J Geograph Syst (2007) 9:103–117
DOI 10.1007/s10109-006-0039-4

ORIGINAL ARTICLE

Critical network infrastructure analysis: interdiction and system flow

Alan T. Murray · Timothy C. Matisziw · Tony H. Grubesic

Received: 8 November 2006 / Accepted: 4 December 2006 / Published online: 12 January 2007

Abstract Effective management of critical network infrastructure requires the assessment of potential interdiction scenarios. Optimization approaches have been essential for identifying and evaluating such scenarios in networked systems. Although a primary function of any network is the distribution of flow between origins and destinations, the complexity and difficulty of mathematically abstracting interdiction impacts on connectivity or flow has been a challenge for researchers. This paper presents an optimization approach for identifying interdiction bounds with respect to connectivity and/or flow associated with a system of origins and destinations. Application results for telecommunications flow are presented, illustrating the capabilities of this approach.

A. T. Murray (✉)
Center for Urban and Regional Analysis, and Department of Geography,
The Ohio State University, Columbus, OH 43210, USA
e-mail: murray.308@osu.edu

T. C. Matisziw
Center for Urban and Regional Analysis, The Ohio State University,
Columbus, OH 43210, USA
e-mail: matisziw.1@osu.edu

T. H. Grubesic
Department of Geography, Indiana University,
Bloomington, IN 47403, USA
e-mail: tgrubesi@indiana.edu

1 Introduction

As a response to the growing threat of terrorism in the late 1990s, the U.S. federal government established the President's Commission on Critical Infrastructure Protection (PCCIP) (E.O. 13010). In this executive order (E.O.) (1995), ''infrastructure'' was defined as:

> The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole (E.O. 13010).

More importantly, E.O. 13010 (1996) suggested that ''... certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.'' The concept of ''vital'' or ''critical'' infrastructure is clearly an important one for establishing national security benchmarks. Basic inventories of critical infrastructure are often subdivided into sectors, and include (E.O. 13010, 1996; White House 2003): telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

Given the vast array of infrastructure in these sectors, it is not surprising that fiscal constraints can limit the scope of protective measures applied to the nation's critical infrastructure.[1] Moreover, the heightened concerns for security threats and the need to safeguard these sectors suggest that optimization-based approaches for identifying risk in networks of all sorts, ranging from gas and oil pipelines to transportation routes to telecommunication systems, are extremely important for prioritizing and evaluating fortification strategies to maintain the continuity of their functions (see White House 2003).

A common theme in the analysis and evaluation of network-based critical infrastructure is *interdiction*, where network elements (nodes or arcs) are disabled, intentionally or otherwise, disrupting the flow of valuable goods or services through the network. There has been much interest in examining vulnerabilities and risk in critical network infrastructure (Carlier et al. 1997; Soni and Pirkul 2000; Palmer et al. 2001; Carreras et al. 2002; Crucitti et al. 2004; Latora and Marchiori 2005; Chassin and Posse 2005; Grubesic and Murray 2006) and interdiction has been implicit, if not explicit, in most cases.

[1] In the fiscal year 2006, $873 million USD were allocated to the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate (DHS 2004, 2005), which coordinates the Federal Government's efforts to protect the Nation's critical infrastructure, including commercial assets (e.g., stock exchanges), government facilities, dams, nuclear power plants, national monuments and icons, chemical plants, bridges, and tunnels. In addition, $94 million USD is allocated to protecting against threats to information technology infrastructure (OMB 2006).

Baran (1964) recognized that some network topologies provide a higher probability of survivability (or connectivity, more specifically) after an attack. In particular, distributed networks with higher levels of redundancy and diversity are good for ensuring connectivity, should interdiction take place. The topological properties of networks are further explored in examining ''scale-free'' networks (Albert et al. 2000; 2004; Barabasi et al. 2000, 2001). Results suggest that although scale-free networks like the Internet are very tolerant of random failures, a series of targeted attacks on the most highly connected nodes or ''hubs'' can be crippling. Nevertheless, performance of a network, viewed in terms of either vulnerability or survivability, ultimately centers on connectivity and whether flow can move between origins and destinations (see Bell 2000; Doyle et al. 2005). If interdiction to network-based critical infrastructure is to be guarded against or managed once it occurs, methods are needed for identifying and examining possible interdiction scenarios, a sentiment shared by Houck et al. (2004) and Salmeron et al. (2004).

The above discussion has highlighted that networks serve to deliver flow through a system of interconnected nodes and arcs and that planning for interdiction of this service is essential. With this in mind, this paper develops an integer programming model to evaluate the upper and lower bounds on flow disruption as a result of facility interdiction in a network. The next section provides a background review of previous modeling work in this area. An integer model formulation is then presented and discussed. An application analyzing potential interdiction of network components for the Abilene Internet2 backbone is given, highlighting the utility of the developed modeling approach. Finally, discussion and conclusions are provided.

2 Background

Optimization techniques have played a significant role in examining potential interdiction impacts, recognizing the insights they can provide for mitigating facility loss and prioritizing fortification efforts. Four categories of approaches are reviewed here: simulation, min-cut/shortest paths, network attributes, and system flow. Common to all categories is that nodes and/or arcs in the network may be interdicted. The differences in the categorical distinctions are the ways in which the network or its performance is evaluated.

Simulation has been an important optimization technique in general terms, and has proven valuable in the analysis of interdiction in critical network infrastructure. One benefit of simulation is that it typically allows for the examination of a range of impacts, with either implicit or explicit notions of optimized performance for a network. For example, Grubesic et al. (2003) examined basic graph theoretic measures of network connectivity, such as the degree of node and nodal centrality, for Internet backbone networks. As network elements were interdicted (or ''removed''), the corresponding changes in network connectivity were documented. Latora and Marchiori (2005) also simulated the removal of nodes in a networked system, assessing

performance and the criticality of each node individually. Crucitti et al. (2004) examined individual nodal capacities for a network and their ability to handle additional/excess information when other network elements (nodes) are lost. Similarly, Albert et al. (2004) apply this logic to simulations of node-based attacks on the North American power grid. In their simulations, consideration for secondary failures spawned by the initial attack is also addressed. These ''cascading'' failures are represented using a rank, remove, and recomputation method, similar to Holme et al. (2002). In this aforementioned work, assessment of origin–destination (O–D) flows is not addressed. Recently, however, Doyle et al. (2005) argue that O–D interaction is in fact an important component of engineered systems and explore a standard metric for network performance that examines end-user traffic demands between all pairs of end vertices (nodes) in a system. While the loss or removal of critical arcs/nodes in these systems can be instructive for identifying the varying levels of connectivity for networks, evaluating individual links independent of the presence or absence of all other network elements (arcs and nodes) can be myopic or misleading.

Another category for network evaluation involves assessing impacts relative to altering the maximum flow or shortest path for a given O–D pair. For example, one strategy for network interdiction is to maximize network disruption by removing the links with the greatest total value in a system (e.g. Wollmer 1964; Ratliff et al. 1975; Ball et al. 1989; Wood 1993). Similarly, one can also seek to maximize network disruption by removing the nodes most critical to system operation (Corley and Chang 1974; Corley and Sha 1982; Nardellia et al. 2003). The notion of flow (and its disruption) is implicit in many of these optimization-based approaches given the focus on altering the maximum O–D flow. However, recent research highlights the importance of explicitly modeling O–D flows (Myung and Kim 2004).

A third category of optimization modeling work characterizes impacts in terms of system performance or network characteristics. For example, Church et al. (2004) consider average service costs and coverage reduction in this context using median and covering location models, respectively. Grubesic and Murray (2006) examine nodal interdiction outcomes quantified as the total attributes (e.g., capacity) of arcs impacted. Extending this, Grubesic et al. (2006) model node and arc attributes, simultaneously, in the context of interdiction for a telecommunication backbone. Yet, while these models can approximate impact to network connectivity, they do not account for O–D flows in the network.

The final category is system flow. A more recent interest in interdiction studies is examining connectivity and O–D flow in networked systems. While maximum flow approaches seek to identify interdiction schemes that reduce the capacity of a particular O–D pair to interact, system flow approaches focus on the interaction between all O–D pairs. To address system flow Myung and Kim (2004) present an integer program to identify those arcs whose removal results in an upper bound on network failure and discuss an algorithm for finding a lower bound. Their formulation relies on identifying feasible paths

for each O–D pair and tracking the availability of facilities involved in each path. A preprocessing technique is employed to focus only on O–D pairs that can be interdicted given the removal of a specified number of arcs. Ultimately, however, both the upper and lower bounds are heuristically derived.

Of interest in this paper is this fourth category, focusing on the explicit representation of O–D flow in a network. To this end, an optimization model is presented to identify optimal upper and lower bounds for potential network interdiction scenarios, with the intent to support management and planning efforts oriented toward assessing vulnerability and reliability in networked systems.

3 Modeling flow interdiction

From a planning and management perspective, an optimization model is necessary for identifying an interdiction scenario that maximizes or minimizes total flow disrupted. In this context, a network component is interdicted, rendering it inoperable, as commonly assumed in the literature. For modeling and discussion purposes, interdiction is limited to nodes in the network, though the work that follows can readily be extended to account for arc interdiction as well. Without loss of generality, the number of facilities interdicted is specified in advance. Given any general network $G = (N,A)$, where N denotes the set of nodes and A the set of component arcs or linkages, it is assumed that all feasible, non-redundant paths in the network can be identified for any interacting pair of nodes. This assumption is not unlike that made to model flow capture (see Hodgson et al. 1996), network design (see Kalvenes et al. 2004), or arc interdiction (see Myung and Kim 2004). The following notation is used to formulate a model for the evaluation of flow interdiction:

k index of paths, entire set denoted K
j index of facilities, entire set denoted J
o index of origins, entire set denoted Ω
d index of destinations, entire set denoted Λ
N_{od} set of paths enabling OD flow
f_{od} flow observed between OD
p number of facilities to remove
ϕ_{k} set of facilities along path k

$$X_j \begin{cases} 1 \text{ if facility } j \text{ is interdicted} \\ 0 \text{ otherwise} \end{cases}$$

$$Y_k \begin{cases} 1 \text{ if path } k \text{ remains uneffected by interdiction} \\ 0 \text{ otherwise} \end{cases}$$

$$Z_{od} \begin{cases} 1 \text{ if no flow possible between } OD \\ 0 \text{ otherwise} \end{cases}$$

3.1 Flow interdiction model

Maximize or Minimize

$$\sum_{o}\sum_{d} f_{od} Z_{od} \tag{1}$$

Subject to:

$$\sum_{k \in N_{od}} Y_k + Z_{od} \geq 1 \qquad \forall o, d \tag{2}$$

$$Z_{od} \leq (1 - Y_k) \qquad \forall o, d, k \in N_{od}, k \tag{3}$$

$$Y_k \geq 1 - \sum_{j \in \Phi_k} X_j \qquad \forall k \tag{4}$$

$$Y_k \leq (1 - X_j) \qquad \forall k, j \in \Phi_k \tag{5}$$

$$\sum_{j} X_j = p \tag{6}$$

$$\begin{aligned} X_j &= \{0,1\}\ \forall j \\ Y_k &= \{0,1\}\ \forall k \\ Z_{od} &= \{0,1\}\ \forall o, d \end{aligned} \tag{7}$$

Objective (1) maximizes or minimizes total flow interdicted. Constraints (2) and (3) account for the existence of paths between a given O–D. Constraints (4) and (5) track whether a path is impacted by an interdiction scenario. Constraints (6) specify that p nodes are to be interdicted. Finally, Constraints (7) impose binary integer restrictions on decision variables.

The FIM is a unified model, structured to identify interdiction schemes that maximize or minimize total flow disruption in the network. It does this by accounting for nodes interdicted, and the subsequent elimination of particular paths between O–D pairs utilizing these nodes. For example, consider three nodes, o, j, and d, with a link connecting o and j and a link connecting j and d, and assume there is flow between od only. If node j is interdicted, then it is inoperable and $X_j = 1$. Assume, without loss of generality, that path k is the only path for od, node j is on path k, and j is the only interdicted node. Given this, Constraint (4) is $Y_k \geq 1–1$, or simply $Y_k \geq 0$. With the objective of maximizing flow disruption, Z_{od} will seek to equal 1 if at all possible. This means that Y_k will equal zero, e.g., $Y_k = 0$, as Constraints (2) and (3) allow $Z_{od} = 1$ only if no path exists for this O–D pair, which it does not in this case because $\sum_{k' \in N_{od}} Y_{k'} = Y_k = 0$ in Constraint (2) and $Y_k = 0$ in Constraint (3). When minimizing flow disruption, (1) will seek out $Z_{od} = 0$, which can only be attained when $Y_k = 1$ as there is only one path. In this case, Constraints (5) are in place to ensure that if any node on path Y_k is interdicted, Y_k is unavailable. Thus, the decision variables and constraints work as intended to account for flow disruption, which is why this is conceived of as a unified approach. While

it would be possible to separate this one model into two models for addressing the respective maximum or minimum case, one approach is capable of addressing both concerns as the two cases are of interest in management and planning contexts.

4 Application

The developed model was applied to the Abilene Internet2 network backbone shown in Fig. 1 to assess interdiction risk. The Abilene backbone is a high performance fiber-optic telecommunication network, consisting of 14 linkages that integrate 11 routers (network nodes), primarily intended to facilitate transmissions between research institutions in the U.S. (Abilene 2005). Flow data (in bytes) observed at network routers was collected by Abilene using Cisco NetFlow (Abilene 2005). Each router serves as both an origin and destination node, resulting in 121 O–D pairs including intra-nodal flow. Given infrastructure capacities, all network elements were considered uncapacitated.

The analysis was carried out on a personal computer with a Xeon 3.0 GHz processor and 4 GB RAM. TransCAD, a commercial geographical information system (GIS) package, was used to manage the Abilene data and extract arc and node incidence relationships. A C++ program was written to enumerate all simple O–D paths using arc/node data exported from TransCAD. For the Abilene network, 907 paths were identified (896 inter-nodal + 11 intra-nodal). However, removing path redundancies reduced the number of necessary paths to 151 (an 83.4% reduction). Path identification required less than one second of computing time. The associated FIM problem instance was

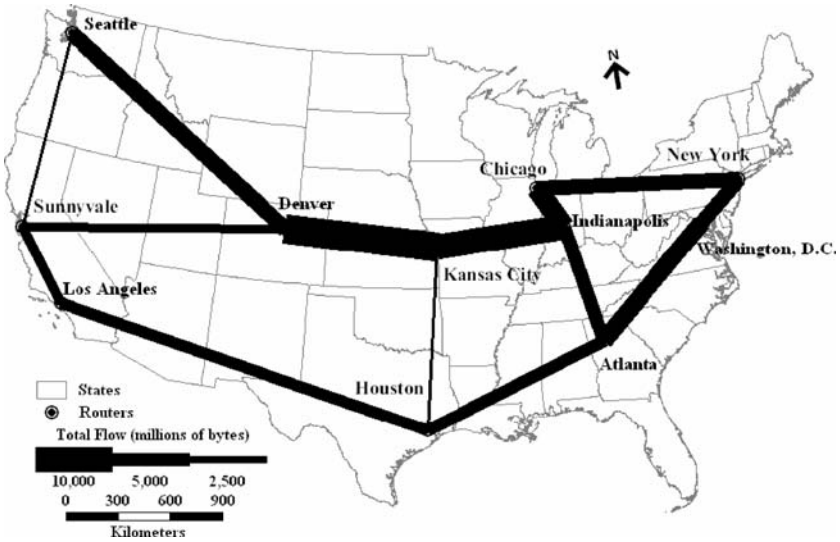

Fig. 1 Flow activity on Abilene Internet2 backbone

then structured, consisting of 228 decision variables and 1,065 constraints. The C++ program then calls ILOG CPLEX 10.01, a commercial optimization package, to solve all instances of the FIM reported in this paper.

The FIM was used to identify potential worst-case and best-case nodal interdiction scenarios. Consistent with much of previous research, we initially evaluate network connectivity using FIM. This is done assuming only a single unit of flow between interacting O–D pairs (e.g., removing f_{od} from the objective) so that all O–D relationships are valued equivalently in the model. Following this, actual observed total flow between interacting O–D pairs is examined using the FIM. Both connectivity and actual flow instances are solved for the entire range of node interdiction possibilities, p = 1–11, the results of which are discussed below.

Connectivity results are provided in Table 1, giving solution details for each level of potential interdiction. Fig. 2 plots the objective function as the number of nodes interdicted increases. The problems required little computational effort, with the greatest effort being for $p = 1$. When one node is interdicted, Indianapolis is identified as the location that, if rendered inoperable, would disrupt the greatest number of O–D pairs (21), some 17% of the 121 interacting pairs. If two nodes are interdicted, we find that Kansas City and Houston would cause a disruption of 80 O–D pairs, or approximately 66% of all interacting pairs. Certainly both cases represent a significant potential impact on the network, but even one additional interdicted node ($p = 3$) would bring the total impact to over 80% of interacting O–D pairs.

Altering the focus slightly, flow interdiction results are provided in Table 2, giving solution details for each scenario level. As was found in Table 1, the problems solved in Table 2 required little computational effort. In contrast to the interdiction of connectivity, we find that explicitly accounting for flow

Table 1 FIM solutions for maximum connectivity interdiction (unit flow on each O–D pair)

p	Objective (O–D pairs)	Cities interdicted	Iterations	Branches	Time (s)
1	21	IND	192	0	0.109
2	80	KC, HOU	67	0	0.016
3	97	KC, ATL, SNV	63	0	0.016
4	108	CHI, KC, ATL, SNV	30	0	0.016
5	113	IND, DEN, HOU, SNV, NY	30	0	0.016
6	116	CHI, IND, DEN, HOU, SNV, WAS	13	0	0.000
7	117	CHI, IND, KC, DEN, HOU, SNV, WAS	10	0	0.016
8	118	SEA, CHI, IND, DC, DEN, ATL, LA, WAS	7	0	0.015
9	119	SEA, CHI, IND, KC, DEN, ATL, HOU, LA, WAS	8	0	0.016
10	120	SEA, CHI, IND, KC, DEN, ATL, HOU, LA, SNV, NY	0	0	0.000
11	121	SEA, CHI, IND, KC, DEN, ATL, HOU, LA, SNV, NY, WAS	0	0	0.000

ATL Atlanta, *CHI* Chicago, *DEN* Denver, *HOU* Houston, *IND* Indianapolis, *KC* Kansas City, *LA* Los Angeles, *NY* New York, *SEA* Seattle, *SNV* Sunnyvale, *WAS* Washington, DC

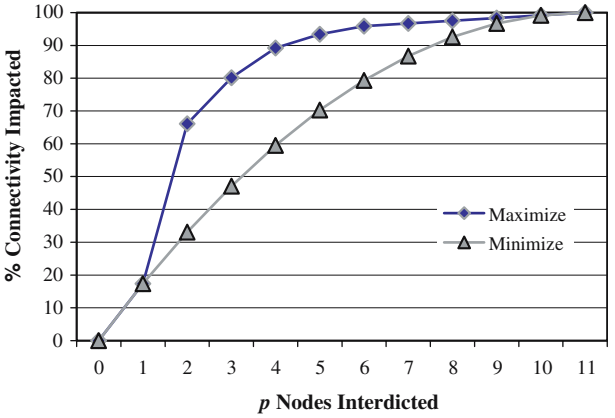

Fig. 2 Connectivity reduction for each interdiction scenario

Table 2 FIM solutions for maximum flow interdiction (actual O–D flow)

p	Objective (bytes)	Cities interdicted	Iterations	Branches	Time (s)
1	18,334,225,068,600	WAS	76	0	0.031
2	35,832,056,381,650	IND, WAS	50	0	0.016
3	39,517,310,353,850	IND, SNV, WAS	70	0	0.047
4	44,640,185,137,700	ATL, KC, NY, SNV	35	0	0.015
5	46,760,549,968,700	ATL, CHI, KC, SNV, WAS	18	0	0.015
6	48,063,525,105,550	DEN, HOU, IND, NY, SNV, WAS	7	0	0.016
7	48,251,182,933,150	CHI, DEN, HOU, IND, NY, SNV, WAS	6	0	0.015
8	48,427,837,682,950	ATL, CHI, HOU, KC, NY, SEA, SNV, WAS	5	0	0.000
9	48,568,772,694,250	ATL, CHI, HOU, IND, KC, NY, SEA, SNV, WAS	2	0	0.016
10	48,656,176,339,000	ATL, CHI, HOU, IND, KC, LA, NY, SEA, SNV, WAS	0	0	0.016
11	48,728,171,337,750	ATL, CHI, DEN, HOU, IND, KC, LA, NY, SEA, SNV, WAS	0	0	0.015

ATL Atlanta, *CHI* Chicago, *DEN* Denver, *HOU* Houston, *IND* Indianapolis, *KC* Kansas City, *LA* Los Angeles, *NY* New York, *SEA* Seattle, *SNV* Sunnyvale, *WAS* Washington, DC

transmission yields very different interdiction scenarios. Table 2 shows that interdicting Washington, D.C. would be the single node causing the greatest impact, representing a decrease in flow of over 37% (total O–D flow is 48,728,171,337,750 bytes). If two nodes are interdicted ($p = 2$), then Washington, D.C. and Indianapolis are found to cause the greatest decrease in flow (over 73%). The tradeoff curve for nodes interdicted versus total flow disrupted is shown in Fig. 3, summarizing the results given in Table 2. To illustrate the spatial impacts of an interdiction scenario, Fig. 4 depicts the $p = 3$ solution from Table 2, a configuration that disrupts over 81% of total system flow. These results highlight an important difference between interdiction of

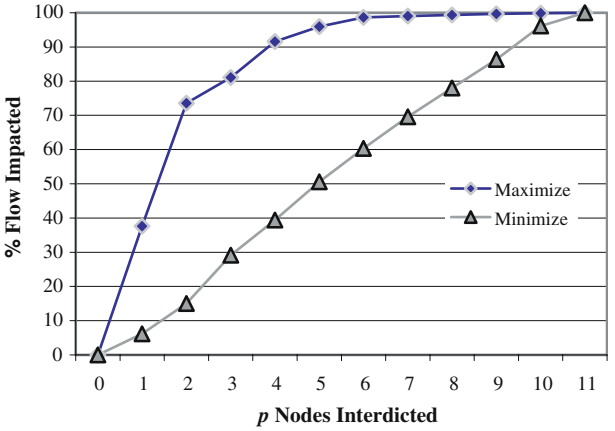

Fig. 3 Flow reduction for each interdiction scenario

connectivity and interdiction of flow. As can be discerned from the Abilene network, the loss of any single node ($p = 1$) will equivalently impact network connectivity. Similarly, several optimal solutions to the disruption of two nodes ($p = 2$) exist for the case of connectivity (Kansas City and Atlanta; Indianapolis and Houston; and Kansas City and Houston). Multiple optima are expected when O–D connectivity is of interest given that O–D pairs are given equitable treatment. In such cases, alternate optima could possibly be identified through incorporating Dantzig-type cuts as is done in ReVelle and Rosing (2000). The existence of multiple optimia changes when impacts to system flow are considered, however. Interdiction impact does not necessarily depend upon level of connectivity, but rather flow between origins and destination. For instance, the two-node interdiction scenario maximizing damage

Fig. 4 Maximal flow interdiction ($p = 3$)

discussed earlier (Washington D.C. and Indianapolis) does not maximize connectivity damage. In fact, six other scenarios cause a greater impact to system flow than this particular interdiction set (Matisziw et al. 2005), highlighting that connectivity and system flow are very different performance issues.

Table 3 and Fig. 2 detail the results for minimizing impact to O–D connectivity. In the best-case scenario, the FIM identified Houston as the location with minimal connectivity loss. As can be observed in Table 3, more computational effort is required when computing a minimum. The results for minimizing impact to O–D flow are shown in Table 4 and Fig. 3. Here, removal of Kansas City impacts system flow the least. Figure 5 illustrates the resulting minimum impact to flow given the interdiction of three nodes. In this case, Indianapolis, Denver, and Kansas City are interdicted.

5 Discussion and conclusions

This paper has introduced an unified spatial optimization formulation, the flow interdiction model (FIM), for examining risk and vulnerability associated with network interdiction. The FIM can be used to identify either worst-case or best-case impacts to system flow given any specified interdiction scenario, providing upper and lower bounds on potential system degradation. Myung and Kim (2004) implicitly attempted to establish such bounds when network arcs were interdicted, but ultimately could do so only heuristically. Specifically, they address system flow interdiction by introducing an integer program and heuristic solution method to identify scenarios maximizing flow disrup-

Table 3 FIM solutions for minimum connectivity interdiction (unit flow on each O–D pair)

p	Objective (O–D pairs)	Cities interdicted	Iterations	Branches	Time (s)
1	21	HOU	482	0	0.235
2	40	ATL, HOU	3,056	78	0.531
3	57	ATL, HOU, LA	4,069	147	0.703
4	72	ATL, HOU, LA, SNV	5,651	217	0.797
5	85	ATL, HOU, LA, SNV, WAS	5,111	239	0.766
6	96	SEA, CHI, IND, KC, DEN, NY	4,388	181	0.672
7	105	SEA, CHI, IND, KC, DEN, NY, WAS	4,116	172	0.594
8	112	SEA, CHI, IND, KC, DEN, SNV, NY, WAS	3,091	77	0.500
9	117	SEA, CHI, IND, KC, DEN, LA, SNV, NY, WAS	1,805	31	0.516
10	120	SEA, CHI, IND, KC, DEN, ATL, LA, SNV, NY, WAS	461	0	0.047
11	121	SEA, CHI, IND, KC, DEN, ATL, HOU, LA, SNV, NY, WAS	0	0	0.000

ATL Atlanta, *CHI* Chicago, *DEN* Denver, *HOU* Houston, *IND* Indianapolis, *KC* Kansas City, *LA* Los Angeles, *NY* New York, *SEA* Seattle, *SNV* Sunnyvale, *WAS* Washington, DC

Table 4 FIM solutions for minimum flow interdiction (actual O–D flow)

P	Objective (bytes)	Cities interdicted	Iterations	Branches	Time (s)
1	3,005,725,742,050	KC	75	0	0.078
2	7,331,100,352,550	DEN, KC	994	0	0.172
3	14,188,998,793,400	IND, DEN, KC	933	0	1.328
4	19,199,863,625,850	SEA, DEN, KC, SNV	712	0	0.984
5	24,632,533,830,000	SEA, IND, DEN, KC, SNV	514	0	0.187
6	29,387,932,211,450	SEA, DEN, KC, SNV, LA, HOU	447	0	0.109
7	33,900,402,066,750	SEA, DEN, KC, SNV, LA, ATL, HOU	475	0	0.125
8	37,991,186,263,500	SEA, IND, DEN, KC, SNV, LA, ATL, HOU	427	0	0.125
9	42,081,550,917,850	SEA, CHI, IND, DEN, KC, SNV, LA, ATL, HOU	364	0	0.078
10	46,847,164,742,900	SEA, CHI, NY, IND, DEN, KC, WAS, LA, ATL, HOU	337	0	0.062
11	48,728,171,337,750	SEA, CHI, NY, IND, DEN, KC, WAS, SNV, LA, ATL, HOU	0	0	0.015

ATL Atlanta, *CHI* Chicago, *DEN* Denver, *HOU* Houston, *IND* Indianapolis, *KC* Kansas City, *LA* Los Angeles, *NY* New York, *SEA* Seattle, *SNV* Sunnyvale, *WAS* Washington, DC

tion. Their model, however, is a special case of the FIM in that it does not permit minimization of system impact, though a lower bound heuristic is suggested. The work of Myung and Kim (2004) highlights the need for the FIM as it provides a unified approach to derive exact bounds on possible network interdiction impacts. The application results highlight the capabilities of the FIM to derive these bounds using commercial optimization software, requiring little computational effort. For the system evaluated here both path enumeration and model solution were easily handled. Though the network application was not particularly large, the developed approach is feasible and valid for examining interdiction risk and vulnerability in network infrastructure.

Another point to elaborate on is the relationship between connectivity and flow, as the applications of the FIM to the Abilene network display some subtle differences. A close examination of Tables 1 and 2 suggests that node combinations associated with maximal system flow interdiction do not correspond to the same nodal combinations when maximizing O–D connectivity interdiction. Obviously the difference is due to the fact that connectivity is not equivalent to total system flow. For example, if we examine the scenario where one node is to be interdicted, the loss of Washington, D.C. disrupts the most flow ($p = 1$ in Table 2) while the loss of Indianapolis disrupts the greatest O–D connectivity ($p = 1$ in Table 1). This is not completely unexpected given the basic flow information and topological characteristics of the network. This is a very important observation for several reasons. First, and most obvious, nodal interdiction combinations for maximizing flow and connectivity disruptions rarely coincide completely. Thus, considering previous work on the attack tolerance and overall robustness of the Internet and other

Fig. 5 Minimal flow interdiction ($p = 3$)

scale-free networks (Albert et al. 2000, 2004; Barabasi et al. 2000, 2001), it is clear that much of the complexity associated with network interaction remains unaddressed. In other words, high nodal connectivity (degree) does not necessarily correspond to an equally high level of network flow or utilization. Second, from a geographic perspective, the nodes identified for interdiction by FIM in the various scenarios are quite interesting. For example, while Denver appears to play an important role in both connectivity and flow for the network (Fig. 1), it is not identified as a high priority interdiction node until $p \geq 5$ in either case. This is somewhat surprising given its relatively central geographic location on the network. In contrast, while Washington is an extremely critical node for network flow, appearing in the interdiction sets for $p = 1$–3 (Table 2), it is not a connectivity priority until $p \geq 6$. Again, this suggests that high levels of network interaction for a node do not necessarily correspond to a high degree of connectivity to the network. Moreover, the implications are that both criteria need to be considered when evaluating the characteristics of a network. These differences might play a more important role when examining the survivability requirements of a network, particularly if the fortification or protection of node-based network elements is being considered.

The FIM was applied to the Abilene network, illustrating its feasibility and validity. Perhaps most significant in this application was that non-intuitive scenarios are found, precisely what we look to optimization models to help us find. Though physical characteristics of networks are typically modeled as interdiction targets, more dynamic and less observable characteristics further increase the level of complexity involved. This is especially true given consideration of multiple origins and destinations and their patterns of spatial interaction. The threat of facility attack is a reality shared by many types of critical network infrastructures, and preparing for such a possibility is chal-

lenging. Here an optimization problem was formulated to address such a need. However, application of the FIM is not limited to planning for network survivability, but can also be useful in the location of facilities to monitor flow activity, such as weigh stations, surveillance points, traffic control, checkpoints, etc.

References

Abilene (2005) http://www.abilene.internet2.edu/

Albert R, Jeong H, Barabasi AL (2000) Error and attack tolerance of complex networks. Nature 406:378–382

Albert R, Albert I, Nakarado GL (2004) Structural vulnerability of the North American power grid. Phys Rev E 69:025103(R)

Ball MO, Golden BL, Vohra RV (1989) Finding the most vital arcs in a network. Oper Res Lett 8:73–76

Barabasi AL, Albert R, Jeong H (2000) Scale-free characteristics of random networks: the topology of the worldwide web. Physica A 281:69–77

Barabasi AL, Ravasz E, Vicsek T (2001) Deterministic scale-free networks. Physica A 299:559–564

Baran P (1964) On distributed communications networks. IEEE Trans Commun Syst 12:1–9

Bell MGH (2000) A game theory approach to measuring the performance reliability of transport networks. Transport Res B 34:533–545

Carlier J, Li Y, Lutton J (1997) Reliability evaluation of large telecommunication networks. Discret Appl Math 76:61–80

Carreras BA, Lynch VE, Dobson I, Newman DE (2002) Critical points and transitions in an electric power transmission model for cascading failure blackouts. Chaos 12:985–994

Chassin DP, Posse C (2005) Evaluating North American electric grid reliability using the Barabasi-Albert Network Model. Physica A 355:667–677

Church RL, Scaparra MP, Middleton RS (2004) Identifying critical infrastructure: the median and covering facility interdiction problems. Ann Assoc Am Geograph 94:491–502

Corley HW, Chang H (1974) Finding the n most vital nodes in a flow network. Manage Sci 21:362–364

Corley HW, Sha DY (1982) Most vital links and nodes in weighted networks. Oper Res Lett 1:157–360

Crucitti P, Latora V, Marchiori M (2004) Model for cascading failures in complex networks. Phys Rev E 69:045104(R)

Department of Homeland Security (DHS) (2004) Sharing information to protect the economy. URL: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml

Department of Homeland Security (DHS) (2005) Sharing information to protect the economy. URL: http://www.dhs.gov/dhspublic/display?theme = 73&content = 1375

Doyle JC, Alderson DL, Li L, Low S, Roughan M, Shalunov S, Tanaka R, Willinger W (2005) The 'robust yet fragile' nature of the Internet. Proc Natl Acad Sci 102:14497–14502

Executive Order 1995—Critical Infrastructure Protection. Federal Register, July 17, 1996. vol 61, no. 138. pp 37347–37350. Reference is on p 37347

Grubesic TH, Murray AT (2006) Vital nodes, interconnected infrastructures and the geographies of network reliability. Ann Assoc Am Geograph 96:64–83

Grubesic TH, O'Kelly ME, Murray AT (2003) A geographic perspective on commercial Internet survivability. Telemat Inform 20:51–69

Grubesic TH, Murray AT, Mefford J (2006) Continuity in critical network infrastructures: accounting for nodal disruptions. In: Murray A, Grubesic T (eds) Reliability and vulnerability in critical infrastructure: a quantitative geographic perspective. Springer, Heidelberg

Hodgson MJ, Rosing KE, Zhang J (1996) Locating vehicle inspection stations to protect a transportation network. Geograph Anal 28:299–314

Holme P, Kim BJ, Yoon CN, Han SK (2002) Attack vulnerability of complex networks. Phys Rev E 65:056109
Houck DJ, Kim E, O'Reilly GP, Picklesimer DD, Uzunalioglu H (2004) A network survivability model for critical national infrastructures. Bell Labs Tech J 8:153–172
Kalvenes J, Kennington J, Olinick E (2004) Hierarchical cellular network design with channel allocation. Eur J OperRes 160:3–18
Latora V, Marchiori M (2005) Vulnerability and protection of infrastructure networks. Phys Rev E 71:015103(R)
Matisziw TC, Murray AT, Grubesic TH (2005). Assessing network interdiction and potential risk to O–D interaction (submitted for publication)
Myung Y-S, Kim H-J (2004) A cutting plane algorithm for computing *k*-edge survivability of a network. Eur J Oper Res 156:579–589
Nardellia E, Proiettia G, Widmayer P (2003) Finding the most vital node of a shortest path. Theor Comput Sci 296:167–177
Office of Management and Budget (OMB) (2006). Homeland security. URL: http://www.whitehouse.gov/omb/pdf/Homeland-06.pdf
Palmer CR, Siganos G, Faloutsos M, Faloutsos C, Gibbons PB (2001) The connectivity and fault-tolerance of the Internet topology. URL: http://citeseer.ist.psu.edu/444798.html
Ratliff HD, Sicilia GT, Lubore SH (1975) Finding the *n* most vital links in flow networks. Manage Sci 2:531–539
ReVelle CS, Rosing KE (2000) Defendens imperium Romanum: a classical problem in military strategy. Am Math Mon 107(7):585–594
Salmeron J, Wood K, Baldick R (2004) Analysis of electric grid security under terrorist threat. IEEE Trans Pow Syst 19:905–912
Soni S, Pirkul H (2000) Design of survivable networks with connectivity requirements. Telecommun Syst 20:133–149
White House (2003) The national strategy for the physical protection of critical infrastructures and key assets. URL: http://www.whitehouse.gov/pcipb/physical_strategy.pdf
Wollmer R (1964) Removing arcs from a network. Oper Res 12:934–940
Wood KR (1993) Deterministic network interdiction. Math Comput Modell 17:1–18