Assessing the vulnerability of military theater distribution routes

Joshua R. Muckensturm and Dave C. Longhorn
*Joint Distribution Process Analysis Center, US Transportation Command,
Scott AFB, Illinois, USA*

Received 27 July 2018
Revised 7 December 2018
15 January 2019
Accepted 16 January 2019

Abstract

Purpose – This paper introduces a new heuristic algorithm that aims to solve the military route vulnerability problem, which involves assessing the vulnerability of military cargo flowing over roads and railways subject to enemy interdiction.

Design/methodology/approach – Graph theory, a heuristic and a binary integer program are used in this paper.

Findings – This work allows transportation analysts at the United States Transportation Command to identify a relatively small number of roads or railways that, if interdicted by an enemy, could disrupt the flow of military cargo within any theater of operation.

Research limitations/implications – This research does not capture aspects of time, such as the reality that cargo requirements and enemy threats may fluctuate each day of the contingency.

Practical implications – This work provides military logistics planners and decision-makers with a vulnerability assessment of theater distribution routes, including insights into which specific roads and railways may require protection to ensure the successful delivery of cargo from ports of debarkation to final destinations.

Originality/value – This work merges network connectivity and flow characteristics with enemy threat assessments to identify militarily-useful roads and railways most vulnerable to enemy interdictions. A geographic combatant command recently used this specific research approach to support their request for rapid rail repair capability.

Keywords Military route vulnerability, Graph theory, Shortest path, Betweenness, Binary integer programming, Heuristics

Paper type Research paper

Introduction

The United States Transportation Command is responsible for identifying vulnerabilities to distribution operations and recommending mitigations (US Joint Chiefs of Staff, 2017). A complex aspect of distribution operations is theater distribution, which is the movement of military cargo over supply routes consisting of roads and railways in an environment likely to be contested by an enemy. Ground assets such as trucks and railcars are the most common means of delivering cargo over military supply routes, which are often vulnerable to enemy interdiction by direct attacks, such as missiles, and indirect attacks, such as cyber operations. A challenge for analysts at the United States Transportation Command is to identify which segments of the theater's

Journal of Defense Analytics and Logistics
Vol. 3 No. 1, 2019
pp. 60-82
Emerald Publishing Limited
2399-6439
DOI 10.1108/JDAL-07-2018-0012

extensive network, often consisting of several thousand nodes connected by roads and railways, are most vulnerable to enemy interdiction given credible threat intelligence estimates. Analysts at the command have informally termed this transportation problem the military route vulnerability problem (MRVP), which is the focus of this paper.

The computational difficulty of identifying critical nodes or edges in networks has been studied extensively (Myung and Kim, 2004; Di Summa *et al.*, 2011; Shen *et al.*, 2012; Dinh *et al.*, 2012), with optimal solutions often intractable for large problems. As such, non-optimal heuristic approaches are usually employed to identify critical elements of large networks. In this paper, a heuristic is developed using a similar approach to solve large instances of the MRVP, which considers three components:

1. topology of roads and railways representing the possible theater distribution routes;
2. a time-phased force deployment and data (TPFDD) describing the military cargo flow requirements from ports of debarkation (PODs) to destinations, otherwise known as tactical assembly areas (TAAs); and
3. intelligence estimates of enemy threats capable of interdicting the network.

The methods used in this paper are rooted in eighteenth-century graph theory concepts, as first posed by Leonhard Euler in his solution of the bridges of Konigsberg problem (Sachs *et al.*, 1988). The graph theory methods used are shortest paths and betweenness. A shortest path in the context of military theater distribution refers to the route between a POD and TAA such that the distance traveled is minimal. Edge betweenness captures the notion of centrality within a graph, i.e. by counting the number of times each edge resides on the shortest path between POD and TAA requirements in the network.

In addition, this paper introduces a binary integer program (BIP) formulation of the MRVP, which is structurally similar to the critical edge detection problem. The MRVP, however, includes the added consideration that some edges may reside within an enemy's threat range. Most notably, the heuristic algorithm aims to solve large instances of the MRVP, which would be computationally inefficient to solve using the BIP. The BIP solution is compared to the heuristic solution for two relatively small problem instances to offer evidence that the heuristic provides meaningful insights. Finally, the heuristic algorithm is tested on a large-scale MRVP, which is indicative of the problems encountered by analysts at the United States Transportation Command.

Literature review

Route vulnerability, particularly with respect to roads, has been the focus of much research. Various definitions have been proposed for transportation network reliability, vulnerability and criticality (Berdica, 2002; Khademi *et al.*, 2015; Rupi *et al.*, 2015). A common theme of such definitions is that the likelihood of network disruption (i.e. the reliability of a specific node or edge in the network) and the resulting consequences of the disruption should both be considered when identifying critical network nodes and edges.

Various solution approaches have been used to identify critical nodes, or alternatively edges, in networks. The reader is directed to the works of Lalou *et al.* (2018) and Pavlikov (2018), who thoroughly reviewed the solution approaches for the critical node (or edge) detection problem. Exact solution methods using linear programming or integer programming (IP) were employed by numerous authors. Myung and Kim (2004) solved the *k*-edge survivability of traffic networks. Murray *et al.* (2007) determined lower and upper bounds on network flow and connectivity disruptions for fiber-optic telecommunications networks; whereas, Matisziw and Murray (2009) determined an upper bound on similar disruptions in the context of disaster management.

Demšar *et al.* (2008) identified and ranked critical locations using betweenness and cut vertices; and Shen *et al.* (2012) deleted subsets of nodes to maximize the disconnectivity of the associated graph. These exact solution methods enabled Shen *et al.* (2013) to identify critical nodes and links vulnerable to unexpected disruptive events or deliberate adversarial attacks and Veremyev *et al.* (2014) to consider both node and edge deletions simultaneously.

Due to the computational challenges of exact solution methods, researchers have also employed heuristics or simulation approaches to identify critical nodes or edges in large networks. Arulselvan *et al.* (2009) used a heuristic to detect critical nodes in sparse graphs and then compared the results to the optimal solution from an IP formulation of the critical node problem. Ventresca and Aleman (2015) used a greedy algorithm with a priority queue to identify critical nodes and edges in large complex networks. Employing a greedy algorithm with path relinking, Purevsuren *et al.* (2016) solved the critical node detection problem. Yu *et al.* (2017) proposed an algorithm to identify critical nodes in a network based on minimum connected dominating sets, specifically choosing the critical node based on its close subsequences. Finally, Matisziw *et al.* (2009) employed a simulation approach to assess the vulnerability of network flow and connectivity, with the authors suggesting that a simulation approach provides meaningful vulnerability insights across a range of disruption scenarios for network problems too large to solve using mathematical optimization.

Although the MRVP has not been directly addressed in the literature, several researchers have extensively studied transportation network vulnerability. Gao *et al.* (2012) examined travel time reliability in the context of military transportation networks. Similarly, Reggiani (2013) offered a framework to integrate network resilience with transport security, and Reggiani *et al.* (2015) proposed a methodological framework to address resiliency and vulnerability concepts. A comprehensive analysis of the vulnerability and resiliency of transport systems was offered by Mattsson and Jenelius (2015), who integrated spatial methods of graph theory with aspects of supply and demand over transportation routes. Also, Zhao *et al.* (2018) used a sample average approximation method to study route planning for military ground vehicles over road networks subject to enemy interdiction.

The research referenced above was instrumental in developing the heuristic algorithm and BIP formulation to solve the MRVP. This algorithm specifically adopts the common theme that both network topology and flow are important factors in identifying critical routes in the transportation network. In addition, it leverages the work of Zhao *et al.* (2018), who allowed alternative destinations to ensure intact routes from the origins; however, the MRVP conversely permits alternative PODs because decision-makers can more easily reroute cargo to different PODs if the original route to the TAA should be interdicted. An idea not referenced in the literature, but certainly applicable to the MRVP, is that an enemy's capability and intent to disrupt network routes also influences which roads and railways are most critical. Therefore, the heuristic algorithm and associated BIP identify critical roads and railways using the topological concepts of shortest path and betweenness, network flow between specific PODs and TAAs and military-specific considerations that allow alternative PODs to keep cargo flowing and give higher relative criticality weights to roads and railways within enemy threat ranges.

Methods

Notation

The MRVP heuristic algorithm involves edge interdictions and network flow assessments. Let the algorithm iteration number be indexed by n, with the first iteration ($n = 1$) involving a baseline network flow assessment with no edge interdiction and subsequent iterations ($n > 1$) each requiring a single edge interdiction followed by a network flow assessment.

The set of TPFDD requirements I is indexed by i. The amount of cargo associated with requirement i, measured in short tons, is represented as C_i. Each requirement originates at a POD, which is either a seaport or an airport. Let PS be the set of all TPFDD seaports and let $PS_i \in PS$ be the TPFDD seaport for requirement i, if requirement i originates at a seaport. Similarly, let PA be the set of all TPFDD airports and let $PA_i \in PA$ be the TPFDD airport for requirement i, if requirement i originates at an airport. Each requirement is to be delivered to a destination node, so let D represent the set of TPFDD destinations and let $D_i \in D$ be the TPFDD destination for requirement i.

The destination is fixed because that location is where the combat capability is required by the geographic combatant commander. However, alternative starting PODs are permissible in the MRVP algorithm, because cargo can enter the theater from different ports provided enough advanced warning is given about expected network interdictions. Thus, let QS represent the set of alternative seaports and let $QS_i \in QS$ represent an alternative seaport for requirement i, if requirement i originates at a seaport. Similarly, let QA represent the set of alternative airports and let $QA_i \in QA$ represent an alternative airport for requirement i, if requirement i originates at an airport. Substituting an alternative port for the TPFDD port is permitted only under specific operational conditions:

- No path exists from the TPFDD port to destination due to successive network edge interdictions.
- Using an alternative port results in a feasible path to the destination.

In addition, the alternative port selected is assumed to have the minimal route distance to the destination from among the possible alternative ports.

Alternative ports from the sets QS and QA may be substituted for TPFDD ports from the sets PS and PA, respectively, during algorithm execution to keep cargo flowing given successive edge interdictions. As such, the possible ports under consideration for network assessments may change as the iteration n increases. Therefore, let W_n be the set of ports (seaports and airports) for the requirements still flowing at iteration n. Similarly, let $W_{n,i}$ represent the selected port at iteration n for requirement i with $W_{n,i} \in W_n$, as defined in equation (1):

$$W_{n,i} = \begin{cases} PS_i \text{ if a path from } PS_i \text{ to } D_i \\ QS_i \text{ if no path from } PS_i \text{ to } D_i \text{ but a path from } QS_i \text{ to } D_i \\ PA_i \text{ if a path from } PA_i \text{ to } D_i \\ QA_i \text{ if no path from } PA_i \text{ to } D_i \text{ but a path from } QA_i \text{ to } D_i \\ \varnothing \text{ if no path from any } \mathit{TPFDD} \text{ port or alternative port to } D_i \end{cases} \tag{1}$$

The entire theater distribution network is composed of road and rail networks; however, the algorithm assesses the route vulnerability of each network separately. Therefore, no distinction in notation is required among the edges in the road or rail network. Let E represent the set of all edges in the network and let $e \in E$ represent an edge in the network. Also, let $S_{n,i}$ be the ordered set of edges representing the shortest path (i.e. minimal distance) for requirement i from port $W_{n,i}$ to destination D_i at iteration n. Likewise, let $R_{n,i}$ reflect the total route distance, measured in miles, of the shortest path $S_{n,i}$. If no route exists to deliver requirement i at iteration n, then let $R_{n,i} = 0$. Another useful flow variable is the Boolean $H_{n,i}$

indicating there is no feasible path to deliver requirement i at iteration n, as defined in equation (2):

$$H_{n,i} = \begin{cases} 1 \text{ if } S_{n,i} = \varnothing \\ 0 \text{ if } S_{n,i} \neq \varnothing \end{cases} \tag{2}$$

The first vulnerability consideration for the MRVP is the spatial network of edges, specifically whether the edge resides on a requirement's shortest path without regard to how much cargo is flowing over the edge. Let the Boolean variable $B_{n,e,i}$, as defined in equation (3), denote if edge e is on the shortest path $S_{n,i}$ for requirement i at iteration n:

$$B_{n,e,i} = \begin{cases} 1 \text{ if } e \in S_{n,i} \\ 0 \text{ if } e \notin S_{n,i} \end{cases} \tag{3}$$

The second vulnerability consideration is the flow of military cargo over the network. Let $A_{n,e,i}$, as defined in equation (4), represent the amount of cargo associated with requirement i that travels over edge e based on its membership in shortest path $S_{n,i}$ at iteration n. As such, $A_{n,e,i}$ gives more importance to edges in the network with higher cargo flows:

$$A_{n,e,i} = \begin{cases} C_i \text{ if } e \in S_{n,i} \\ 0 \text{ if } e \notin S_{n,i} \end{cases} \tag{4}$$

The final vulnerability consideration is the laydown of enemy threats capable of interdicting the network. Let $T_e = 1$ for an edge e that resides outside the enemy threat range and, conversely, let $T_e = U$ represent an edge e within the enemy threat range with U being some user-defined multiplier ($U > 1$). A higher value of U represents higher confidence in the credibility of the military intelligence estimates.

Measures

The route vulnerability algorithm uses three primary measures. Each measure depends on the algorithm iteration number n. The first measure is *edge vulnerability* (EV), which is calculated for each edge used to move cargo over the network. The EV is a composite metric at each iteration n calculated by multiplying:

- the number of times edge e resides on the shortest path between the assigned PODs and TAAs;
- the total amount of cargo traversing edge e; and
- a user-defined multiplier that gives higher relative weight if edge e resides within the enemy threat range.

The EV metric is defined in equation (5):

$$EV_{n,e} = \left(\sum_i B_{n,e,i}\right)\left(\sum_i A_{n,e,i}\right) T_e \tag{5}$$

Higher values of the EV metric suggest the edge is more critical, or vulnerable, to the flow of military cargo over the network. The EV metric is critical for ranking each edge e in the network for interdiction (i.e. removal) at each algorithm iteration n. Finally, the EV metric is used internally by the algorithm and is not reported as an output measure.

The second measure is *cargo rerouting* (CR), which is an aggregate output at each iteration n that reports the change in ton-miles due to successive interdictions. Ton-miles is a common metric for freight distribution (US Department of Transportation, 2018), because it captures both the magnitude of cargo flowing over the network and the associated distance. The ton-miles value is calculated as the sum of the tonnage of each requirement multiplied by its corresponding route distance between POD and TAA. The CR metric is defined in equation (6):

$$CR_n = \sum_i C_i R_{n,i} \tag{6}$$

Higher relative values of the CR metric suggest a more complicated military theater distribution, because the cargo will usually be transported over longer distances due to rerouting. The CR metric need not increase among successive iterations, because cargo requirements without a path will have a route distance of zero and the associated cargo amount will not contribute to the CR metric. Instances of rerouting cargo is a desired effect of enemy route interdictions, because rerouting complicates the theater distribution mission for the geographic combatant commander with longer cargo distribution routes and possibly increased exposure to enemy threats (US Joint Chiefs of Staff, 2016); however, the cargo is still deliverable to the TAA.

The final measure is *cargo halting* (CH), which is an aggregate output at each iteration n that reports the percent of total cargo that is not deliverable due to successive edge interdictions. The CH metric is defined in equation (7):

$$CH_n = \frac{\sum_i H_{n,i} C_i}{\sum_i C_i} \tag{7}$$

Higher relative values of the CH metric suggest a more interdicted network resulting in more cargo undeliverable to TAAs. In addition, the CH metric is monotonically non-decreasing as the iteration number n increases, because successive edge interdictions will result in either the same amount of cargo delivered, albeit using a different route, or more cargo undelivered. Instances of cargo being halted are more concerning to a geographic combatant commander than instances of cargo rerouting.

Assumptions

TPFDD ports, alternative ports and destinations are assumed to be well fortified and protected, e.g. armed guards to deter sabotage, defense systems to intercept missile strikes. As such, the immediate two edges out of PODs and the immediate two edges into TAAs are assumed to be excluded from interdiction during algorithm execution. Similarly, Zhao *et al.* (2018) assumed origins were protected, but that road transit over the network would be subject to the highest chance of enemy threat interdictions.

All road or rail segments within the enemy threat ring are equally at risk of attack. Also, the length of a segment is not a factor in which segment will be interdicted. Although shorter segments are susceptible to interdiction via concentrated kinetic attacks, the longer segments are more susceptible to interdiction via asymmetrical attacks, including sabotage (US Joint Chiefs of Staff, 2013).

The TPFDD is time-phased, i.e. requirements are specified with a set of dates that reflect when cargo is scheduled to depart the POD and when cargo should arrive at the

TAA. However, the route vulnerability algorithm does not consider time in any sense, but instead collapses the spatial and temporal aspects of the TPFDD into a more computationally feasible spatial problem of total requirements flowing over a contested road or rail network subject to route interdictions. The algorithm's exclusion of time is a limitation if intelligence estimates on the timing of enemy threats and network attacks are known with precision, which is rarely the case. Conversely, the ability of the algorithm to give quick insights into network vulnerabilities offsets this perceived limitation to some degree.

Heuristic pseudocode

The following pseudocode outlines the MRVP heuristic algorithm:

```
Algorithm Military Route Vulnerability
 1: build set $E$ given road or rail network
 2: assign $n = 1$
 3: build set $I$
 4: Set $L \leftarrow \emptyset$
 5: repeat
 6:      build set $W_n$
 7:      if $n > 1$
 8:           remove $m_{n-1}$ from $E$
 9:      end if
10:      for each $i \in I$
11:           compute $S_{n,i}$ from $W_{n.i}$ to $D_i$
12:           if $S_{n,i} \neq \emptyset$
13:                assign $H_{n,i} = 0$ and compute $R_{n,i}$
14:                for each $e \in S_{n,i}$
15:                     assign $A_{n,e,i} = C_i$ and $B_{n,e,i} = 1$
16:                     if $e$ in threat ring
17:                          assign $T_e = U$
18:                     else
19:                          assign $T_e = 1$
20:                     end if
21:                end for
22:           else if $\exists S_{n,i}$ from alternative ports
23:                assign $W_{n+1,i}$ to alternative port
                          having the minimum distance
24:                repeat steps 12-20
25:           else
26:                assign $H_{n,i} = 1$ and $R_{n,i} = 0$
27:           end if
28:    end for
29:    compute $CR_n$ and $CH_n$
30:    compute $EV_{n,e}$ for each $e$
31:    $m_n = \textbf{argmax}\{EV_{n,e}\}$
32:    $L \leftarrow L \cup \{m_n\}$
33:    for each $i$ with $H_{n,i} = 1$
34:         remove $i$ from $I$
35.    end for
36:    $n \leftarrow n + 1$
37: until $I = \emptyset$
38: output $L$
```

Binary integer program formulation

A BIP formulation was created specifically to validate the heuristic algorithm for small problems, as presented in the Results section. The BIP identifies the minimal number of edges that, if interdicted, would halt the most cargo flow given enemy threats to specific network edges. Cargo rerouting is not an explicit goal of the BIP, because the BIP will always interdict as many edges as necessary to halt all cargo flow. The notation for the BIP is as follows:

$i \in I$ = set of all TPFDD requirements;

$e \in E$ = set of edges among network nodes (PODs, transshipment nodes, and TAAs);

α = user-defined scalar in the objective function applied to the halted cargo;

β = user-defined scalar in the objective function applied to the edges not interdicted;

C_i = cargo flow for requirement i;

g = generic path index with caveat that $g = 1$ represents the original TPFDD shortest path;

G_i = number of paths for requirement i from POD (TPFDD or alternative) to TAA;

$P_{i,g}$ = ordered list of edges of path g for requirement i; sorted from shortest to longest path;

f = number of edges in the network; and

M = arbitrarily large value (big-M) to control constraints

$$T_e = \begin{cases} U \text{ if edge } e \text{ resides in an enemy threat range } (U > 1) \\ 1 \text{ otherwise} \end{cases}$$

$$X_e = \begin{cases} 1 \text{ if edge } e \text{ is interdicted} \\ 0 \text{ otherwise} \end{cases}$$

$$Y_{i,g} = \begin{cases} 1 \text{ if path } g \text{ for requirement } i \text{ is taken} \\ 0 \text{ otherwise} \end{cases}$$

$$Z_{i,g} = \begin{cases} 1 \text{ if path } g \text{ for requirement } i \text{ is closed} \\ 0 \text{ otherwise} \end{cases}$$

$$V_i = \begin{cases} 1 \text{ if some path exists for requirement } i \\ 0 \text{ otherwise} \end{cases}$$

The BIP formulation is specified in equations (8)-(15):

$$\text{Maximize} \sum_{i \in I} \alpha(C_i(1 - V_i)) + \beta\left(f - \sum_{e \in E} X_e\right) + \sum_{e \in E} (T_e - 1)X_e \tag{8}$$

subject to:

$$\sum_{e \in E} X_e \leq f \tag{9}$$

$$\sum_{e \in P_{i,g}} X_e \geq Z_{i,g} \ \forall i \forall g \tag{10}$$

$$\sum_{g=1}^{G_i} Y_{i,g} = V_i \ \forall i \tag{11}$$

$$Y_{i,g} + Z_{i,g} \leq 1 \ \forall i \forall g \tag{12}$$

$$\sum_{g=1}^{G_i} \left(1 - Z_{i,g}\right) \leq MV_i \ \forall i \tag{13}$$

$$\mathrm{X}_e \in \{0,1\} \ \forall e \tag{14}$$

$$V_i \ \in \{0,1\} \ \forall i \quad Y_{i,g} \ \in \{0,1\} \ \forall i \forall g \ \ Z_{i,g} \ \in \{0,1\} \ \forall i \forall g \tag{15}$$

The objective function in equation (8) is a composite equation of three separate components with the first two components multiplied by the user-defined scalars, α and β, with $\alpha \gg \beta \gg 1$. The first component reflects halted flow with the larger multiplier, given by α, which is the primary goal of the BIP. The second component suggests using the fewest edge interdictions to disrupt the cargo flow, which is influenced by the smaller multiplier β. The final component gives preference to edge interdictions within the enemy's threat range. Equation (9) constrains the maximum number of edge interdictions possible, and equation (10) allows a specific path g to be interdicted. Equation (11) forces cargo flow over only one path if it exists, and equation (12) prevents each path g from being both taken and interdicted. Equation (13) forces flow if a path is available. Equations (14) and (15) enforce binary constraints on the variables.

Results

The results presented are based on notional, unclassified theater distribution scenarios. A typical MRVP is within an overseas country that is likely to be contested by an enemy; however, the notional scenarios in this paper are entirely within the USA to avoid security classification issues. The notional scenarios described in this section show the accuracy and efficiency of the MRVP heuristic.

Scenario #1 description

Scenario #1 involves moving military cargo from US seaports to inland destinations using militarily-useful roads, although a similar analysis may be conducted using the militarily-useful railways. These roads consist of 112 segments and 98 intersections (Figure 1), which represent a small subset of the entire US network and the first component of the algorithm.

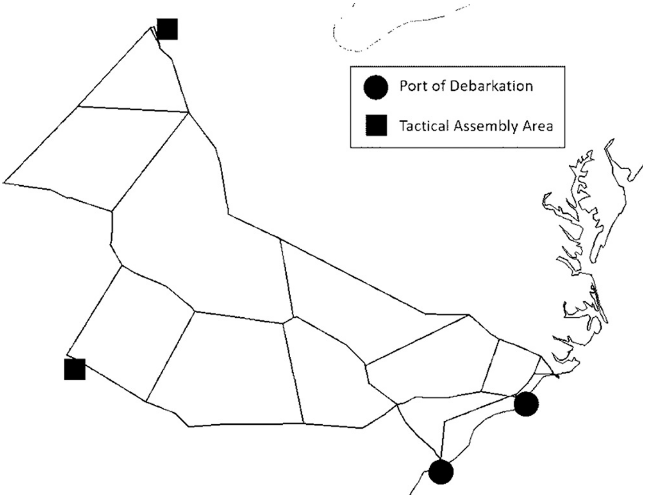

Figure 1. Scenario #1 topological representation of road routes

A road in Figure 1 may contain more than one segment. Figure 1 also shows the two PODs and two TAAs in Scenario #1.

The cargo flowing over the network represents the second component of the algorithm. This notional scenario contains four distinct POD to TAA requirements, as reflected in Table I. The algorithm also allows the use of alternative ports in the event the enemy interdicts the route between the TPFDD POD and TAA. For Scenario #1, the allowable alternative ports can be any port used in the TPFDD requirements. The ports in this scenario consist of only seaports; therefore, the alternative seaports available for each requirement are restricted to Charleston and Wilmington.

The final component of the MRVP heuristic algorithm is the enemy threat range based on available military intelligence of enemy capabilities and intent to disrupt the flow of military cargo. In Scenario #1, the intelligence indicates a single enemy threat ring with a radius of 142.4 nautical miles, as shown by the shaded area in Figure 2.

To test the accuracy of the MRVP heuristic algorithm, two separate runs (Run A and Run B) were conducted using Scenario #1. Run A included the first two components of the algorithm, i.e. topology and associated cargo flow. Run B incorporated an enemy threat ring. The comparison of these two runs showed the added value of considering credible enemy attack capabilities to solve the MRVP. Next, the BIP results were compared to the Run B heuristic results to assess the credibility of the heuristic given the same network components of topology, flow, and threat intelligence. The geographical locations of each run's interdictions were also provided at the end of this section.

Requirement	POD	TAA	Cargo Tonnage
1	Charleston	FT Sheridan	32,912.5
2	Wilmington	FT Sheridan	34,822.2
3	Charleston	Memphis	34,882.3
4	Wilmington	Memphis	33,672.9

Table I. Scenario #1 requirements

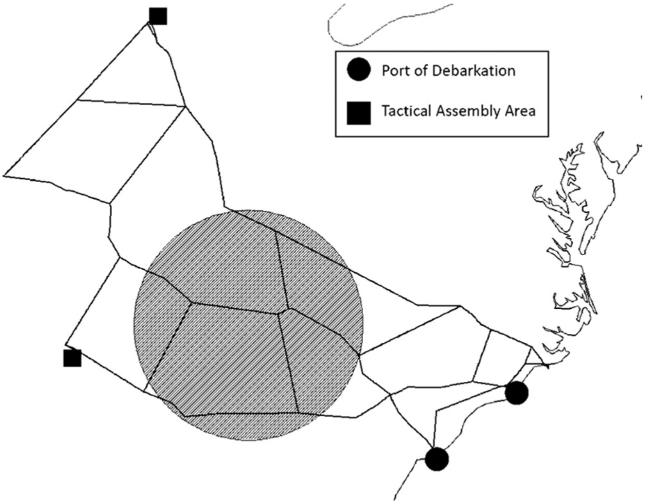

Figure 2.
Scenario #1 enemy threat ring indicated by shaded circle

Scenario #1 – Run A results

In Run A, the algorithm is executed without enemy threats, which means $T_e = 1$ for all edges in the network. Such situations exist when there is no credible enemy threat intelligence available, so all roads have the same likelihood of interdiction. Run A identified four critical roads out of 112 total roads (or about 4 per cent) that may halt 100 per cent of the cargo flow over the network. Such information suggests the enemy could cause serious disruption to the network by interdicting about four per cent of the network.

The two output measures at each iteration of the algorithm, cargo halted and cargo rerouted, are shown in Table II with the specific roads interdicted at each iteration.

The two measures provide meaningful insights to logistics planners and decision-makers. If an edge is interdicted and does not affect the amount of cargo halted, the cargo rerouting measure generally increases, because a longer path is found. However, if an interdiction results in some amount of cargo being halted, the associated cargo rerouting measure drops, because there is less total cargo transported over the network. There may be instances of the cargo rerouting measure dropping without cargo being halted, which occurs when the algorithm finds an alternative POD that is closer to the TAA than the previously used POD. These instances occur when no available path from the previously used POD to its TAA could be found.

Table II.
Scenario #1 – Run A measures

No. of roads interdicted	Road name	Cargo halted (%)	Cargo rerouted (ton-miles)
0		0	1.10E + 08
1	I20 + 15,891-28,300	0	1.19E + 08
2	I26 + 15,776-28,373	0	1.41E + 08
3	road-53,363	0	1.45E + 08
4	road-53,365	100	0

Scenario #1 – Run B results

When including enemy threats, the algorithm identified just three roads (or about 3 per cent) that, if interdicted, could halt all cargo flow. The user-defined multiplier (U) selected for this run was 10; therefore, $T_e = 10$ for each edge within the threat ring. The two output measures, cargo halted and cargo rerouted, at each iteration are shown in Table III with the names of the interdicted roads.

Each of the three identified critical roads are within the threat ring. Interestingly, the critical roads identified in Run A and Run B are mutually exclusive. The critical roads identified in Run A are also not within the threat ring provided in Run B. Thus, the critical roads identified in Run A without regard to credible enemy threats may falsely identify vulnerabilities outside the enemy's conceivable threat range. This observation suggests the importance of considering enemy threats within MRVPs.

Binary integer program results

To validate the MRVP heuristic algorithm, the BIP was used to identify the optimal solution for Scenario #1 with the enemy threats included. The user-defined values for the BIP were $U = 10$, α =1,000 and β =100. The BIP requires an enumerated set of all possible paths from each POD to TAA requirement, as reported in Table IV. The computational time required to enumerate the paths grows considerably as the problem size increases. Each of these paths contain 40-70 individual road segments.

The BIP reports the minimum number of road interdictions to halt all cargo flow. The optimal results for Scenario #1, as shown in Table V, report three critical roads out of the 112 total possibilities, i.e. interdicting these three roads would halt 100 per cent of the cargo flow. More importantly, two of the three critical roads identified were the same roads identified by the MRVP algorithm in Run B. The third edge of the BIP (i.e. "I640 ± 5,840") was arbitrarily selected as it resides on the same stretch of road segments as the remaining critical road (i.e. "road-53353") identified by the algorithm in Run B; therefore, the interdiction of either of these roads on the same stretch would result in the same amount of network disruption. The BIP results suggest that the heuristic algorithm correctly identifies network vulnerabilities, because:

No. of roads interdicted	Road name	Cargo halted (%)	Cargo rerouted (ton-miles)	Within threat ring?
0		0	1.10E + 08	
1	I20 + 4,553-9,587	0	1.19E + 08	Yes
2	road-53,353	0	1.51E + 08	Yes
3	road-53,369	100	0	Yes

Table III. Scenario #1 – Run B measures

Requirement	POD	TAA	No. of paths
1	Charleston	FT Sheridan	5,064
2	Wilmington	FT Sheridan	5,640
3	Charleston	Memphis	2,784
4	Wilmington	Memphis	3,120

Table IV. Number of paths per requirement in scenario #1

- the same number of road interdictions were required to halt all cargo flow;
- the specific roads interdicted were identical or arbitrarily similar; and
- all interdictions were within the enemy's threat range.

Scenario #1 – Geographical locations of interdictions

An overlay of each of the run's interdiction locations is provided in this section. Figure 3 shows the road segments identified as critical in Run A, which excluded threat intelligence.

When considering the threat intelligence, the MRVP algorithm identified road segments within the threat ring as critical. Figure 4 shows the geographical locations of the road segments interdicted in Run B, while Figure 5 shows the geographical locations of the road segments identified by the BIP. The locations of the interdictions from the algorithm and BIP are fairly similar.

Scenario #2 description

This scenario has the same PODs, TAAs, enemy threat ring, and cargo movement requirements as Scenario #1, but the road network contains five additional roads (117 total). The slightly denser network adds complexity to the MRVP with over four times as many paths between POD-TAA pairs (Table VI), but the problem is still solvable by the BIP in a reasonable amount of time.

Table V.
Scenario #1 – BIP results

Road name	Within threat ring?
I20 + 4,553-9,587	Yes
I640 ± 5,840	Yes
road-53,369	Yes

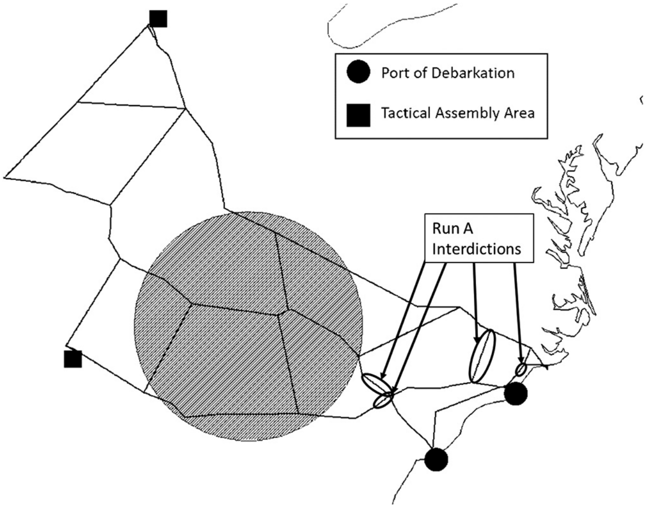

Figure 3.
Scenario #1 – Run A interdiction locations

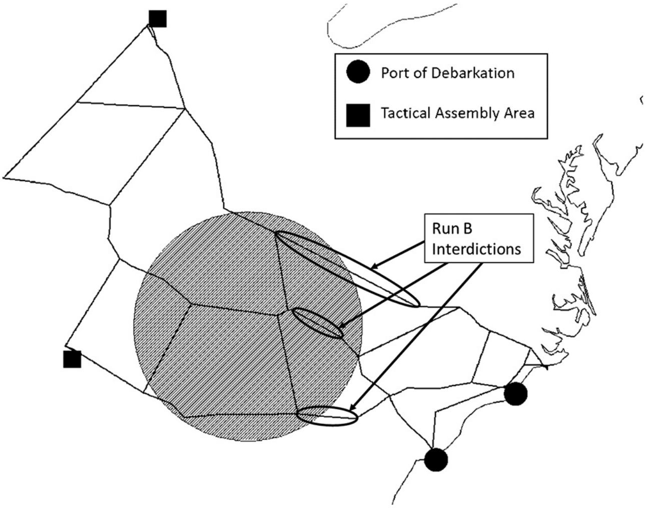

Figure 4.
Scenario #1 – Run B interdiction locations

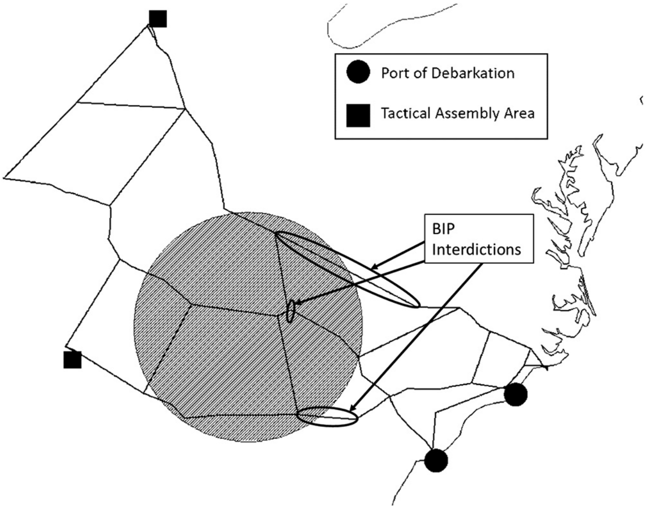

Figure 5.
Scenario #1 – BIP interdiction locations

Requirement	POD	TAA	No. of paths
1	Charleston	FT Sheridan	24,502
2	Wilmington	FT Sheridan	26,014
3	Charleston	Memphis	11,692
4	Wilmington	Memphis	12,916

Table VI.
Number of paths per requirement in scenario #2

Scenario #2 results

The road interdictions selected by the algorithm (Figure 6) and BIP (Figure 7) are similar. Each requires four interdictions to halt all cargo and each interdiction is within the threat ring. In fact, the only difference between the algorithm and BIP interdictions are arbitrary selections on the same stretch of road.

Scenario #3 description

The networks in Scenarios #1 and #2 are small and simplistic compared to the typical size and complexity of MRVPs encountered at the United States Transportation Command.

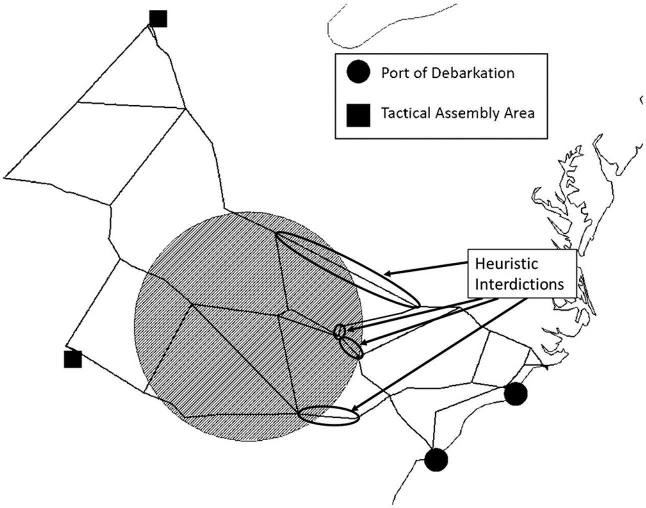

Figure 6.
Scenario #2 – Heuristic interdiction locations

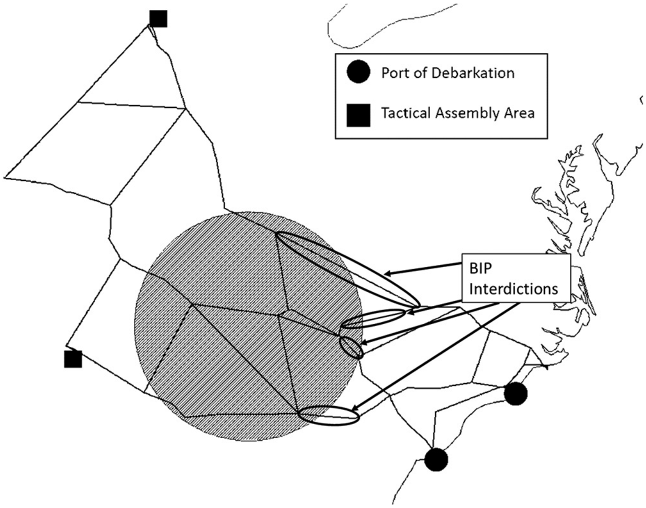

Figure 7.
Scenario #2 – BIP interdiction locations

Thus, Scenario #3 is offered to test the algorithm's efficiency at identifying critical edges for a larger theater network. As a result, the number of unique POD to TAA requirements and the topological complexity of the network in Scenario #3 is vastly increased from Scenarios #1 and #2.

Scenario #3 involves moving military cargo from US airports and seaports to destinations using militarily-useful roads. The associated road network consists of 8,059 links and 7,257 nodes, as represented in Figure 8. The computational expense of enumerating all possible paths for each unique requirement is exceedingly high in this scenario. Therefore, the BIP used to solve Scenarios #1 and #2 cannot be used to efficiently solve Scenario #3. The MRVP heuristic algorithm, however, can be used to identify critical roads in the network vulnerable to enemy interdiction without computational difficulty.

Scenario #3 contains 43 distinct POD to TAA requirements using 16 distinct PODs and 20 distinct TAAs, as shown in Table VII.

The specific alternative seaports and airports available to the MRVP heuristic algorithm are listed in Tables VIII and IX, respectively. As in Scenario #1, only those ports listed in the requirements are activated as alternatives for Scenario #3. However, alternative seaports may only be substituted for the requirements originating at a seaport and alternative airports may only be substituted for requirements originating at an airport.

The final requirement of the algorithm is the enemy threat assessment based on credible intelligence estimates, which will be used to specify areas of the network with higher likelihood of attack. This scenario assumes notional intelligence about an enemy threat ring of radius 267 nautical miles in Southeast USA. The circular ring is centered over a subset of states in the southeast, as shown in Figure 9.

Scenario #3 results

The algorithm identified 85 critical roads out of 8,059 total roads in the network, or about 1 per cent of all roads. Interdiction of these 85 critical roads would result in the entire theater distribution requirement being undeliverable, which suggests the enemy could cause serious

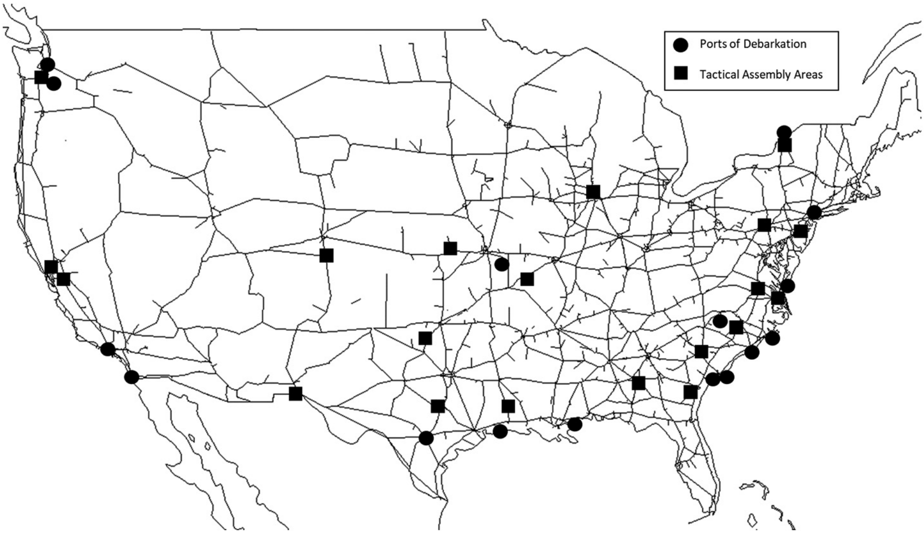

Figure 8.
Scenario #3 network of militarily-useful US roads

Table VII. Scenario #3 POD to TAA requirements

Requirement	POD	TAA	Cargo tonnage
1	Bayonne	FT Drum	180,972.9
2	Wheeler Sack AAF	FT Drum	108,654.6
3	Morehead City	FT Benning	22,236
4	Wilmington	FT Benning	15,125.5
5	Wilmington	FT Bliss	15,125.5
6	Beaumont	FT Bragg	73,173.5
7	Charleston	FT Bragg	4,942.9
8	Gulfport	FT Bragg	1,534.9
9	Long Beach	FT Bragg	282
10	Morehead City	FT Bragg	34,332.5
11	NORFOLK	FT Bragg	3,514.3
12	Pope AFB	FT Bragg	2,123.2
13	San Diego	FT Bragg	714.6
14	Tacoma	FT Bragg	1,592.7
15	Wilmington	FT Bragg	1,081.9
16	Beaumont	FT Carson	73,565
17	Wilmington	FT Carson	14,983.8
18	Morehead City	FT Dix	22,236
19	Wilmington	FT Dix	15,125.5
20	Morehead City	FT Eustis	967.6
21	Beaumont	FT Hood	66,333.1
22	Charleston	FT Hood	88,984.1
23	Gulfport	FT Hood	6,415.9
24	Morehead City	FT Hood	68,015.9
25	Norfolk	FT Hood	62,783.5
26	Morehead City	FT Jackson	22,236
27	Wilmington	FT Lee	15,125.5
28	Charleston	FT Leonard Wood	3,006.5
29	Whiteman AFB	FT Leonard Wood	17.7
30	Mcchord AFB	FT Lewis	18.3
31	Charleston	FT Polk	2,487.2
32	Wilmington	FT Polk	22,236
33	Morehead City	FT Riley	22,236
34	Wilmington	FT Sheridan	15,125.5
35	Beaumont	FT Sill	76,555.9
36	Charleston	FT Sill	5,048.3
37	Morehead City	FT Sill	355.8
38	San Diego	FT Sill	53
39	Charleston	FT Stewart	172,697.9
40	Norfolk	FT Stewart	345.8
41	Charleston AFB	Mechanicsburg	248
42	Lackland-Kelly	Tracy	367.2
43	Beaumont	Travis AFB	913.4

disruption to the network by interdicting relatively few roads. Furthermore, 35 of the critical roads identified were within the enemy threat ring, which suggests the enemy would need to attack roads outside the threat range to halt all cargo. This insight is relatively straightforward from a visual examination of the possible road routes outside the threat ring between PODs and TAAs, as reflected in Figure 9. Regardless, such insights into the vulnerability, or conversely the resiliency, of the military theater distribution network are useful to military logistics planners.

Figures 10 and 11 report the output measures *cargo halted* and *cargo rerouted*, respectively, on the vertical axis for each successive interdiction (i.e. algorithm iteration) on the horizontal axis. The successive interdiction of roads reveals an interesting breaking point at the 50th interdiction, which results in over 90 per cent of the requirements being

Seaport name	State
Bayonne	New jersey
Beaumont	Texas
Charleston	South carolina
Gulfport	Mississippi
Long beach	California
Morehead city	North carolina
Norfolk	Virginia
San diego	California
Tacoma	Washington
Wilmington	North carolina

Table VIII.
Scenario #3 available alternative seaports

Airport Name	State
Charleston AFB	South carolina
Lackland-Kelly	Texas
Mcchord AFB	Washington
Pope AFB	North carolina
Wheeler Sack AAF	New york
Whiteman AFB	Missouri

Table IX.
Scenario #3 available alternative airports

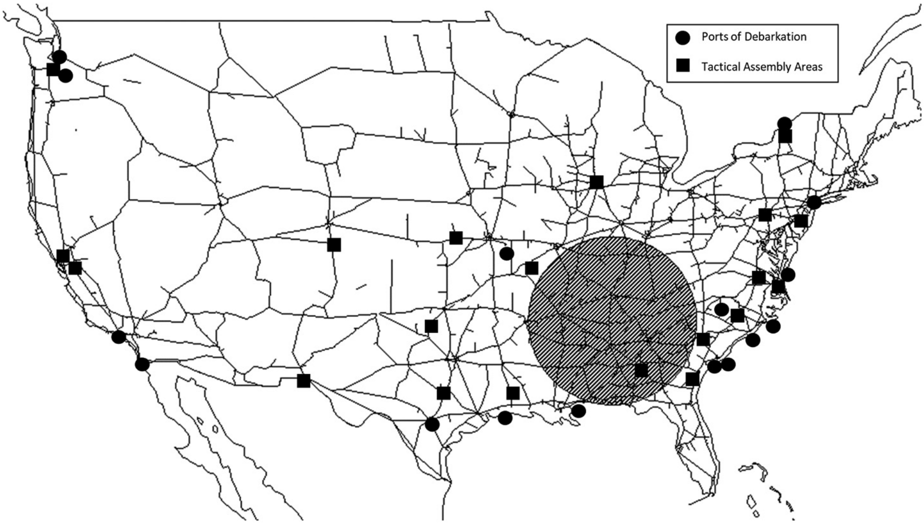

Figure 9.
Scenario #3 threat ring indicated by the shaded circle

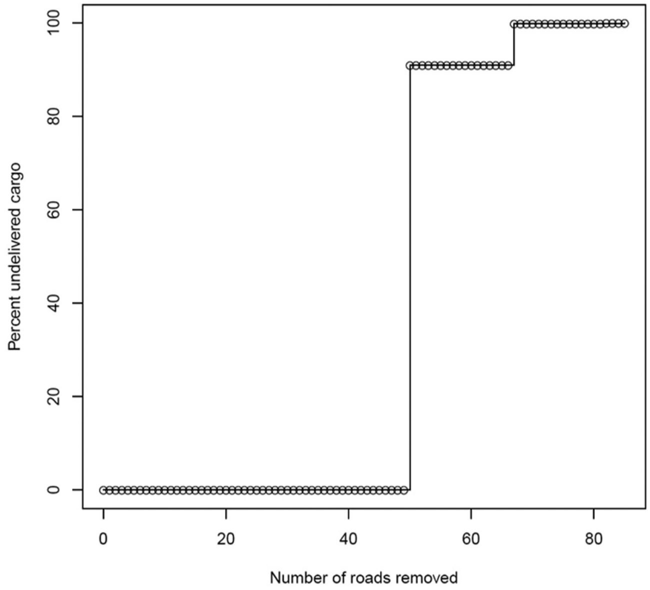

Figure 10.
Scenario #3 per cent of cargo halted after successive road interdictions

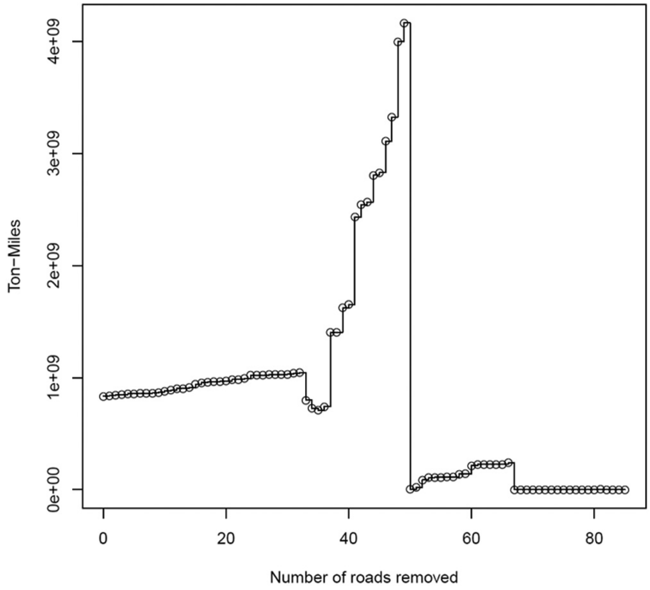

Figure 11.
Scenario #3 cargo rerouted after successive road interdictions

undeliverable, as shown in Figure 10 with the steep increase in halted cargo after 50 roads were removed. Therefore, the protection of these 50 roads is necessary to ensure successful delivery of cargo to TAAs, although cargo rerouting is still required. Similarly, there is a sharp decrease in cargo ton-miles in Figure 11 after the 50th road interdiction, which is expected given the corresponding increase in halted cargo after these 50 successive interdictions. The user-defined multiplier (U) selected for this run was 10; therefore, $T_e = 10$ for each edge within the threat ring.

Software and hardware specifications

The MRVP heuristic algorithm has been implemented in the RStudio v1.0.453 software (Team, 2017) using R v3.5.1 and seven primary R packages: igraph (Csardi and Nepusz, 2006), data.table (Dowle and Srinivasan, 2017), maps (Becker *et al.*, 2016b), mapdata (Becker *et al.*, 2016a), geosphere (Hijmans, 2016), ggplot2 (Wickham, 2009) and dplyr (Wickham and Francois, 2016). The BIP has been implemented in the General Algebraic Modeling System (GAMS) v24.3.3 software. The solutions for both the MRVP heuristic and BIP have been generated on a common computing environment, specifically a 64-bit Windows 7 computer with an Intel Xeon CPU at 3.33 GHz and 48 GB of RAM. The computational times for the runs conducted are listed in Table X.

Discussion

Previous research by Murray *et al.* (2007), Matisziw and Murray (2009) and Shen *et al.* (2013) on network vulnerability problems suggest the need to consider both topology and flow when identifying network vulnerabilities. As such, network topology and flow were included as central tenets of the MRVP solution methods described in this paper. Unfortunately, previous network vulnerability research of general transportation (Reggiani, 2013; Mattsson and Jenelius, 2015) and military logistics (Gao *et al.*, 2012; Zhao *et al.*, 2018) did not specifically address enemy threat capabilities and intent to disrupt network flows, which is an important factor in most MRVPs. Therefore, the MRVP solution approaches presented in this paper integrate enemy threats into the critical edge detection problem, thereby filling a perceived research gap in the current literature with respect to military applications of network vulnerability problems.

The MRVP solution approach of developing a heuristic algorithm accompanied by an IP to test its accuracy follows the general approach of other network vulnerability researchers (Myung and Kim, 2004; Arulselvan *et al.*, 2009). Indeed, the MRVP heuristic algorithm and associated BIP produced similar results on two small-scale scenarios. In each notional scenario tested, the MRVP heuristic algorithm identified a relatively small subset of network edges (i.e. under about 5 per cent) as being critical to the flow of military cargo from PODs to TAAs. The route vulnerability results could be used to alert military logistics planners and decision-makers about potential vulnerabilities to specific roads and railways given credible enemy threat capabilities and intent. More importantly, the MRVP heuristic algorithm

Scenario	Type	Computational time (seconds)
#1 – Run A	Heuristic	2.5
#1 – Run B	Heuristic	2.3
#1 – BIP	BIP	18.0
#2	Heuristic	3.0
#2	BIP	932.4
#3	Heuristic	130.5
#3	BIP	*

Note: Scenario #3 was too computationally expensive to enumerate all acyclic paths required for the BIP

Table X. Computational time comparisons

performs efficiently on larger problems indicative of the size and complexity of MRVPs encountered at the United States Transportation Command.

Conclusion

Networks are ubiquitous and span diverse domains including transportation, telecommunications and social systems. As such, much research has been done to better understand network vulnerability against various forms of disruption. Common research themes suggest network vulnerability depends on the topology of nodes connected by edges and the flow among specific nodes. Two well-studied aspects of network vulnerability include the critical node detection problem and critical edge detection (or disruption) problem. Solution approaches to these important problems have included optimal IPs and non-optimal heuristics, with large instances of the problems typically solved using heuristics.

The research presented in this paper introduces a similar network problem, informally termed the MRVP, which is to identify military theater distribution roads and railways most vulnerable to enemy interdiction. The MRVP heuristic algorithm and associated BIP introduced in this paper adds to the extensive research into network vulnerability. Specifically, the MRVP identifies critical, or vulnerable, elements of the physical road and rail network considering an enemy's ability and intent to interdict routes. The enemy's goal of route interdictions is to either force cargo to be rerouted over longer distances or halted altogether if no feasible route exists.

The results presented for two notional small-scale scenarios suggest the MRVP heuristic produces accurate results compared to the optimal results from the associated BIP. More importantly, the heuristic quickly generated meaningful route vulnerability results for a notional scenario similar to the size and complexity of problems encountered by United States Transportation Command analysts.

Most networks are dynamic (Kolaczyk and Csárdi, 2014) and military transportation networks are no exception. The heuristic presented herein could be applied iteratively to small segments (e.g. weekly) of the deployment timeline, which often spans multiple months. As such, each iteration could incorporate any known changes to the transportation network, including recent interdictions of roads or railways, updated enemy threat conditions, or updated requirements not reflected in the original TPFDD. These iterative route vulnerability insights would be useful to commanders dealing with dynamic changes to the network and wartime conditions.

A limitation of the MRVP solution approaches presented in this paper is that the dynamic network changes, especially related to time, are not explicitly reflected in the problem. Few enemies would have unlimited means to interdict transportation routes, so it is likely they would synchronize route interdictions with periods of high cargo flow to cause the most network disruption. Future work on the MRVP could incorporate various network dynamics, including the fluctuation of cargo requirements over time and the timing of enemy interdictions.

References

Arulselvan, A., Commander, C.W., Elefteriadou, L. and Pardalos, P.M. (2009), "Detecting critical nodes in sparse graphs", *Computers and Operations Research*, Vol. 36 No. 7, pp. 2193-2200.

Becker, R.A. Wilks, A.R. and Brownrigg, R. (2016a), "Mapdata: extra map databases", R package version 2.2-6.

Becker, R.A. Wilks, A.R. Brownrigg, R. Minka, T.P. and Deckmyn, A. (2016b), "Maps: draw geographical maps", R package version 3.1.1.

Berdica, K. (2002), "An introduction to road vulnerability: what has been done, is done and should be done", *Transport Policy*, Vol. 9 No. 2, pp. 117-127.

Csardi, G. and Nepusz, T. (2006), "The igraph software package for complex network research", *InterJournal, Complex Systems*, Vol. 1695 No. 5, pp. 1-9.

Demšar, U., Špatenková, O. and Virrantaus, K. (2008), "Identifying critical locations in a spatial network with graph theory", *Transactions in GIS*, Vol. 12 No. 1, pp. 61-82.

Di Summa, M., Grosso, A. and Locatelli, M. (2011), "Complexity of the critical node problem over trees", *Computers and Operations Research*, Vol. 38 No. 12, pp. 1766-1774.

Dinh, T.N., Xuan, Y., Thai, M.T., Pardalos, P.M. and Znati, T. (2012), "On new approaches of assessing network vulnerability: hardness and approximation", *IEEE/ACM Transactions on Networking*, Vol. 20 No. 2, pp. 609-619.

Dowle, M. and Srinivasan, A. (2017), "Data.table: extension of 'data.frame", R package version 1.10.4.

Gao, J., Liu, X.L. and Rong, L.Q. (2012), "Study on travel time reliability of military transportation network", *2012 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE)*, *IEEE*, pp. 232-235.

Hijmans, R.J. (2016), "Geosphere: spherical trigonometry", R package version 1.5-5.

Khademi, N., Balaei, B., Shahri, M., Mirzaei, M., Sarrafi, B., Zahabiun, M. and Mohaymany, A.S. (2015), "Transportation network vulnerability analysis for the case of a catastrophic earthquake", *International Journal of Disaster Risk Reduction*, Vol. 12, pp. 234-254.

Kolaczyk, E.D. and Csárdi, G. (2014), *Statistical Analysis of Network Data with R*, Springer, New York, NY.

Lalou, M., Tahraoui, M.A. and Kheddouci, H. (2018), "The critical node detection problem in networks: a survey", *Computer Science Review*, Vol. 28, pp. 92-117.

Matisziw, T.C. and Murray, A.T. (2009), "Modeling s-t path availability to support disaster vulnerability assessment of network infrastructure", *Computers and Operations Research*, Vol. 36 No. 1, pp. 16-26.

Matisziw, T.C., Murray, A.T. and Grubesic, T.H. (2009), "Exploring the vulnerability of network infrastructure to disruption", *The Annals of Regional Science*, Vol. 43 No. 2, pp. 307-321.

Mattsson, L.G. and Jenelius, E. (2015), "Vulnerability and resilience of transport systems-a discussion of recent research", *Transportation Research Part A: Policy and Practice*, Vol. 81, pp. 16-34.

Murray, A.T., Matisziw, T.C. and Grubesic, T.H. (2007), "Critical network infrastructure analysis: interdiction and system flow", *Journal of Geographical Systems*, Vol. 9 No. 2, pp. 103-117.

Myung, Y.S. and Kim, H.J. (2004), "A cutting plane algorithm for computing k-edge survivability of a network", *European Journal of Operational Research*, Vol. 156 No. 3, pp. 579-589.

Pavlikov, K. (2018), "Improved formulations for minimum connectivity network interdiction problems", *Computers and Operations Research*, Vol. 97, pp. 48-57.

Purevsuren, D., Cui, G., Win, N.N.H. and Wang, X. (2016), "Heuristic algorithm for identifying critical nodes in graphs", *Advances in Computer Science: An International Journal*, Vol. 5 No. 3, pp. 1-4.

Reggiani, A. (2013), "Network resilience for transport security: some methodological considerations", *Transport Policy*, Vol. 28, pp. 63-68.

Reggiani, A., Nijkamp, P. and Lanzi, D. (2015), "Transport resilience and vulnerability: the role of connectivity", *Transportation Research Part A: Policy and Practice*, Vol. 81, pp. 4-15.

Rupi, F., Bernardi, S., Rossi, G. and Danesi, A. (2015), "The evaluation of road network vulnerability in mountainous areas: a case study", *Networks and Spatial Economics*, Vol. 15 No. 2, pp. 397-411.

Sachs, H., Stiebitz, M. and Wilson, R.J. (1988), "An historical note: Euler's Königsberg letters", *Journal of Graph Theory*, Vol. 12 No. 1, pp. 133-139.

Shen, S., Smith, J.C. and Goli, R. (2012), "Exact interdiction models and algorithms for disconnecting networks via node deletions", *Discrete Optimization*, Vol. 9 No. 3, pp. 172-188.

Shen, Y., Nguyen, N.P., Xuan, Y. and Thai, M.T. (2013), "On the discovery of critical links and nodes for assessing network vulnerability", *IEEE/ACM Transactions on Networking*, Vol. 21 No. 3, pp. 963-973.

Team, R.C. (2017), "R: a language and environment for statistical computing", R Foundation for Statistical Computing, Vienna, available at: www.R-project.org/

US Department of Transportation (2018), "Bureau of transportation statistics", US ton-miles of freight, available at: www.bts.gov/content/us-ton-miles-freight

US Joint Chiefs of Staff (2013), "Joint publication 3-35", Deployment and Redeployment Operations, 1.

US Joint Chiefs of Staff (2016), "Joint publication 3-03", Joint Interdiction, 9.

US Joint Chiefs of Staff (2017), "Joint publication 4-01", The Defense Transportation System, 7.

Ventresca, M. and Aleman, D. (2015), "Efficiently identifying critical nodes in large complex networks", *Computational Social Networks*, Vol. 2 No. 1, p. 6.

Veremyev, A., Prokopyev, O.A. and Pasiliao, E.L. (2014), "An integer programming framework for critical elements detection in graphs", *Journal of Combinatorial Optimization*, Vol. 28 No. 1, pp. 233-273.

Wickham, H. (2009), *ggplot2: elegant Graphics for Data Analysis*, Springer-Verlag, New York, NY.

Wickham, H. and Francois, R. (2016), "Dplyr: a grammar of data manipulation", R package version 0.5.0.

Yu, F., Xia, X., Li, W., Tao, J., Ma, L. and Cai, Z.Q. (2017), "Critical node identification for complex network based on a novel minimum connected dominating set", *Soft Computing*, Vol. 21 No. 19, pp. 5621-5629.

Zhao, T., Huang, J., Shi, J. and Chen, C. (2018), "Route planning for military ground vehicles in road networks under uncertain battlefield environment", *Journal of Advanced Transportation*, Vol. 64 No. 1.

Corresponding author
Joshua R. Muckensturm can be contacted at: joshua.r.muckensturm.civ@mail.mil