yes
Generate criticality ranking and data for vulnerability assessment
End

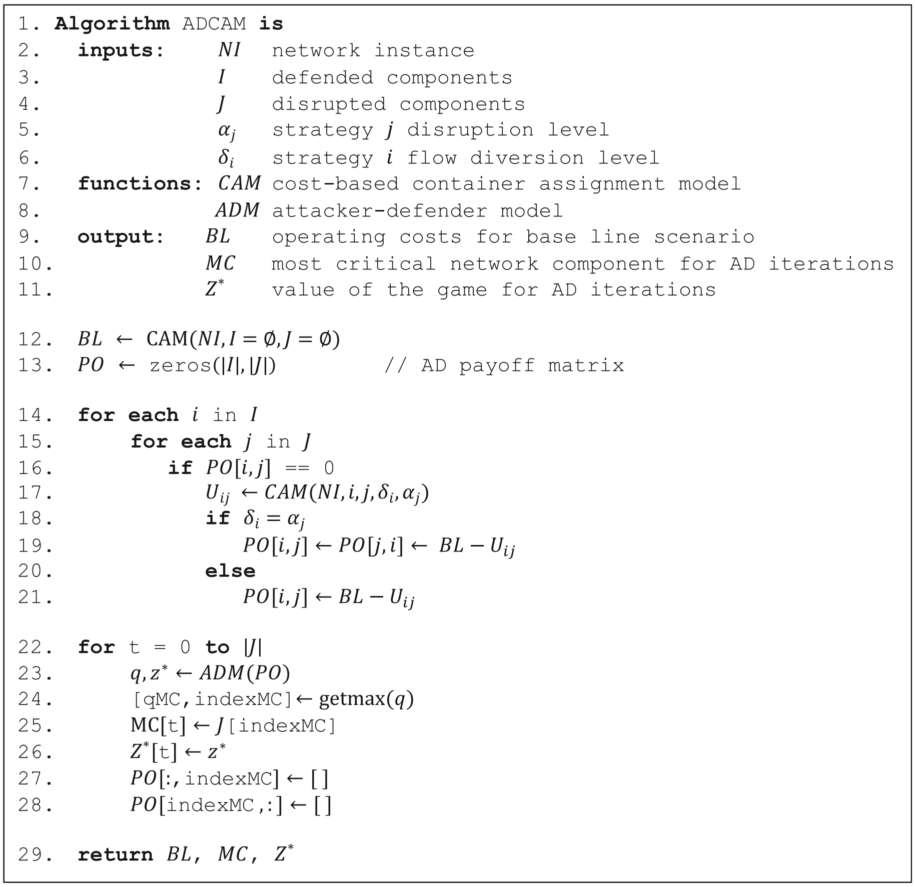
Fig. 2 ADCAM implementation workflow

the ADM can only identify few components with high attack-probabilities and many components with non-differentiable attack probabilities which impede the understanding of their relative importance within the network. This limitation is caused by the liner shipping operational characteristic of high concentrations of cargo flows in few components (e.g. *major* transhipment ports or import/export gateways).

The two-stage ADCAM framework is, therefore, is a suitable method for computing criticality rankings of components and quantifying the potential impact of disruptions in the liner shipping networks.LINER-LIB dataset developed by Brouer et al. (2014). LINER-LIB was initially intended for use as a benchmark dataset for liner-shipping network design algorithms. However, as it was developed in close co-operation with industry stakeholders and it is deemed to be sufficiently representative for use in a broader spectrum of liner shipping studies.

Network parameters that were used in the analysis are summarised in Table 2. Container rental and cargo depreciation costs used for this case study follow from Bell et al. (2013), while container handling costs are defined as the ratio of time charter rates against the average TEU capacity of each vessel class. This is an improvement upon earlier studies on container assignment, the majority of which tend to use constant values across the entire network. Cost rates were also obtained from the LINER-LIB dataset, and incorporate operating expenses, crew salaries and maintenance costs. For this study, we assume that these do not depend upon vessel utilisation, which would have been considered during service design.

The ports selected for disruption analysis (listed in Table 3) are located in Northwest Europe and are recognised as trade gateways, with significant transhipment and feeder traffic. Port throughput rates (TEU handled per year) were obtained from Containerisation International (2012) and were used to define the upper bound



```
Algorithm ADCAM is
  inputs:     $NI$   network instance
              $I$    defended components
              $J$    disrupted components
              $\alpha_j$   strategy $j$ disruption level
              $\delta_i$   strategy $i$ flow diversion level
  functions:  $CAM$  cost-based container assignment model
              $ADM$  attacker-defender model
  output:     $BL$   operating costs for base line scenario
              $MC$   most critical network component for AD iterations
              $Z^*$   value of the game for AD iterations

  $BL \leftarrow \mathrm{CAM}(NI, I = \emptyset, J = \emptyset)$
  $PO \leftarrow$ zeros($|I|, |J|$)        // AD payoff matrix

  for each $i$ in $I$
      for each $j$ in $J$
         if $PO[i,j]$ == 0
            $U_{ij} \leftarrow CAM(NI, i, j, \delta_i, \alpha_j)$
            if $\delta_i = \alpha_j$
               $PO[i,j] \leftarrow PO[j,i] \leftarrow BL - U_{ij}$
            else
               $PO[i,j] \leftarrow BL - U_{ij}$

  for t = 0 to $|J|$
      $q, z^* \leftarrow ADM(PO)$
      [qMC, indexMC] $\leftarrow$ getmax($q$)
      MC[t] $\leftarrow J$[indexMC]
      $Z^*$[t] $\leftarrow z^*$
      $PO$[:, indexMC] $\leftarrow$ [ ]
      $PO$[indexMC, :] $\leftarrow$ [ ]

  return $BL$, $MC$, $Z^*$
```

Fig. 3 ADCAM algorithm

Table 2 Case study network parameters

Network particulars			
Depreciation rate for container cargo			80 USD/TEU/day
Undelivered container penalty (loaded)			50,000 USD/TEU
Undelivered container penalty (empty)			5,000 USD/TEU
Rental cost for loaded/empty containers			18 USD/TEU/day
Transport cost per vessel class			
Vessel class	Capacity (TEU)	Time charter (USD/day)	Handling cost (USD/TEU/day)
Feeder_450	900	4,680	5.20
Feeder_800	1,600	7,966	4.98
Panamax_1200	2,400	11,683	4.86
Panamax_2400	4,800	21,774	4.53
Post_Panamax	8,400	33,922	4.04
Super_PostPanamax	15,000	48,750	3.25

capacity values for ports in the network. As these figures are aggregate and describe all container traffic regardless of carrier, we use the approach described in Achurra-Gonzalez et al. (2017) to obtain the downscaled capacity PT_k for all 230 ports in the case study network as follows:

$$PT_k = \frac{\sum\limits_{n \in N} LS_{nk}}{\sum\limits_{\hat{n} \in \hat{N}} LS_{\hat{n}k}} RT_k \quad \forall k \in K \tag{4.1}$$

Where:

K	Set of all ports in the case study network
$\hat{N}$	Set of all liner services in the original dataset
N	Subset of services considered by the case study
LS_{nk}, $LS_{\hat{n}k}$	Weekly capacity of liner services $n \in N$ and $\hat{n} \in \hat{N}$, calling at port $k \in K$
PT_k	Adjusted weekly throughput for port $k \in K$
RT_k	Reported weekly throughput for port $k \in K$

A transhipment incidence parameter TI_k was used to indicate the relative proportion of transhipment traffic for any port k that can be disrupted. This was determined using (3.2) and is defined as the percentage of transhipment flows from the total weekly throughput at port k in the baseline scenario (BST_k) without disruptions and flow diversions. Results for each of the ports surveyed, accompanied by their corresponding UNLOCODE, reported throughput (RT_k) and adjusted port capacity (PT_k) are provided in Table 3.

$$TI_k = \frac{BST_k - \left(\sum\limits_{r \in R} TD^f_{rk} + \sum\limits_{s \in S} TD^f_{ks}\right)}{BST_k} \quad \forall k \in K \tag{4.2}$$

where:

K	Set of all ports
R	Set of origin ports
S	Set of destination ports
BST_k	Weekly baseline scenario throughput at port $k \in K$
RT_k	Reported weekly throughput of port $k \in K$
TD^f_{rk}	Weekly demand for loaded containers from $r \in R$ to port $k \in K$
TD^f_{ks}	Weekly demand for loaded containers from port $k \in K$ to destination $s \in S$
TI_k	Transhipment incidence of port k in the case study network

Table 3 Container ports in strategy sets *I* and *J*

Port name	Country	UNLOCODE	RT_k	PT_k	BST_k	TI_k
Antwerp	BE	BEANR	162,856	27,686	5,208	68.6%
Hamburg	DE	DEHAM	151,924	12,002	2,522	15.8%
Zeebrugge	BE	BEZEE	45,960	6,342	3,214	16.6%
Bremerhaven	DE	DEBRV	93,678	54,614	28,936	34.9%
Rotterdam	NL	NLRTM	214,342	50,156	26,648	46.8%
Felixstowe	UK	GBFXT	65,384	19,812	11,146	43.7%

The model formulations and overall algorithm were implemented and solved using a combination of MATLAB, the IBM OPL modelling language, and the IBM CPLEX solver (version 12.6). The model was executed on a high-performance workstation with an E5-2640v3 Xeon CPU and 192GB RAM. The average solution time for each CAM iteration was 17.4 min with a standard deviation of 1.8 min. The number of iterations required varies by the defender flow diversion percentage δ_i and the attacker capacity disruption percentage α_j ($\alpha_j = \delta_i$ in Case 1 and $\alpha_j \neq \delta_i$ for Case 2).

Complete disruptions

In the first instance, we considered disruptions affecting port operations, with a defender response involving the complete diversion of cargo from the ports in question (Case 1 where $\alpha_j = \delta_i = 100\%$). Key events at each timestep are presented in the list below.

t = 0: The port of Bremerhaven is initially identified as the most critical port in the case study network, with an attack estimated to result in a cost of 771.5 mil USD/ week.

t = 1: Bremerhaven is defended against disruptions (and is therefore excluded from the list of ports that can be attacked). The cost of disruption is reduced by 89 USD million/week (– 11.6% marginal disruption cost z^* decrease). Rotterdam and Felixstowe are identified as the most critical ports, with attack probability values of 0.90 and 0.10 respectively.

t = 2: Following defensive measures at Rotterdam, disruption costs are decreased by 376 million USD/week (48.7%) Felixstowe and Antwerp are identified as potential targets, with attack probabilities of 0.77 and 0.23, respectively.

t = 3: An intervention in Felixstowe reduces the estimated cost of disruption by 145.3 USD million/week (– 18.8%). Three ports are identified as potential targets, with probabilities of 0.57 for Antwerp, 0.31 for Zeebrugge, and 0.12 for Hamburg.

t = 4: Antwerp is defended against disruptions resulting in financial gains of 52.8 million USD/week (– 5.9% marginal z^* decrease). Updated attack probabilities for the two remaining ports are 0.56 for Zeebrugge and 0.44 for Hamburg.

Iterations $t = 5$ and $t = 6$ defend Zeebrugge and Hamburg respectively with combined financial gains of 107 million USD/week. A summary of results and the resulting payoff matrix are provided in Table 4, which also provides an outline of intervention strategies at critical network components. Figure 4 plots the changes in disruptions costs from the network interventions at the most critical port identified at $t - 1$ as well as marginal financial gains from such interventions.

Partial disruptions

We conduct a sensitivity analysis that evaluates how changes in disruption (α_j) and flow diversion (δ_i) influence network vulnerability and criticality ranking of the selected ports (Case 2 where $\alpha_j \neq \delta_i$). The evaluated disruption and flow diversion levels between the range of 0% to 100% at increments of 20% in 30 distinct network instances. Figure 5 illustrates the changes in network disruption costs z^* and the changes in criticality rankings.

Table 4

CAM Payoff matrix disruption costs (USD/week)

	Network Components	Attacker: Scenarios j					
		DEBRV	NLRTM	GBFXT	BEANR	BEZEE	DEHAM
Defender: Scenarios i	DEBRV	7.14E+08	1.37E+09	9.91E+08	8.41E+08	7.94E+08	7.77E+08
	NLRTM	1.37E+09	6.56E+08	9.34E+08	7.85E+08	7.36E+08	7.19E+08
	GBFXT	9.91E+08	9.34E+08	2.77E+08	4.06E+08	3.57E+08	3.40E+08
	BEANR	8.41E+08	7.85E+08	4.06E+08	1.28E+08	2.08E+08	1.91E+08
	BEZEE	7.94E+08	7.36E+08	3.57E+08	2.08E+08	8.05E+07	1.43E+08
	DEHAM	7.77E+08	7.19E+08	3.40E+08	1.91E+08	1.43E+08	6.27E+07

Attacker-Defender Model (ADM)

t	Intervention Strategy	Disruption costs z* (USD/week)	Marginal financial gains (USD/week)	Attack probabilities					
				DEBRV	NLRTM	GBFXT	BEANR	BEZEE	DEHAM
0	NONE	7.72E+08	-	0.91	0.09	0	0	0	0
1	DEBRV	6.82E+08	8.94E+07	0	0.9	0.1	0	0	0
2	NLRTM	3.06E+08	3.76E+08	0	0	0.77	0.23	0	0
3	GBFXT	1.61E+08	1.45E+08	0	0	0	0.57	0.31	0.12
4	BEANR	1.08E+08	5.29E+07	0	0	0	0	0.56	0.44
5	BEZEE	6.27E+07	4.52E+07	0	0	0	0	0	1
6	DEHAM	0.00E+00	6.27E+07	0	0	0	0	0	0

For disruption levels $\alpha_j \leq 20\%$, Felixstowe is the most critical port in the network with disruption costs ranging from 70.5 thousand USD/week (at defender flow diversion $\delta_i = 0\%$) up to 62.74 million USD/week (at $\delta_i = 100\%$). At this disruption level, Rotterdam is the second most critical port followed by Bremerhaven. Disruptions costs at Rotterdam are similar to those in Felixstowe ranging from 65.3 thousand USD/week at $\delta_i = 0\%$ up to 62.73 million USD/Week at $\delta_i = 100\%$.

For Bremerhaven, disruption costs at $\alpha_j \leq 20\%$ are lower when the defender does not divert any cargo flow (327 USD/week at $\delta_i = 0\%$ up to 62.67 million USD/Week at $\delta_i = 100\%$). This suggests that in the case study network, Felixstowe and Rotterdam

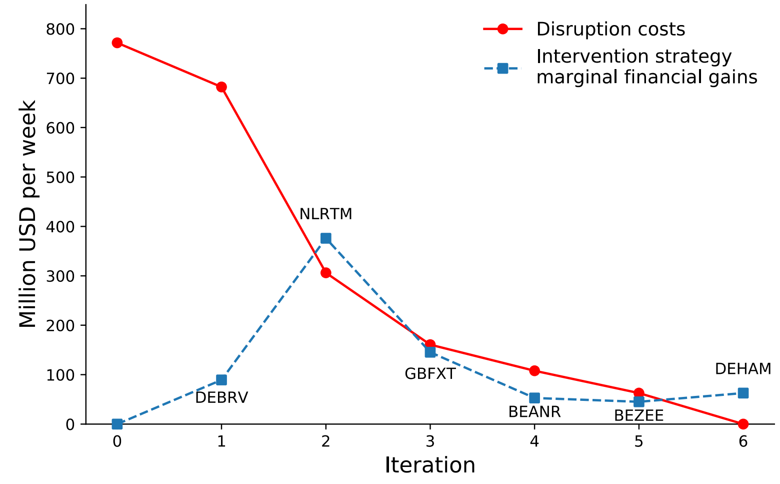


Fig. 4 Disruption costs and intervention financial gains

have less spare capacity to withstand disruptions that are lower than 20% when compared to Bremerhaven.

As shown in Figure 5, the criticality ranking of remaining ports in the network for $\alpha_j \leq 20\%$ is Antwerp (4th most critical), Zeebrugge (5th most critical), and Hamburg (6th most critical). Disruptions costs range from 0 USD/week when the defender does not divert any cargo flows ($\delta_i = 0\%$) to 62.6 million USD/week when the defender deviates all cargo flows to other terminals ($\delta_i = 100\%$).

For disruption levels α_j between 20% and 40%, Felixstowe remains the most critical port in the network with costs between 3.3 million USD/week (at $\delta_i = 0\%$) and 65.9 million USD/week (at $\delta_i = 100\%$). For this interval, Bremerhaven becomes the second most critical port, surpassing Rotterdam. For these two ports, disruptions costs range from 1.5 million USD/week (at $\delta_i = 0\%$) up to 64.5 million USD/week at $\delta_i = 100\%$. The criticality ranking of Antwerp, Zeebrugge remain unchanged at this disruption interval.

For the remaining ADCAM instances with disruption levels α_j greater than 60%, Bremerhaven becomes the most critical port of the network with disruption costs up to 771.5 million USD/Week ($\alpha_j = 100\,\%\,,\ \delta_i = 100\,\%$). Rotterdam remains as the second most critical port in the network with disruption costs up to 682.2 million USD/week whereas Felixstowe falls to the third position with disruption costs of up to 306.1 million USD/week.

Discussion

The available spare capacity in the network primarily drives the changes in criticality ranking of ports and overall disruption costs that each port must meet its inbound and outbound throughput as well as any transhipment cargo flows. Since Felixstowe operates with lower spare capacity, it is more susceptible to lower disruptions levels (e.g. $\alpha_j \leq 40\%$) when compared with Rotterdam and Bremerhaven. As such, it is the most critical port for lower disruption levels.

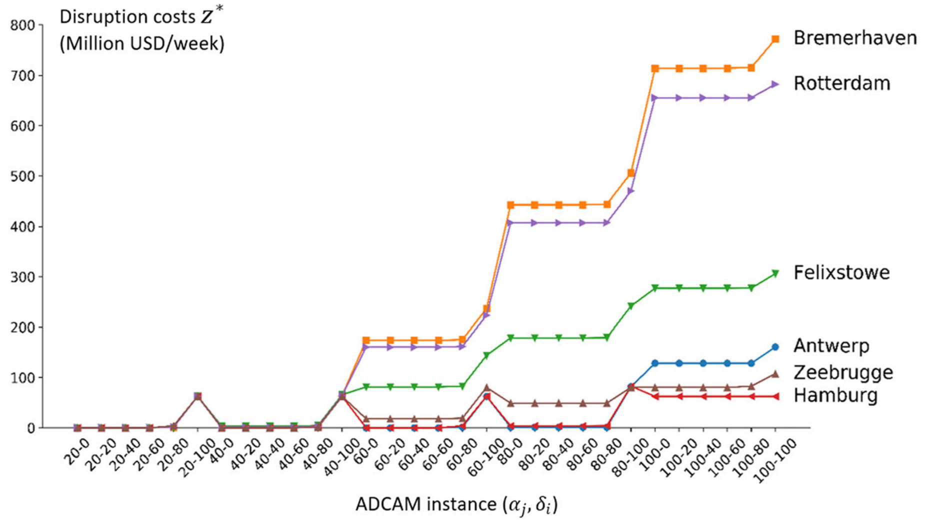


Fig. 5 Disruption costs for all ADCAM instances

In contrast, Bremerhaven and Rotterdam, which operate with more spare capacity, are capable of withstanding disruption levels below 40% without significantly increasing the overall network disruption costs. However, these ports surpass Felixstowe in the criticality ranking for disruptions levels above 60% due to the considerable number of containers affected when disruptions occur at Bremerhaven or Rotterdam.

These results are significantly influenced by the OD matrix input where most container flows are destined to Bremerhaven, Rotterdam, and Felixstowe. Consequently, disruptions in Antwerp, Zeebrugge, and Hamburg have less impact on the overall network vulnerability. The latter ports have lower inbound and outbound flows in the case study network (between 2.5 and 5.2 thousand TEU/week).

In the case study network, ports with high transhipment incidence in the baseline scenario (e.g. Antwerp with about 69%) are avoided following a disruption by using alternative paths. In contrast, Bremerhaven, Rotterdam, and Felixstowe have the characteristic feature of lower transhipment incidence (between 35 and 47%) and high inbound and outbound flows (between 18 and 50 thousand TEU/week). As such, interventions that prevent disruptions at these ports result in higher financial gains across the ADCAM instances evaluated.

Conclusions and further research

This study proposes a new framework capable of identifying the most critical network components and quantifying the systemic vulnerability of realistic large-scale liner shipping networks with limited or no historical disruption data available. To test the proposed family of models, we performed a numerical case study using a subset of the European port system.

Results indicate a significant concentration of attack probabilities in specific ports, rendering the evaluated port system particularly susceptible to disruptions. These outputs are significantly influenced by the characteristics of the case study OD matrix drawn from practice where most of the cargo flows are bound to a small number of import gateway ports in Europe. As such, disruptions in other regional ports with higher transhipment incidence have a lower impact on the overall system vulnerability.

We conducted a sensitivity analysis modifying the flow diversion strategies and the network disruption levels of the scenarios modelled. Key insights of this sensitivity evaluation demonstrated how regional criticality ranking can vary significantly depending on the available spare capacity of each port which dictates the terminal's capability to withstand disruptions. This allows us to identify network components that were more susceptible to lower levels of disruptions (e.g. Felixstowe in our case network) which are more common in practice and quantify financial gains from network interventions aimed at preventing disruptions in the most critical ports at various levels of disruptions.

The outputs of our proposed framework can, therefore, support the network design decision process of ocean carriers and other industry stakeholders (e.g. port operators and governments) establishing performance baselines and testing the effectiveness of interventions intended to increase the overall resilience of liner shipping networks. Examples of such interventions include the restructuring of liner service port calls and public-private investments aimed at increasing the spare capacity of critical container terminals.

Contrary to previous complex network pure-topological approaches, our framework provides an enhanced representation of liner shipping network operations under disruptions because it captures the re-distribution of container flows considering secondary paths and aggregating cost dependencies such as container transport costs and penalty costs for cargo not routed.

Interventions proposed by this study assume that it is possible to make centralised decisions on network structure when aiming to reduce exposure to disruptions. While this may be possible in some instances (e.g. an international financial institution allocating funds to port infrastructure in each region), in most cases, liner shipping stakeholders would be subject to competitive tendencies. Therefore, we identify the relationship between market dynamics and the collective actions that contribute to robustness against disruptions as a fertile ground for future work.

The maritime component of international shipping networks used in this study provides a good indication of overall liner service network vulnerability but do not capture hinterland intermodal connectivity links which can also serve as secondary paths between ports in regions such as Europe. Future improvements such as the inclusion of hinterland links and their corresponding costs can highlight relevant network vulnerabilities not captured in this study.

The ADM formulation and numerical implementations presented in this study provide the expected worst-case scenario for an ocean carrier against a single network attacker (global demon). However, given that in recent years global ocean carriers have consolidated into three mega alliances, the proposed analysis can be improved presenting a broader scope of the liner shipping industry where the worst-case scenario for the majority of liner services worldwide can be modelled using three attackers (e.g. one for each alliance).

Furthermore, as discussed in Schmöcker et al. (2009), the Spiess and Florian hyperpath concept used in the embedded linear program of CAM used in this study can be adapted to a non-cooperative game between a network router (e.g. the ocean carrier) and multiple node-specific attackers that can penalise individual links or legs exiting nodes.

Multiple node-specific demons can improve the limitation of the single attacker presented in this study which is only capable of penalising a single component anywhere in the network. This is an essential consideration in container liner networks where multiple node-specific demons can produce more realistic routing strategies (resulting from more than a single incident) avoiding nodes with longer total delays (Schmöcker et al. 2009).

Another future enhancement to the ADM proposed in this study is the formulation of less extreme attackers. As described in Bell et al. (2008), a logit model approach can be used to adjust the level of aggressiveness of attackers (or user pessimism) that a certain network component will fail in the network evaluated. This approach allows to depart from worst-case scenario analysis resulting from the formulation of extremely aggressive attackers or pessimistic users (as presented in this study) and provide a vulnerability assessment of transport networks exposed to less extreme events or test the functioning of the ADM methodology considering random disruptions such as accidents or natural disasters. Future improvements to this framework could also include the use of an $n+m$ player game structure where multiple carriers compete in cargo rerouting.

Abbreviations

ADCAM: Attacker-Defender and Container Assignment Integration Framework; ADM: Attacker-Defender Model; BEANR: Antwerp UNLOCODE; BEZEE: Zeebrugge UNLOCODE; CAM: Container Assignment Model; CPLEX: IBM ILOG CPLEX Optimization Studio; DEBRV: Bremerhaven UNLOCODE; DEHAM: Hamburg UNLOCODE; GBFXT: Felixstowe UNLOCODE; MC: Most Critical Network Component; NCGT: Non-cooperative Game Theory; NLRTM: Rotterdam UNLOCODE; OD: Origin-Destination; OPL: Optimisation Programming Language; PIANC: World Association for Waterborne Transport Infrastructure; PO: Pay-off Matrix; PORTeC: Port Operations Research and Technology Centre; TC: Timer charter; TEU: Twenty-foot Equivalent Unit; UNCTAD: United Nations Conference on Trade and Development; UNLOCODE: United Nations Code for Trade and Transport Locations; USD: United States Dollars

Acknowledgements

The authors extend their gratitude to the Georgia Tech Panama Logistics Innovation & Research Centre for contributing part of the data used in the study. We also thank colleagues at the Port Operations Research & Technology Centre of Imperial College London for their valuable feedback to previous versions of work.

Funding

The authors would like to thank the UK Engineering and Physical Sciences Research Council (EPSRC) for funding portions of this work. The corresponding author would like to thank the National Secretariat of Science Technology and Innovation of the Republic of Panama for the financial support received through research fellowship No. 2199-35-2012. No additional external funding was used to support the research presented in this study.

Availability of data and materials

The LINER-LIB dataset used in this study is publicly available at https://github.com/blof/LINERLIB/. Additional data used in this study can be obtained from the corresponding author on reasonable request.

Authors' contributions

All authors have directly contributed to the planning, analysis, and writing of the paper. All authors have read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 30 January 2019 Accepted: 29 April 2019
Published online: 13 June 2019

References

Achurra-Gonzalez PE, Angeloudis P, Zavitsas K, Niknejad A, Graham DJ (2017) Attacker-defender assessment of vulnerability in maritime logistics corridors. In: Ducruet C (ed) Advances in shipping data analysis and modeling. Tracking and mapping maritime flows in the age of big data. Routledge. https://www.taylorfrancis.com/books/e/9781315271446/chapters/10.4324/9781315271446-18.

Achurra-Gonzalez PE, Novati M, Foulser-Piggott R, Graham DJ, Bowman G, Bell MGH, Angeloudis P (2016) Modelling the impact of liner shipping network perturbations on container cargo routing: Southeast Asia to Europe application. Accid Anal Prev. https://doi.org/10.1016/j.aap.2016.04.030

Angeloudis P, Bichou K, Bell MGH, Fisk D (2007) Security and reliability of the liner container-shipping network: analysis of robustness using a complex network framework. In: Risk Management in Port Operations, Logistics and Supply Chain Security, pp 95–106

Angeloudis P, Fisk D (2006) Large Subway systems as complex networks. Phys A Stat Mech Appl 367:553–558. https://doi.org/10.1016/J.PHYSA.2005.11.007 North-Holland

Bartholdi JJ, Jarumaneeroj P, Ramudhin A (2016) A new connectivity index for container ports. Marit Econ Logistics 18(3):231–249. https://doi.org/10.1057/mel.2016.5 Palgrave Macmillan UK

Bell MGH (2000) A game theory approach to measuring the performance reliability of transport networks. Transp Res B Methodol 34(6):533–545. https://doi.org/10.1016/S0191-2615(99)00042-9

Bell MGH (2003) The use of game theory to measure the vulnerability of stochastic networks. IEEE Trans Reliab 52(1):63–68. https://doi.org/10.1109/TR.2002.808062

Bell MGH, Cassir C (2002) Risk-averse user equilibrium traffic assignment: an application of game theory. Transp Res Part B Methodol 36(8):671–681. https://doi.org/10.1016/S0191-2615(01)00022-4 Pergamon

Bell MGH, Kanturska U, Schmöcker J-D, Fonzone A (2008) Attacker–defender models and road network vulnerability. Philos Trans A Math Phys Eng Sci 366(1872):1893–1906. https://doi.org/10.1098/rsta.2008.0019

Bell MGH, Kurauchi F, Perera S, Wong W (2017) Investigating transport network vulnerability by capacity weighted spectral analysis. Transp Res Part B Methodol 99:251–266. https://doi.org/10.1016/J.TRB.2017.03.002 Pergamon

Bell MGH, Liu X, Angeloudis P, Fonzone A, Hosseinloo SH (2011) A frequency-based maritime container assignment model. Transp Res B Methodol 45(8):1152–1161. https://doi.org/10.1016/j.trb.2011.04.002

Bell MGH, Liu X, Rioult J, Angeloudis P (2013) A cost-based maritime container assignment model. Transp Res B Methodol 58:58–70. https://doi.org/10.1016/j.trb.2013.09.006

Bencomo LA (2009) Modeling the effects of a transportation security incident on the commercial transportation system. Naval Postgraduate School, Monterey https://calhoun.nps.edu/handle/10945/4648

Brouer BD, Fernando Alvarez J, Plum CEM, Pisinger D, Sigurd MM (2014) A Base Integer Programming Model and Benchmark Suite for Liner-Shipping Network Design. Transp Sci 48(2):281–312. https://doi.org/10.1287/trsc.2013.0471 INFORMS

Calatayud A, Mangan J, Palacin R (2017) Vulnerability of international freight flows to shipping network disruptions: a multiplex network perspective. Transp Res Part E Logistics Transp Rev 108:195–208. https://doi.org/10.1016/J.TRE.2017.10.015 Pergamon

Containerisation International (2012) Containerisation international yearbook 2012. Informa Maritime & Transport, London. ISBN 978184311906. https://unov.tind.io/record/28438?ln=en

Ducruet C (2016) The polarization of global container flows by interoceanic canals: geographic coverage and network vulnerability. Marit Policy Manag 43(2):242–260. https://doi.org/10.1080/03088839.2015.1022612

Ducruet C, Lee S-W, Ng AKY (2010) Centrality and vulnerability in liner shipping networks: revisiting the northeast Asian port hierarchy. Marit Policy Manag 37(1):17–36. https://doi.org/10.1080/03088830903461175

Ducruet C, Zaidi F (2012) Maritime constellations: a complex network approach to shipping and ports. Marit Policy Manag 39(2):151–168. https://doi.org/10.1080/03088839.2011.650718

Hollander Y, Prashker JN (2006) The applicability of non-cooperative game theory in transport analysis. Transportation 33(5): 481–496. https://doi.org/10.1007/s11116-006-0009-1

Hosseini S, Barker K, Ramirez-Marquez JE (2016) A review of definitions and measures of system resilience. Reliability Eng Syst Saf 145:47–61. https://doi.org/10.1016/j.ress.2015.08.006

Kanturska U, Angeloudis P (2013) Introduction to network theory and game theory as frameworks for the analysis of critical infrastructure. In: The Institution of Engineering and Technology. Infrastructure Risk and Resilience: Transportation, pp 22–28. https://doi.org/10.1049/PERIRR3E_ch3

Kjeldsen KH, Ergun O, Lysgaard J, Erera A (2011) Rescheduling ships and cargo in liner shipping in the event of disruptions. Liner Shipping, p. 105.

Mattsson L-G, Jenelius E (2015) Vulnerability and resilience of transport systems – a discussion of recent research. Transp Res Part A Policy Pract 81:16–34. https://doi.org/10.1016/J.TRA.2015.06.002 Pergamon

Muriel-Villegas JE, Alvarez-Uribe KC, Patiño-Rodríguez CE, Villegas JG (2016) Analysis of transportation networks subject to natural hazards – insights from a Colombian case. Reliability Eng Syst Saf 152:151–165. https://doi.org/10.1016/j.ress.2016.03.006

Ouyang M, Zhao L, Pan Z, Hong L (2014) Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks. Phys A Stat Mech Appl 403:45–53. https://doi.org/10.1016/j.physa.2014.01.070

Paul JA, Maloni MJ (2010) Modeling the Effects of Port Disasters. Maritime Economics & Logistics 12(2):127–146. https://doi.org/10.1057/mel.2010.2 Palgrave Macmillan UK

PIANC (2017) Resilience of the maritime and inland waterborne transport system. In: The world Association for Waterborne Transport Infrastructure

Qi X (2015) Disruption Management for Liner Shipping. In: Lee C-Y, Meng Q (eds) Handbook of ocean container transport logistics: making global supply chains effective. International Series in Operations Research & Management Science. Springer International Publishing, pp 231–249 https://link.springer.com/chapter/10.1007/978-3-319-11891-8_8

Qiao W, Lu Y, Xiong C, Haghani A (2014) A game theory approach for the measurement of transport network vulnerability from the system prospective. Transp B Transpt Dyn 2(3):188–202. https://doi.org/10.1080/21680566.2014.929058

Reggiani A, Nijkamp P, Lanzi D (2015) Transport resilience and vulnerability: the role of connectivity. Transp Res Part A Policy Pract 81:4–15. https://doi.org/10.1016/J.TRA.2014.12.012 Pergamon

Schmöcker J-D, Bell MGH, Kurauchi F, Shimamoto H (2009) A game theoretic approach to the determination of Hyperpaths in transportation networks. In: Transportation and traffic theory 2009: Golden Jubilee. Springer US, Boston, MA, pp 1–18. https://doi.org/10.1007/978-1-4419-0820-9_1

Sullivan JL, Novak DC, Aultman-Hall L, Scott DM (2010) Identifying critical road segments and measuring system-wide robustness in transportation networks with isolating links: a link-based capacity-reduction approach. Transp Res A Policy Pract 44(5):323–336. https://doi.org/10.1016/j.tra.2010.02.003

Taylor MAP (2012) Network vulnerability in large-scale transport networks. Transp Res Part A Policy Pract 46(5):743–745. https://doi.org/10.1016/j.tra.2012.02.001 Network vulnerability in large-scale transport networks

Tsavdaroglou M, Al-Jibouri SHS, Bles T, Halman JIM (2018) Proposed Methodology for Risk Analysis of Interdependent Critical Infrastructures to Extreme Weather Events. Int J Crit Infrastructure Prot 21:57–71. https://doi.org/10.1016/J.IJCIP.2018.04.002 Elsevier

UNCTAD (2017) Review of maritime transport 2017. United Nations Conference on Trade and Development (UNCTAD). Geneva. ISBN 978-92-1-112922-9.

Viljoen NM, Joubert JW (2016) The vulnerability of the global container shipping network to targeted link disruption. Phys A Stat Mech Appl 462:396–409. https://doi.org/10.1016/j.physa.2016.06.111

Wang Q (2012) Game theory approach to transportation network vulnerability measurement. University of Connecticut https://opencommons.uconn.edu/gs_theses/211/

Zavitsas K (2011) The vulnerability of the petroleum supply chain. Imperial College, London