

Network Interdiction Methods and Approximations in a Hazmat Transportation Setting

Justin Yates

Introduction

The United States transportation system is an extensive and integrated component in the eight key infrastructures upon which the livelihood of the U.S. is dependent (Department of Homeland Security 2009). The accessibility and mobility enabled through open use of the transportation system is a vital and necessary freedom which contributes to the fluidity of the American environment. The transportation system is expansive and heavily utilized with an average of over 2 billion daily vehicle-miles of travel (nearly twice as much travel since the early 1980s) on the roughly 4 million miles of paved roadway, nearly 47,000 miles of Interstate highway, 600,000 bridges and 366 U.S. highway tunnels over 100 m (Texas Transportation Institute 2011; Transportation Security 2012). Travelers and shippers may also choose to utilize more than 300,000 miles of freight rail, nearly 10,000 miles of urban and commuter rail systems, or connect between 500 commercial-service and 14,000 general aviation airports (Transportation Research 2002).

In this chapter, a general review of network-based hazardous material transportation models will be given. Specific attention will be given to the network interdiction model and its variants (e.g. shortest path network interdiction) as these models have recently become popular in the domain of homeland security. The chapter will focus on the application of network interdiction models to networks of various size and structure and the ensuing computational performance (including objective value, sensitivity to network properties, etc.) and spatial structure (e.g. resource allocation, network connectivity/density) of the interdiction solutions. A systematic experimental analysis will be designed to identify salient network and regional properties impacting interdiction solutions (e.g. proximity to origin points, initial arc

J. Yates (✉)

Industrial and Systems Engineering, Texas A&M University, College Station, TX, USA
e-mail: jtyates@tamu.edu

metric values, etc.). Current approximations for the network interdiction model will also be analyzed against the obtained solutions, including alternate approximation formulations as well as alternate solution approaches. The evaluation of such techniques will lead to greater insight on the effect of network and problem structure to resource allocation in interdiction models.

Literature Review

This section will provide some supporting background in past and current hazardous materials transportation research. A history and survey of past research initiatives will be followed by identification of current research threads in network-based infrastructure protection whose roots and foundation can be traced back to the hazardous material literature. Attention will be given to the quantification of risk, potential pitfalls, and benefits/drawbacks of estimation as a tool to measure risk. Discussion and justification for a selection of related mathematical models such as the Vehicle Routing Problem with Time Windows, Discrete Fractional Programming, and Shortest Path Network Interdiction will be provided in addition to some brief detail on algorithm/heuristic modeling within hazardous materials transportation problems. In addition to optimization, this section will introduce past practices in the field of Geographic Information Science (GIS) geared towards supporting and augmenting risk analysis, routing and scheduling problems through spatial reasoning methods. This section will conclude with a detailed discussion on the Network Interdiction problem, which is used as the test-bed formulation throughout the remainder of this chapter.

In 2001, there were 41,527 active hazmat motor carriers in the United States driving an average of 800,000 truck shipments per day of hazardous materials (hazmat) over the nation's roadways (Field 2004). By 2011, the number of active hazmat motor carriers has grown to 61,000, transporting over 2 billion tons of hazmat annually (Transportation Security 2012). Similarly in 2011, there were 5.76 million hazmat inspections carried out by the U.S. Department of Transportation with 3.75 million vehicle inspections. In approximately 19,400 of 740,000 inspection cases on interstate and hazmat certified carriers, unsafe or fatigued driving conditions were reported (Transportation Security 2012).

The commingling of commercial, personal, and hazmat travel has fueled an emphasis on safety in the transportation industry, not merely from the perspective of individual harm, but also the durability and maintenance of the integrity and serviceability of the transportation systems themselves (as an example, the U.S. Department of Transportation (DOT) publishes a biennial report on the status of hazmat transportation) (National Highway 1996; US Department of Transportation 2006). Additionally, academic researchers have heightened focus on the problem of increasing safety and, more recently, security of hazmat shipments, especially through populated areas or near perceived targets (i.e. nuclear power plants, water resource plants, etc.).

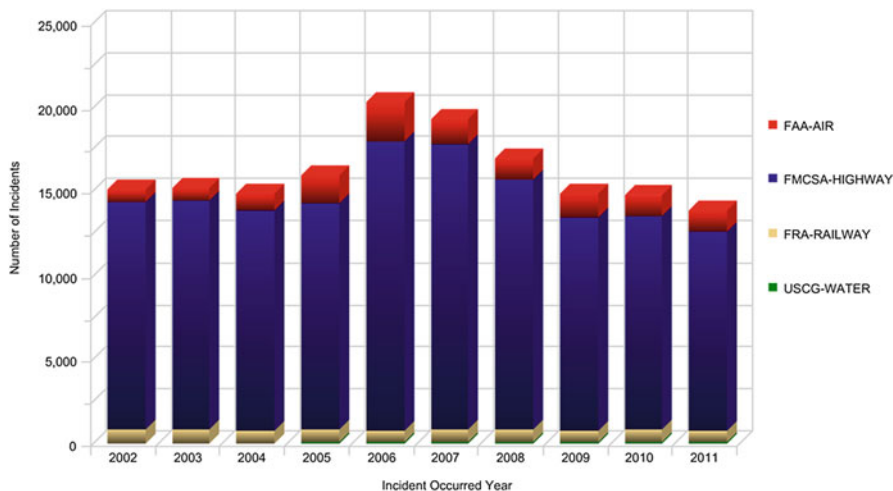


Fig. 1 All incidents by mode and incident year (US Department of Transportation 2012)

Figure 1 and Tables 1, 2, 3, and 4 illustrate the frequency of incidents occurring during hazmat transportation by air, highway, railway and waterway. Hazardous material transportation incidents in 2011 resulted in over \$100 million in damages with a 10-year cumulative total of over \$670 million. Additionally, the size and magnitude of hazmat transportation across the U.S. and the attractiveness of its cargo (which could be used by both domestic and international organizations to create situations of intentional public exposure or weaponization) generates support for an immense number of research opportunities geared towards creating safer, more stable and less vulnerable hazmat transportation.

A History in Hazardous Materials Transportation Research

The concept of risk, and its quantification, however ambiguous, has been the driving force behind many popular models related to infrastructure protection, transportation and, in recent years, homeland security. Risk in hazardous materials transportation was most succinctly measured as the product of incident probability and incident consequence. Incident probability implies occurrence of an accident that releases or exposes a region/population to hazardous material while incident consequence quantitatively measures the impact(s) of release. Ideally, these probabilities would be based on real-world data and historical statistics, leaving little room for interpretation. In practice, there are many pitfalls in quantifying risk, including, the lack of accurate and specific historical data and lack of a clear and agreed upon definition of risk head this list. With respect to data collection, a true calculation of risk would include meteorological and topological knowledge, accurate effects

Table 1 Incidents by mode and incident year

Mode of transport	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	Grand total
FAA-AIR	732	750	993	1,654	2,406	1,556	1,278	1,356	1,293	1,240	13,258
FMCSA-HIGHWAY	13,502	13,594	13,068	13,460	17,159	16,930	14,805	12,730	12,645	11,857	139,750
FRA-RAILWAY	870	802	765	745	703	753	748	642	751	692	7,471
USCG-WATER	10	10	17	69	68	61	99	90	105	63	592
Grand total	15,114	15,156	14,843	15,928	20,336	19,300	16,930	14,818	14,794	13,852	161,071

Table 2 Fatalities by mode and incident year

Mode of transport	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	Grand total
FAA-AIR	0	0	0	0	0	0	0	0	0	0	0
FMCSA-HIGHWAY	9	15	11	24	6	9	6	11	8	10	109
FRA-RAILWAY	1	0	3	10	0	0	1	1	0	0	16
USCG-WATER	0	0	0	0	0	0	3	0	0	0	3
Grand total	10	15	14	34	6	9	10	12	8	10	128

Table 3 Injuries by mode and incident year

Mode of transport	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	Grand total
FAA-AIR	4	1	11	44	2	8	7	10	2	7	96
FMCSA-HIGHWAY	118	105	155	178	192	160	153	153	153	109	1,476
FRA-RAILWAY	14	13	122	693	25	57	63	38	13	20	1,058
USCG-WATER	0	0	0	0	15	3	0	0	2	8	28
Grand total	136	119	288	915	234	228	223	201	170	144	2,658

Table 4 Damages by mode and incident year

2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	Grand total
\$108,630	\$100,483	\$188,481	\$198,316	\$670,521	\$88,030	\$191,434	\$707,939	\$20,267	\$171,467	\$2,445,568
\$48,075,528	\$49,109,443	\$47,157,765	\$40,179,241	\$59,502,295	\$47,279,979	\$42,889,714	\$50,628,781	\$63,841,312	\$96,629,446	\$545,293,504
\$9,745,140	\$4,126,165	\$13,901,020	\$15,454,556	\$10,739,810	\$27,305,219	\$7,939,038	\$17,557,034	\$17,358,060	\$7,013,438	\$121,139,480
\$247,802	\$261,324	\$1,654,664	\$114,000	\$58,828	\$19,097	\$138,350	\$100,887	\$574,103	\$205,000	\$3,374,055
\$58,177,100	\$53,597,415	\$62,901,930	\$55,946,113	\$70,971,454	\$74,692,325	\$51,158,536	\$68,994,641	\$71,793,742	\$104,019,351	\$672,252,607

and dispersion of the spilled substance, location of individuals at the time of the incident, and human does response, to name a few. Note that this list does not begin to include components related to economic and environmental damage, as well as social and socio-economic implications which may be desired in quantifying incident consequence) (List et al. 1991; Erkut and Verter 1998). This impracticality has led hazmat modelers to adopt estimation metrics that avoid such extensive, time consuming data collection, with varying degrees of complexity and success.

The ultimate goal of risk measurement is to utilize estimation techniques that drive the optimization procedure and accurately replicate real-world scenarios without obtaining an overwhelming amount of data. List et al. (1991) refers to this as constructed risk or a constructed index. A constructed index, in its most simplistic form, decomposes the network, examining its individual arcs, assigning a pseudo cost to each arc, and implementing algorithms such as Yen's shortest path algorithm in an effort to succinctly yet accurately represent the true environment. Here, (1) illustrates the risk function, where R_{AB} is the risk (which would be used instead of link length as the cost in a shortest path algorithm) for link AB , p_{AB} is the probability of an incident occurring on link AB , and C_{AB} is the consequence for AB , which is nearly always contingent (either partially or exclusively) on the population density within a certain vicinity of the road segment (Erkut and Verter 1998).

$$R_{AB} = p_{AB}C_{AB} \quad (1)$$

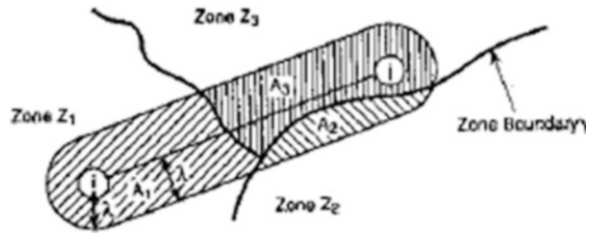
Assisting in the determination of p_{AB} , incident probability studies examining variations in release rate by mode, carrier type, vehicle type, road classification, time of day and weather conditions may be used (List et al. 1991). Estimation tools for incident consequence typically take on the form of a "danger circle" (Erkut and Verter 1998) or "buffer zone" (Laefer and Pradhan 2006; Huang et al. 2004) such that all individuals within the zone are determined to be exposed to a fatal hazmat incident. It is important to note that, depending on the time of day and area, population estimates may vary significantly from static figures such as census counts (Erkut and Verter 1998). Total edge consequence may be derived under the assumption that an edge is composed of n unit segments, each with uniform parameters (Erkut and Verter 1998). Expected edge consequence may then be defined by (2) (variable interpretation is the same as above) and, since p (probability of a hazmat incident) is typically very small (on the order of one per one million miles), approximated as in (3) (Erkut and Verter 1998).

$$pC + (1 - p)pC + (1 - p)^2pC + \dots + (1 - p)^{n-1}pC \quad (2)$$

$$(pn)C \quad (3)$$

It is this value that would be substituted in the objective function of a shortest path problem, creating an optimization problem that would return the path of minimum risk from an origin-destination (O-D) pair given the current network.

Fig. 2 Zone segmentation along a link



While this approach is eloquent in its relative simplicity, key assumptions reduce the realism of the output. Primarily, the assumption that each unit segment of an edge has uniform properties is limiting. Additional nodes that separate a link without uniform properties into its uniform components may be added, without influencing the optimal outcome. However, this approach is impractical for large networks and also increases the number of constraints in the optimization problem, potentially increasing computation time significantly. If this assumption cannot be made, then expected edge consequence may not be approximated as succinctly as in (3), preventing the shortest path approach (Erkut and Verter 1998).

In practice, multiple trips are necessary to effectively move material, and consideration of consequence over numerous shipments between an O-D pair is necessary to accurately reflect the repercussions of an incident. Viewing these shipments as a sequence of independent Bernoulli trials was discussed in detail by Jin et al. (1996) and Jin and Batta (1996) and continued in Batta and Chiu (1998). Underlying these works is the observation that multiple, but finite, hazmat trips are often needed to transport all of the material. Total shipments may be unrestricted (continuing until all material is shipped), or may be suspended or ceased after a critical threshold on the number of accidents is reached (Jin et al. 1996). Probability of link incident (p_i) and consequence of link incident (C_i) remain, while introduction of the variable t (threshold number of accidents) and T (total trips to be made) allow for new objective considerations (Jin et al. 1996). Varying the values of t and T , alternative objectives such as expected total consequence, expected consequence per trip, and expected number of trips between two successive accidents are considered (Jin and Batta 1996).

Risk equity, described as the fair dispersion of risk throughout a population, represents yet another way that hazmat transportation has been viewed and modeled. The objective function in a risk equity problem is to find a set T of routes (not necessarily distinct) that minimize total risk over a network/region while constraining the difference in total risk between every pair of zones within a specified threshold T_μ (Gopalan et al. 1990). Figure 2 illustrates a typical instance of network segmentation, where link (i, j) directly spans two zones and indirectly influences a third (Gopalan et al. 1990).

Instead of viewing the incident and its consequence separately, multi-criterion optimization problems can be formulated to consider individual hazmat transportation problem components individually within a system-optimized mathematical

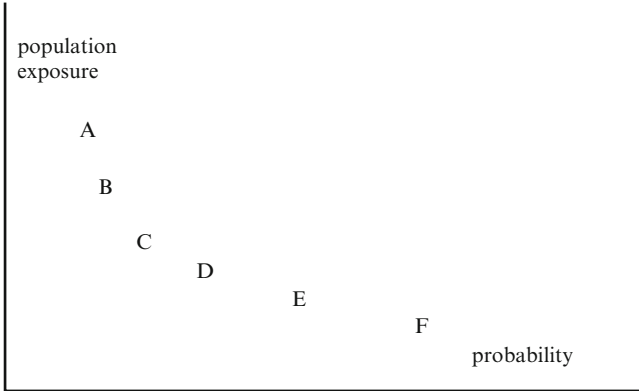


Fig. 3 Efficient frontier of a typical bi-criterion minimization problem

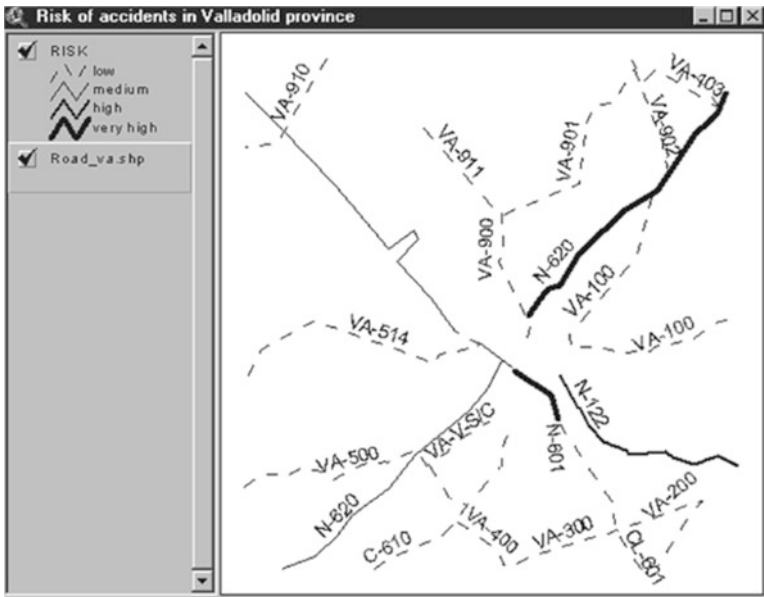


Fig. 4 Risk map for aniline transportation in Valladolid

model. Figure 3 shows a typical bi-criterion efficient frontier for two factors (incident probability and population exposure), with each letter representing a different optimal solution on the efficient frontier generated applying different weights to the objective function criteria (Erkut and Verter 1998). Huang et al. (2004) extends this approach, identifying five criteria (exposure, socio-economic impact, risk of hijack, traffic conditions, and emergency response) of potential interest in hazmat route choice (Fig. 4).

Shifting from the macro-scale view of equity and multiple criteria, approaches focusing on individual network components at a micro scale emerged as a natural complement. Arc vulnerability modeling considers extrinsic, tangible elements that lie in the vicinity of the link (i.e. hospitals, education centers, sports facilities, shopping centers, power stations, water treatment centers, etc.) to quantify an individual arc metric which is used to formulate the given optimization problem. The concept may be enhanced by incorporating non-vicinity related tangibles such as network redundancy, capacity, traffic demand and highway configuration, which may positively or negatively influence the importance of a link (Cova and Conger 2003). Also, natural disasters such as earthquakes, may cause fires, landslides, and facilitate dam failures (and consequently floods), all possible contributors to network disconnection and transportation disruption. The flexibility such approaches gave to modelers has made them strong favorites and many contemporary homeland security models can be traced back to these formulations.

Considering, for example, least-flood-risk as an additional criteria for routing in a multi-criterion model, link cost could be quantified as in (4), where the denominator models flood characteristics ($\alpha_h \in [0, 1]$ representing flood height and $\alpha_v \in [0, 1]$ representing flood velocity) such that if no flooding is present, the cost is simply the numerator (in this case, the length of link (i, j)) (Cova and Conger 2003).

$$c_{ij} = \frac{L_{ij}}{\alpha_h \alpha_v} \quad (4)$$

Simulation software may also be used to help quantify link vulnerability, especially in the area of natural disasters. The Federal Emergency Management Agency (FEMA) has created a software tool named HAZUS, which may be used to observe how transportation networks react to the adverse affects of natural disasters (Federal Emergency Management 2006). Similarly, the Federal Highway Administration recognizes REDARS, used exclusively to determine how seismic events impact road and highway systems (MCEER 2006).

Network Models and Interdiction

Network stability and the maintenance of serviceability have already been shown to be of great concern when considering the routing of hazmat. The functioning of links in a network may be negatively influenced by congestion and accidents, weather, seismic activity and natural disasters, the occurrence of hazmat incidents, intentional acts to disrupt the network, or by the combination of any two or more such instances.

One way to identify network vulnerability is through the identification of critical links. A link is deemed “weak” if incident probability is high, “important” if consequence of an incident is large, and “critical” if it is both weak and important (Jenelius et al. 2006). These values are derived through the observation of how

link absence affects path travel time, using multiple, predetermined, O-D paths to evaluate (Jenelius et al. 2006). Additionally, incorporation of key-infrastructure (i.e. proximity of the link to schools, hospitals, military, power or water facilities) could assist in more realistic modeling, where such vulnerable sites (potential targets) contribute to the link's importance (Luedtke and White 2002). Criticality of links is also dependent on the geographic features over which the network lies (i.e. coastline, mountain ridge). These features hinder the existence of nearby options available for re-routing without significant time delay. Therefore, it is useful to consider inherent network vulnerability through quantitative means and incorporate this into a risk or routing model. The generality of Jenelius et al. (2006), is applied to optimization of hazmat transportation, developing a mathematical model called the Hazardous-Network Design Problem (HDP).

Given a road network, HDP selects links that should be closed to hazmat transportation in order to minimize total risk (Kara and Verter 2004). The formulation of the HDP is bi-level, containing an outer and inner problem that more accurately represents the interaction between policy makers and hazmat carriers (there is often predominance in hazmat routing problems favoring the carriers' viewpoint (i.e. routing) and omitting regulator decision-making pertaining to link availability). The inner problem minimizes the combined travel distance of the trucks subject to flow conservation, and may be viewed as either a minimum cost network flow or a constrained shortest path problem, while the solution of the outer problem minimizes population exposure. The two problems interact with the binary decision variables of the outer problem becoming the parameters of the inner problem (Kara and Verter 2004). Success of the model prescribes the available road network and route choices for hazmat transportation.

The term interdict is defined by Merriam-Webster's dictionary as the adjective "to destroy, damage, or cut off (as an enemy line of supply) by firepower to stop or hamper an enemy." The problem of network interdiction may then be taken to mean the intentional destruction, by force, of a network to impede or cease enemy use. Within the realm of optimization, especially in the military community, the study of interdiction problems has been given significant attention.

Considering network flow, the interdiction problem may be represented as a multi-commodity problem with two players (Lim and Smith 2007). The first player, the follower, makes profit by delivering commodities to designated destinations. The leader attempts to minimize the followers profit by selectively destroying arcs, the destruction of which costs the leader by subtracting a link destruction amount from the leaders' interdiction budget. Arcs may either be destroyed discretely (either capacity flow is possible or no flow is possible) or continuously (partial flow over links is allowed). The Multi-Commodity Flow Network Interdiction Problem (MFNIP) is then modeled as the minimization of the maximum profit the follower may achieve, subject to conservation of flow constraints, the leaders' budget constraint, and non-negativity (Lim and Smith 2007). From the followers' perspective, MFNIP quantifies a worst-case scenario that showcases the weakest (or most vulnerable) links in a network. This information may then be used in the strengthening of weak points or the enhancement of network connectivity to

better secure the system (Qiao et al. 2007). In addition to transportation networks, the multi-commodity flow problem may be applied to airline operations, supply chains, and telecommunications, as well as water supply networks, and power grid systems, all of which may then be examined through the MFNIP formulation to gauge network security and stability.

A review of early literature on the routing, schedule, location and risk analysis for hazardous materials transportation can be found in List et al. (1991). Specifically associated with risk analysis, Erkut and Verter (1998) provides model overviews and examines how the quantification of risk in these models affects model performance/accuracy. In the case where risk is taken to be the acceptable threshold of accidents in transport willing to be endured, Jin and Batta (1996) gives a nonlinear constrained shortest path approach and examines the effect of the accident threshold on routing decisions.

Beginning with Wood (1993) and continuing through Israeli and Wood (2002), Brown et al. (2006) and others, network interdiction began to emerge as a natural extension to hazardous materials transportation research. The problems are decidedly similar and deal with undesirable transportation through a network. In the hazardous materials transportation problems, risk and exposure were two of the quantifiable measures applied to each arc or node of the network and used as the basis for determining appropriate route selections. In the case of Israeli and Wood (2002) and Brown et al. (2006), the quantifiable arc measure is length, which is increased when an arc is interdicted. In these two-player network interdiction problems, these elongated arcs effectively deter the opposing player from using these arcs in composing their shortest path. Scaparra and Church (2008) and Church and Scaparra (2007) model interdiction at network nodes with interdiction removing the ability of a facility located at that specific node from satisfying demand to other nodes. Considering the minimization of weighted demand-distance as the objective, an optimal nodal interdiction strategy will increase the opposing player's cost to satisfy network demand.

As these and other recent mathematical models transition from an emphasis on risk assessment and hazardous materials transportation to problems of homeland security and extreme events, five major factors can be used to delineate and differentiate model focus, intent and capability. The five major factors offered in Yates and Sanjeevi (2012) are formulation, objective function, interdiction metric, component interdiction and the Origin–destination policy. Formulation refers to single versus bi/multi-level models. Objective function details whether the original objective function provided for a given problem is additive or multiplicative/probabilistic (note that this is the original objective function and does not refer to any transformations applied during the solution process). Interdiction metric refers to whether the individual metrics used are continuously or discretely interdicted while Component Interdiction dictates whether these metrics are arc-based, node-based, or network/spatially based. Lastly, Origin–destination policy refers to the existence of a single O-D pair or multiple O-D pairs in the problem. Table 5 is now introduced to provide an overview of some representative recent

Table 5 Summary of interdiction-related problem properties (Yates and Sanjeevi 2012)

	Formulation		Objective function		Interdiction metric		Component interdiction	
	Single level	Multi-level	Summation	Product	>0	[0,1]	Arc	Node
						Z+		
Wein and Atkinson (2007)	x			x		Layers	N/A	N/A
Israeli and Wood (2002)		x	x		Length		x	x
Brown et al. (2006)		x	x		Length/value		x	x
Morton et al. (2007)		x		x		Detection	x	Probabilistic
Scaparra and Church (2008)		x	x		Weighted distance		x	x
Church et al. (2004)	x		x		Weighted distance		x	x
Church and Scaparra (2007)		x	x		Weighted distance		x	x
Murray et al. (2007)	x		x		Flow		Connectivity	x
Matisziw et al. (2007)	x		x		Flow		Connectivity	x
Matisziw and Murray (2009)	x		x		Flow		Connectivity	x
Grubescic and Murray (2005)	x		x		Demand		x	x
Southworth (2009)	x		x		Population exposure		Spatial	No origins/destinations

network interdiction literature published after 2004. For additional discussion of network interdiction problems published prior to 2004, refer to Church et al. (2004).

At its core, the shortest path network interdiction problem (SPNIP) is a two-player deterministic game being played over a network composed of arcs and nodes with a given arc/node metric (length, detection probability, etc.) and with identified origin and destination sets. In these models, any and all of these components could be completely known by both players (i.e. having perfect information) or could contain some element of mis-information, deception (imperfect information). The ability to interdict is also constrained by limited resources, which could be modeled as a finite number of arcs/nodes to interdict or a budget limitation where each interdiction comes with some associated interdiction cost.

Developed interdiction models can have objective functions that are a single level or multiple levels to reflect to degree of interaction and knowledge among the players being modeled. Examples of single-level models include Church et al. (2004) and Church and Scaparra (2007). In this case, these models are variants of traditional optimization models such as the p-Median and Maximal Covering problems that have been adapted to include interdiction concepts. In many instances, these single-layer models are solved for a variety of problem parameters and threshold values to determine a pareto front, or set of interdiction strategies to better gain situational knowledge. Such analysis is extremely useful when the capability/intent of an adversary is in question or when information is unreliable/imperfect.

Multi-level models (Morton et al. 2007; Israeli and Wood 2002; Brown et al. 2006; Church and Scaparra 2007), in contrast to single-level models, are often integer or mixed integer programs that model the decision making of players sequentially in the same formulation. Instead of solving under multiple parameter and threshold instances, the interaction between the interdictor and the defender is modeled simultaneously. The objective function in multi-level models is one that typically reflects pure competition, with the interdictor seeking to minimize an overall network metric (such as flow or satisfied demand) and the defender seeking to maximize this minimum metric. In other words, the defender's job is to minimize the effect of interdiction on their network operations. In Table 1, ">0" indicates that the interdiction metric is continuous (i.e. interdiction increases arc length by x with $x > 0$), "Z⁺" indicates the metric is integral (i.e. interdiction is based upon the number of layers penetrated) and "[0, 1]" indicates that the metric is probabilistic. In the probabilistic case, interdiction can be modeled as the probability of path detection P where $P = \prod_i a_i x_i$, $i \in P$ models path probability as the product of all arc probabilities a_i on path P ($x_i = 1$ if $i \in P$, 0 otherwise).

Multi-level models, due to their structure, can often be decomposed and solved iteratively to optimality using standard optimization techniques. One of the most straight-forward and intuitive of these solution approaches is Bender's Decomposition (Bard 1998), where the interdictor and defender "trade" moves and with each move providing some degree of information to their counterpart (recall that these problems can be set up with perfect or imperfect information). In this way, information from these consecutive player movements is continually accrued and used within the next iteration of the decomposition. At some point, the interdictor

and defender reach a state of equilibrium where no new strategies are employed. In the worst case, this equilibrium occurs after all possible moves have been explored (i.e. complete enumeration), though in practice significantly less iterations are required. This certificate of optimality, in conjunction with its intuitive approach, is a major benefit to using Bender's Decomposition (Bard 1998).

Formulating Interdiction Models

In this section, we begin to explore the shortest path network interdiction problem (SPNIP) as defined by Israeli and Wood (2002) and discuss multiple variations which can be derived from it. We will begin examining solutions to the SPNIP and its variations by looking at their computational performance when solved using Bender's Decomposition, implementation of which will also be addressed. As patterns and trends emerge in the solutions, we will begin to motivate development of alternative heuristic and approximation techniques to solve network interdiction problems. These techniques will be discussed and compared in "[Developing interdiction approximations and heuristics](#)" of this chapter.

Mathematical Models and Notation

SPNIP and SPNIP-M

We begin by presenting the SPNIP formulation of Israeli and Wood (2002) and a modified shortest path network interdiction problem (SPNIP-M) formulation of Yates and Casas (2010). Each is a discrete bi-level optimization problem with an attacker and defender. The attacker considers all identified origins and targets and uses the network to find the path with, in this case, lowest detection probability (note that many network measures such as distance or cost, could be used in place of detection). The defender locates a limited number of resources which increase arc (and subsequently path) detection probabilities. Through the remainder of this work, we will refer to the defense resources as sensors, though this term is used relatively loosely. In our modeling, a sensor's properties include a predefined range (beyond which their influence is considered to be null) as well as an associated location cost and a parameter for sensor strength.

As a point of delineation, we note that the formulation of SPNIP assumes that sensors are located directly on network arcs in a 1-to-1 fashion. SPNIP-M, on the other hand, locates sensors geographically within the region at pre-specified locations. These locations, referred to as atoms, are point locations within the continuous region containing the network/infrastructure of interest. The atom set containing all possible sensor locations for a given problem is determined through a number of different methods which can include set distances, line-of-sight, proximity, or a function containing any combination of measurable geographic

and network properties. For our initial models, we assume a simple and uniform grid pattern for atoms, though section “[Developing Interdiction Approximations and Heuristics](#)” will discuss how more intelligent atom derivations can be derived and implemented within SPNIP-M. Overall, the geographic structure of SPNIP-M increases the complexity and realism of sensor location in the interdiction model, giving the modeler more flexibility.

Terminology

Atom: Potential sensor location point within the geographic region occupied by the network.

Attacker: Seeks the path of lowest detection (i.e. shortest path) on the network. The obtained path is simple and complete and will consider all possible origin and destination pairs (previously referred to as the follower).

Defender: Allocates sensors to increase detection probability. Sensors may be located directly on the network arcs in SPNIP or at designated geographic locations (atoms) in SPNIP-M and SPNIP-LB.

Detection: The probability that movement along a given arc (path) will be observed.

Sensor: Increases detection on arcs which fall within its given range. The degree to which detection is increased depends upon the sensor’s power. Sensors are placed directly on arcs in the SPNIP and at designated geographic locations (atoms) in SPNIP-M and SPNIP-LB. Sensors have a known allocation cost.

Notation

A	Set of suitable sensor locations	c_s	Cost to locate a type s sensor
Λ	Set of network arcs	k_{ni}	$\{1, -1\}$ if node $n \in N$ is the $\{head, tail\}$ or arc $i \in \Lambda$, else 0
B	Total defense budget	η_s	Sensitivity of sensor type s , with $0 \leq \eta_s \leq 1$
N	Set of network nodes	$q_s = \{1, -1, 0\}$ if node $n \in N$ is $\{origin, target, intermediate\}$	
S	Set of sensor types	$r^{as}(i)$	1 if arc $i \in R^{as}$, else 0
τ	Overlapping coverage threshold	u_{ist}	Probability of non-detection for i covered by t type s sensors
R^{as}	Set of arcs within the influence range of a type s sensor located at atom $a \in A$		

Decision Variables

$w_i = 1$ if arc i is used in the attacker path, else 0.

$y_{as} = 1$ if sensor type s is located at atom a , else 0.

$x_{ist} = 1$ if arc i is covered by t type s sensors, else 0.

$$\begin{array}{ll}
 \text{[SPNIP]} & \text{[SPNIP-M]} \\
 z = \min \max \prod_{i,s,t} u_{ist}^{w_i y_{at}} & z^m = \min \max \prod_{i,s,t} u_{ist}^{w_i x_{ist}} \\
 \text{s.t. } \sum_i k_{ni} w_i = q_n \quad \forall & \text{s.t. } \sum_i k_{ni} w_i = q_n \quad \forall n \\
 \sum_s y_{is} = 1 \quad \forall i & x_{ist} - \frac{1}{i} \sum_a r^{as}(i) * y_{as} \leq 0 \quad \forall i, s, t \\
 \sum_{i,s} c_s y_{is} \leq B & \sum_{s,t} x_{ist} = 1 \quad \forall i \\
 w, x, y \in \{0, 1\} & \sum_{a,s} c_s y_{as} \leq B \\
 & w, x, y \in \{0, 1\}
 \end{array}$$

Regardless of the formulation, we assume a non-zero detection probability for all arcs as an attacker can never realistically be guaranteed to reach his/her target. When dealing with network-based transportation, this detection probability, albeit potentially small, can be attributed to incidental traffic violations, accidents with other motorists, or a concerned citizen alerting local authorities to a suspicious individual or vehicle. We assume that these initial arc non-detection probabilities are known. We also assume that detection is equivalent to capture as a simplistic proxy for the more complicated case where detection and interception (i.e., capture) are separate factors.

As the SPNIP and SPNIP-M formulations show, the objective function yields a path detection probability calculated by multiplying arc non-detection values for all arcs comprising the optimal attacker simple path through the network (i.e. one that begins at a designated origin, terminates at a designated target and does not cycle) given the defender's optimal sensor location strategy. We calculate the impact of a sensor's coverage as $u_{ist} = u_{i01} \prod_t \eta_s$ where η_s indicates the sensor's strength. In SPNIP-M, there is a maximum threshold of coverage, τ , beyond which an arc's non-detection probability will not be affected by additional sensor coverage. In this way, all u_{ist} values may be calculated a-priori.

In both models, the first set of constraints imposes a conservation of flow within paths that the attacker identifies and is the only constraint which includes the attacker decision variable w_i . The second constraint set in SPNIP-M does not appear in the SPNIP model and functions as a relational constraint between sensor location and the corresponding arc influence upon the network. Simply stated, an arc cannot be influenced by t type s sensors unless the defender has allocated t type s sensors containing arc i in their respective ranges. The remaining constraints in both models

guarantee arc coverage (every arc is either covered, $x_{iI} = 1$, or not covered, $x_{iO} = 1$) and limit the defender’s available resources. All variables are modeled as binary decision variables.

SPNIP-LB

In both SPNIP and SPNIP-M, an arc is considered as covered by a sensor when any portion of that arc, no matter how large or small, falls within the sensor’s range. Using this type of binary approach to coverage is highly restrictive and, one can argue, does not accurately reflect real-world sensor performance. Functions exist which define this type of behavior and have been used in past military models, where longer time spent in the range of enemy radar functionally increased one’s detection probability (Przemieniecki 2000). Using a similar functional approach, we define a length-based approach to shortest path network interdiction (SPNIP-LB) to augment the binary SPNIP and SPNIP-M formulations.

[Length Based]:

- u_i = initial probability of non-detection for arc i
- l_{ias} = length of arc i within the range of a type s resource located at atom a
- v_{ias} = proportion of non-detection reduction when arc i is influenced by a type s resource at atom a
- = $e^{-\eta_s l_{ias}}$ where $\eta_s \geq 0 \quad \forall s \in S$

SPNIP-LB

$$\begin{aligned} & \min_{y,x} \max_w \prod_{s,a,i} u_i^{w_i} v_{ias}^{w_i x_{ias}} \\ \text{s.t.} \quad & \sum_i k_{ni} w_i = q_n \quad \forall n \in N \\ & x_{ias} - r_i^{as} y_{as} \leq 0 \quad \forall i \in I, a \in A, s \in S \\ & \sum_a \sum_s x_{ias} \leq 1 \quad \forall i \in I \\ & \sum_s \sum_a c_s y_{as} \leq B \\ & w, x, y \in \{0, 1\} \end{aligned}$$

The SPNIP-LB formulation is defined by the same constraint sets as the binary SPNIP-M. In terms of modeling, SPNIP-LB differs in its derivation of non-detection

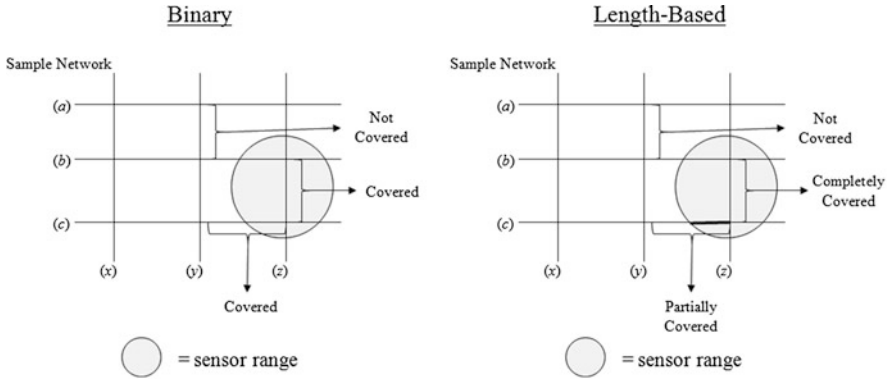


Fig. 5 Differentiating between the binary SPNIP-M and length-based SPNIP-LB formulations (Yates and Sanjeevi 2012)

probability and in composition of the objective function. In SPNIP-LB, calculation of non-detection probability is performed through a more complex function which more realistically models the connection between detection probability and time spent inside a sensor’s range (Przemieniecki 2000). Figure 5 illustrates the concept of partial coverage and how it’s able to be captured through formulation of the SPNIP-LB, adding yet another dimension of complexity for interdiction modelers.

Obtaining Solutions Through Bender’s Decomposition

The interdiction formulations previously discussed share one major property that allows for a separation-based solution approach; no single set of constraints contains both attacker and defender variables. This means that the formulations may be divided into sub-problems for the attacker and defender respectively. Once these sub-problems are composed, they may be solved iteratively and linked together in a way that the solutions obtained in one sub-problem are used to feed the other cyclically. This approach is known as Bender’s Decomposition (Bard 1998).

Implementing Bender’s Decomposition for the aforementioned interdiction models, we derive an attacker sub-problem which maximizes path non-detection and is constrained by the conservation of flow constraints and fixed defender decision variables $\bar{x}_{i, st}$ (this results in the formation of a node-arc incidence matrix where the LP relaxation will return integral solutions (Nemhauser and Wolsey 1999)). We derive the defender sub-problem to minimize path non-detection subject to the remaining constraints with the defender variables x and y and with fixed attacker decision variables \bar{w}_i . Both sub-problems are now provided, along with an illustration of the decomposition approach in Fig. 6.

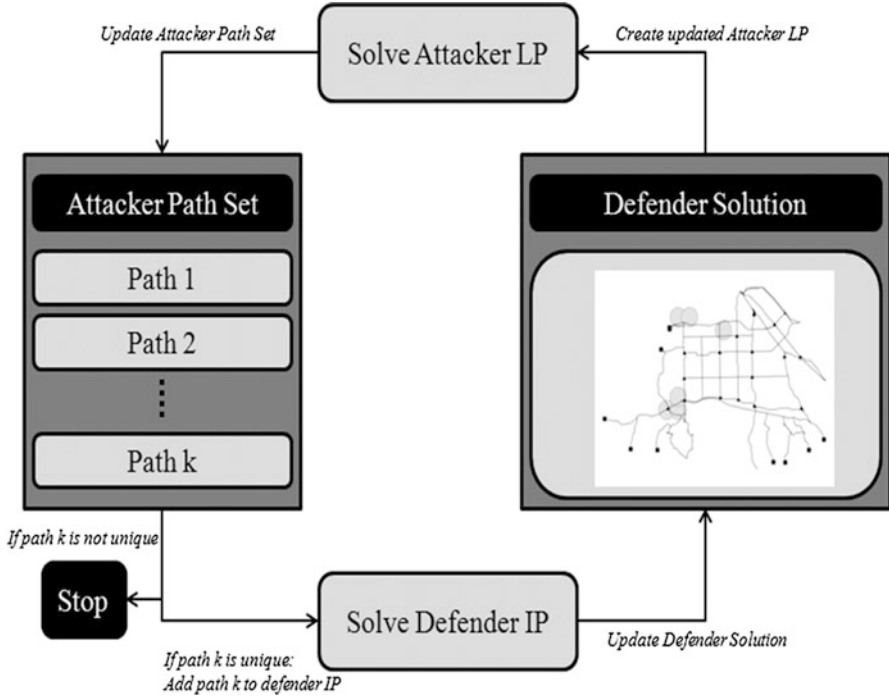


Fig. 6 Illustration of the Bender’s decomposition method (Yates and Casas 2010)

[Attacker Sub-Problem]

$$\begin{aligned}
 z^{att} &= \max \sum_{i,s,t} \log(u_{ist}) w_i \bar{x}_{ist} \\
 s.t. & \sum_i k_{ni} w_i \leq q_n \quad \forall n \\
 & w_i \in R^+
 \end{aligned}$$

[Defender Sub-Problem]

$$\begin{aligned}
 z^{def} &= \min V \\
 s.t. & x_{ist} - \frac{1}{T} \sum_a r_i^{as} y_{as} \leq 0 \quad \forall i, s, t \\
 & \sum_{i,s,t} x_{ist} = 1 \quad \forall i \\
 & \sum c_s y_{as} \leq B \\
 & \sum \log(u_{ist}) \bar{w}_i x_{ist} \leq V \\
 & y_{as}, x_{ist} \in Z^+
 \end{aligned}$$

As in Fig. 6, the technique iteratively solves the attacker and defender sub-problems, passing solution information sequentially. Within each iteration, the defender allocates its resources optimally considering only those attacker paths found through previous iteration. This optimal allocation is then used to update all arc non-detection probabilities and used to obtain the attacker’s path of maximum non-detection given the current resource allocation. If the path obtained by the attacker has already been considered in the constraint set (i.e. it has already been found in a previous iteration), an optimal defense resource allocation has been found

and the method stops. If the obtained path is not currently in the attacker path set, it is added and the defender sub-problem is solved again with the additional path considered. Bender's Decomposition yields provably optimal solutions and, in the worst-case, will iterate once for every unique, complete, simple path of the network (resulting in a worst-case performance of complete enumeration). In practice, Bender's Decomposition requires significantly less iterations to find the optimal resource allocation strategy.

Examining Network Interdiction Solutions

To assess interdiction solutions, we develop an experimental design that is used to examine two sub-networks of the Los Angeles County region. Multiple factors make up the experimental design, including road network and formulation type. Each identified factor has at least two test levels. Table 6 provides information pertaining to the initial experimental design and Fig. 7 illustrates the two test networks.

M-AST (Additive, Single Sensor Type)

M-NAST (Non-additive, Single Sensor Type)

M-NAMT (Non-additive, Multiple Sensor Types)

In Table 6, the parameter settings that define each of the six formulation levels are provided. The SPNIP-Length Based model has three distinct levels varying by sensor power (LB-1, LB-2 and LB-3). For SPNIP-M, three variations result. In M-NAST (Non-additive, Single Sensor Type), only a single sensor type is considered and no overlapping sensor coverage is allowed (i.e. $t=1$). In M-AST (Additive, Single Sensor Type), only a single sensor type is considered but overlapping coverage is allowed until a given threshold, beyond which additional sensor coverage will not reduce arc non-detection. In M-NAMT (Non-additive, Multiple Sensor Types), multiple sensor types with various costs and sensor power parameters are considered, however no overlapping coverage is allowed (i.e. $t=1$).

In Fig. 7, a uniform grid structure was used to establish the atom locations. The grid's scale is consistent for both Lancaster and Northridge, with these networks being chosen for experimental study due to their diversity in scale, complexity and density. Table 7 provides specific information on the network and atom sets for Lancaster and Northridge. Figure 8 illustrates the specific origin and critical infrastructure target locations for Lancaster and Northridge and Fig. 9 shows how arc influence is determined for SPNIP-M and SPNIP-LB on each network. U.S. Census Bureau classification (CFCC) was used to determine appropriate targets as follows (U.S. Census Bureau 2008). Green = {all regional airports}, Blue = {all regional airports and hospitals}, Yellow = {all regional airports, hospitals and police/fire stations}, Orange = {all regional airports, hospitals, police/fire stations and landmarks}, Red = {all regional airports, hospitals, police/fire stations, landmarks and schools/universities}. Note that any given target level includes all targets identified at preceding levels (i.e. all blue targets are included in the yellow target set). Origins were chosen randomly from the set of external/boundary nodes for each network.

Table 6 Experimental design factors, levels and problem parameters to evaluate SPNIP-M performance

Experimental design factors and levels			Parameter levels						
Level	Network	Destination	Budget	Formulation	Formulation	Sensor power, $\eta(0)$	Sensor power, $\eta(1)$	Sensor cost	Initial arc non-detection, $u(i 01)$
1	Lancaster	Red	\$800	M-AST	M-AST	1	0.5	\$200	Uniform [0.3,0.7]
2	Northridge	Orange	\$1,200	M-NAST	M-NAST	1	0.5	\$200	Uniform [0.3,0.7]
3		Yellow	\$1,600	LB-1	M-NAMT	1	Varies	Varies	Uniform [0.3,0.7]
4		Blue		LB-2	LB-1	0	2	\$200	Uniform [0.3,0.7]
5		Green		LB-3	LB-2	0	3	\$200	Uniform [0.3,0.7]
					LB-3	0	4	\$200	Uniform [0.3,0.7]

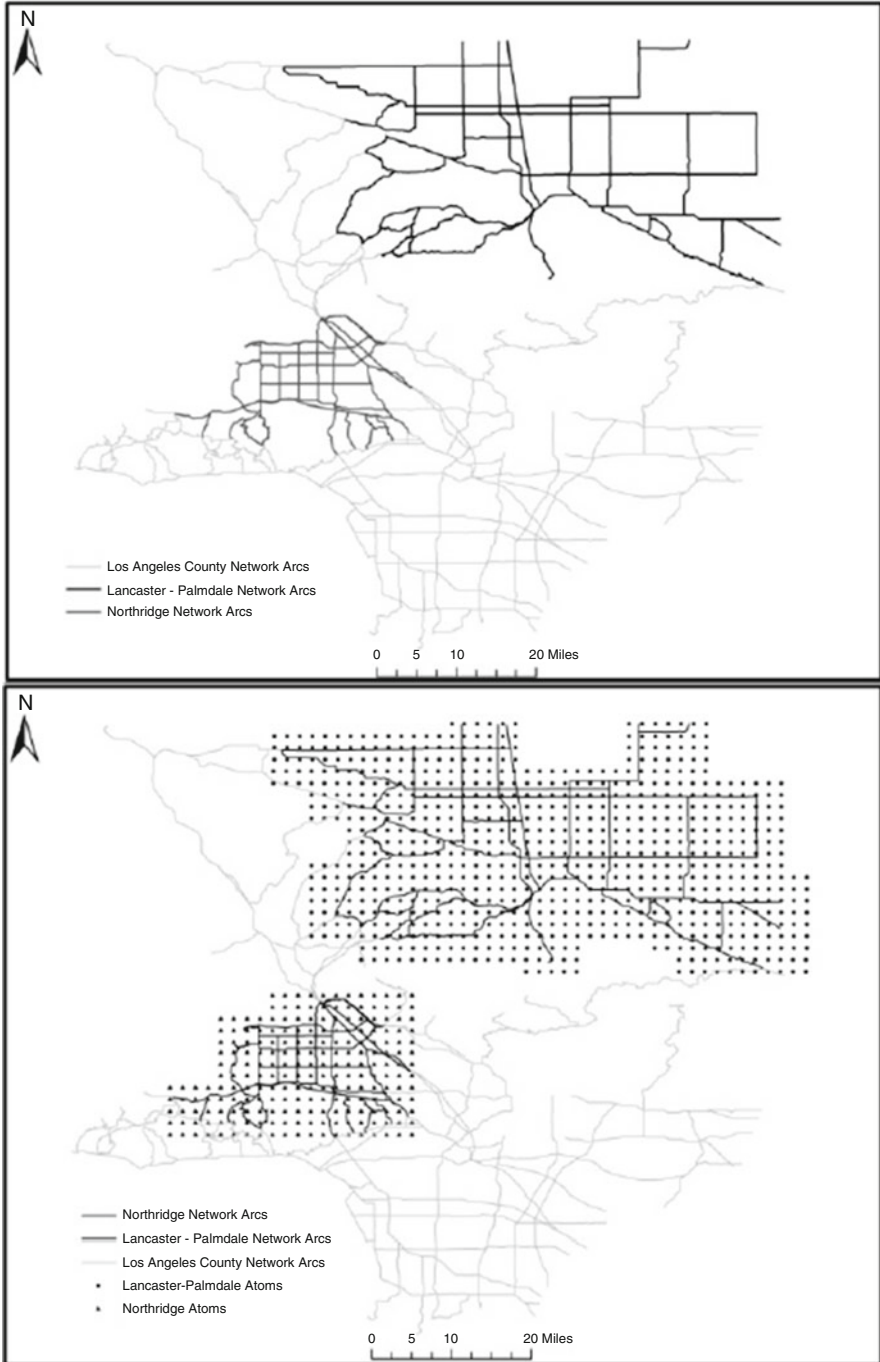


Fig. 7 Lancaster and Northridge test-case networks and their position within the Los Angeles County road network (Yates and Casas 2010)

Table 7 General regional and network data for Lancaster and Northridge

	Regional data			Road network data ^a				
	Area (sq. miles)	# Atoms	Atom density	Total	Density	Min	Max	Mean
Lancaster	1,295.61	743	0.57	465.61	0.36	0.12	14.51	4.47
Northridge	361.18	220	0.61	246.64	0.68	0.01	8.16	1.32

^aTotal, min, max and mean are measured in miles

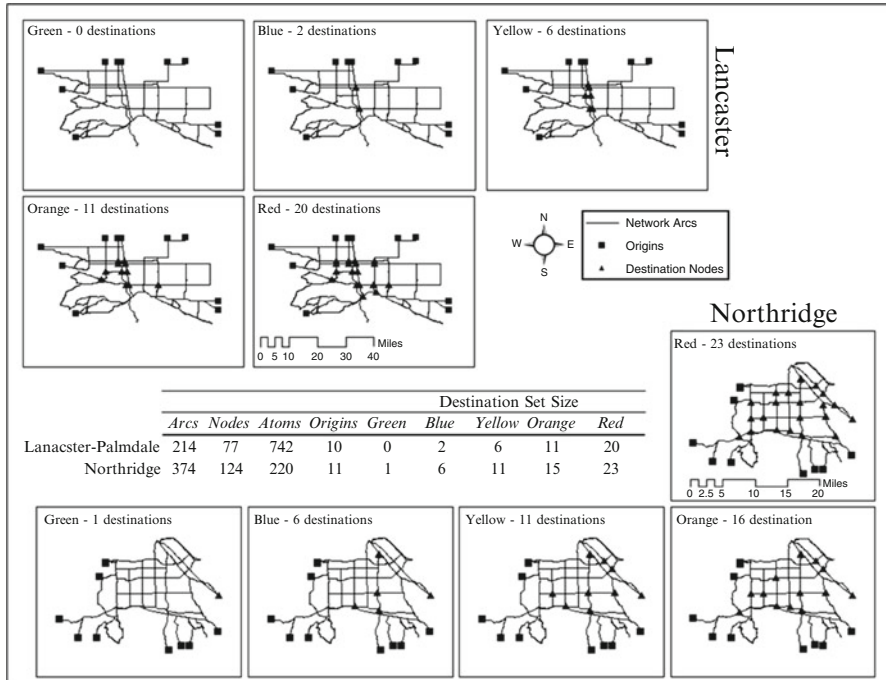


Fig. 8 Lancaster-Palmdale (top) and Northridge (bottom) network entry and CIKR target points at each identified threat level (Yates and Sanjeevi 2012)

Recalling that Benders Decomposition was used to solve for optimal SPNIP values, the resulting experimental design defined 30 individual problem instances for each of the six formulation levels (a total of 180 individual problem instances). Table 8 gives the aggregated results for five of the six formulation levels (M-NAMT is excluded as it is the only formulation which includes multiple sensor types). Tables 9 and 10 provide the individual run results for all SPNIP-M instances while Fig. 10 illustrates a typical SPNIP-M solution for the Northridge network.

In examining these solutions, we notice that, as expected, network and formulation choice directly impact objective value and computation time (significant differences are present across all formulation levels). Specifically, we begin to notice that SPNIP-M and SPNIP-LB performance is not monotonic. From Table 8, the results of the experimental design show that SPNIP-M is more efficient computationally in solving instances on the Lancaster network while SPNIP-LB is more efficient with respect to Northridge.

Table 8 Statistical summary of experimental results (Yates and Sanjeevi 2012)

	Lancaster				Northridge				Objective
	Average	Std dev.	Min	Max	Average	Std dev.	Min	Max	
SPNIP-M NAST	0.052	0.023	0.013	0.087	2.76E-02	0.024	5.30E-06	5.59E-02	Iterations
SPNIP-M AST	0.027	0.024	0.003	0.087	1.38E-02	0.019	5.19E-09	5.59E-02	
SPNIP-LB 1	0.004	0.009	1.17E-06	0.023	8.76E-04	0.002	5.36E-24	8.08E-03	
SPNIP-LB 2	0.004	0.009	2.21E-08	0.023	2.67E-04	0.001	7.10E-34	2.72E-03	
SPNIP-LB 3	0.004	0.009	2.80E-10	0.023	9.03E-05	2.43E-04	9.41E-44	9.18E-04	
SPNIP-M NAST	11	4.3485	6	18	17.2	11.3528	8	39	
SPNIP-M AST	15.25	3.7689	9	22	20.73	9.55784	5	35	
SPNIP-LB 1	14	4.4313	7	22	10	4.86973	2	19	
SPNIP-LB 2	14.67	6.3865	7	29	9.8	4.76895	2	17	
SPNIP-LB 3	14.75	5.7228	6	27	10.6	5.65433	2	21	
SPNIP-M NAST	N/A				N/A				Comp time
SPNIP-M AST	4.58	6.43	0.67	22.09	2,063.64	3,829.42	8.73	13,012.98	
SPNIP-LB 1	28.85	23.59	4.30	81.58	19.66	13.85	0.41	42.34	
SPNIP-LB 2	43.82	56.17	4.14	193.80	18.18	14.36	0.42	49.95	
SPNIP-LB 3	51.26	60.22	7.22	206.15	18.20	13.88	0.41	51.55	

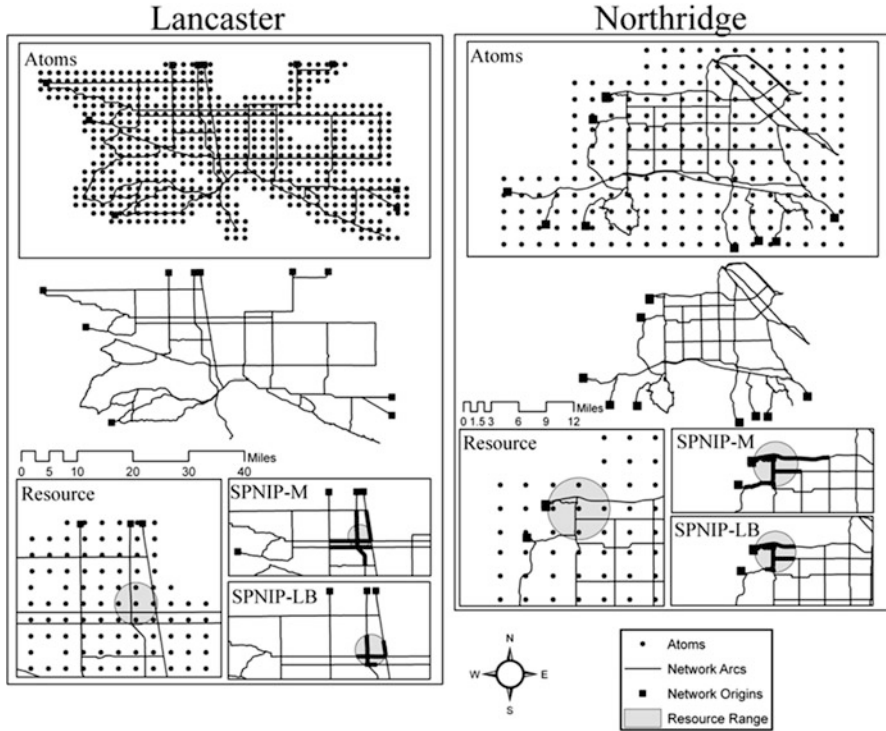


Fig. 9 Illustration of the network atom sets and a sample resource allocation (Yates and Sanjeevi 2012)

Extending SPNIP-LB

In SPNIP-LB, modification to the sensor model creates a simple function that enables the modeling of dynamic sensors. In contrast with the sensors used to this point, dynamic sensors are allocated to arcs within the network, repeatedly looping (i.e. covering) these arcs in similar fashion to a local law enforcement vehicle on patrol. The available dynamic sensor paths are finite and pre-determined and are represented by the set P . The collection of all sensor locations, which includes the set of atoms A for immobile or static sensors, is written as $C = A \cup P$.

Call t_i the amount of time spent traversing arc i of path p and t_p the total path traversal time for path p . A uniform distribution determines the probability that the sensor is present on arc i . The definition in (5), we can calculate the probability of non-detection for arc i under the influence of mobile sensor c as in (6)

$$P(T_{ip}) = \frac{t_i}{t_p} \tag{5}$$

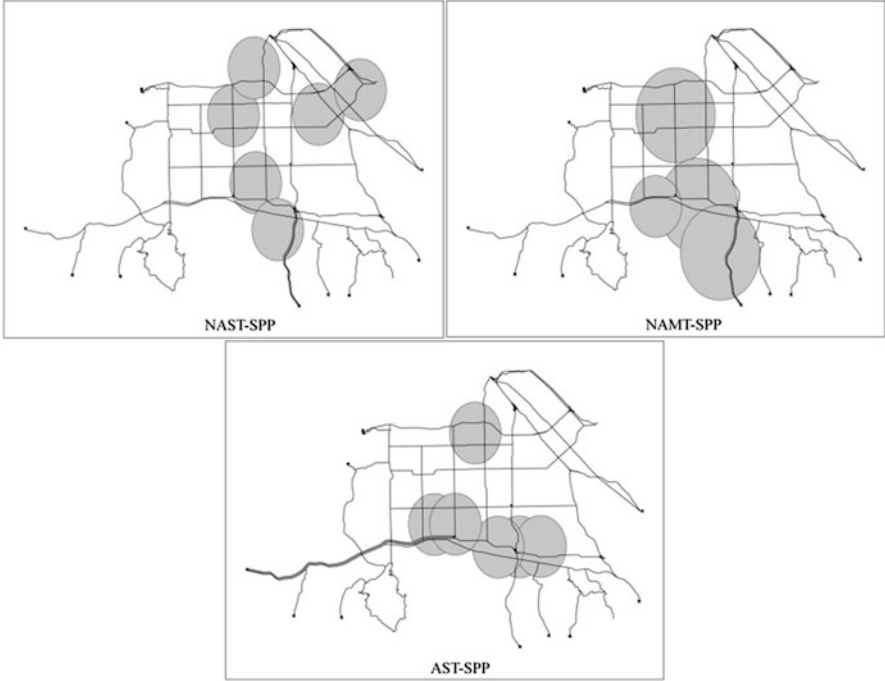


Fig. 10 Illustration of representative sensor placement results (Northridge shown)

$P(ND_{cip}|T_{ip})$ is the probability of non-detection for arc i covered by sensor located on path $p \in C$ (note that if path p contains the single arc i , then $t_i = t_p$ and $P(ND_{cip}, T_{ip})$ equals the static sensor detection rate).

$$P(ND_{cip}|T_{ip}) = e^{-\eta l_{ic}}$$

$$\begin{aligned} P(ND_{cip}, T_{ip}) &= P(ND_{cip}|T_{ip})P(T_{ip}) \\ &= e^{-\eta l_{ic}} \frac{t_i}{t_p} \\ &= u_{ic} \quad \forall c \in P \end{aligned} \tag{6}$$

$P(ND_{cip}|T_{ip})$ is the probability of non-detection for arc i covered by sensor located on path $p \in C$ (note that if path p contains the single arc i , then $t_i = t_p$ and $P(ND_{cip}, T_{ip})$ equals the static sensor detection rate. Also, dynamic sensors are assumed to have an influence range of 1.5 miles such that a 0.5 mile arc would have $l_{ic} = 0.5$ while a 2.4 mile arc would have $l_{ic} = 1.5$). Figure 11 illustrates an adaptation of the Northridge network to include six dynamic/mobilesensor paths in

Table 10 Number of paths used at all threat levels for the Lancaster and Northridge test networks (number of paths represents the number of Bender's Decomposition iterations necessary to obtain an optimal solution)

	Green	Blue	Yellow	Orange	Red										
Lancaster	NAST	12	17	10	7	6	9	15	14						
	NAMT	16	16	19	10	9	10	7	10	8	12	16	14		
	AST	11	15	22	13	15	18	11	15	18	9	18	18		
Northridge	NAST	38	39	9	9	18	16	12	8	8	13	13	12		
	NAMT	36	34	32	8	9	10	24	22	18	9	9	12	11	
	AST	21	30	33	16	19	32	15	32	35	5	12	18	8	15
Budget	\$800	\$1,200	\$1,600	\$800	\$1,200	\$1,600	\$800	\$1,200	\$1,600	\$800	\$1,200	\$1,600	\$800	\$1,200	\$1,600

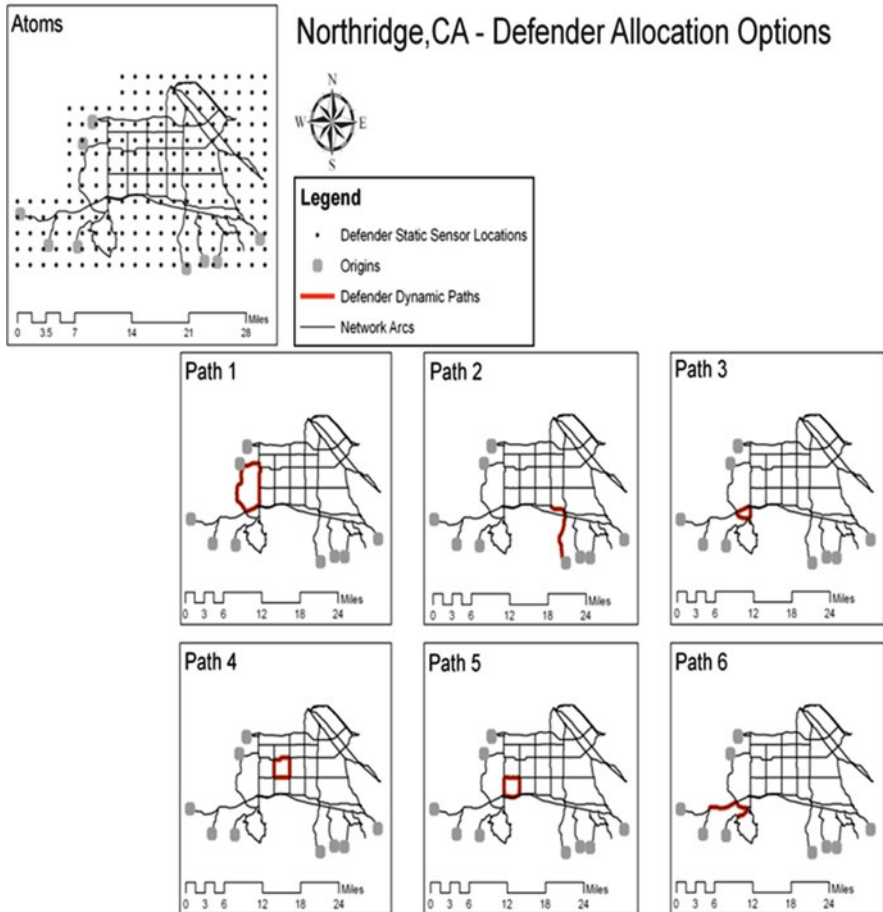


Fig. 11 Static and dynamic sensor locations for Northridge, CA (Yates and Sanjeevi unpublished)

addition to the static atom locations for the SPNIP-LB formulation. Figure 12 and Table 11 provide solution results after running several instances of SPNIP-LB with dynamic sensors.

Analyzing the Spatial Properties of SPNIP-M and SPNIP-LB Solutions

We use ArcGIS 10 to perform common spatial analysis techniques such as clustering and autocorrelation on the SPNIP-M and SPNIP-LB solutions. We note that much exists in the analysis of global and local clustering measures (local indicators of

Fig. 12 Sample SPNIP-LB solution: “Level 4 Threat” with $\eta = 2$; (a) $B = \$800$ (b) $B = \$1,600$ (Yates and Sanjeevi unpublished)

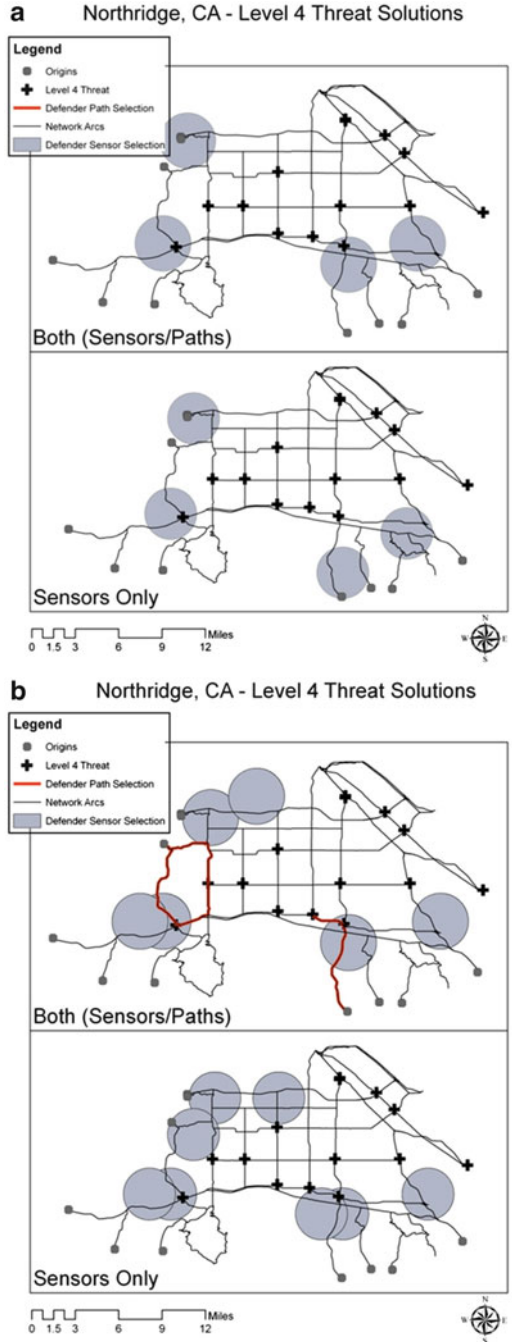


Table 11 Atom and path allocations for level 4 threat (Yates and Sanjeevi unpublished)

Allocation type	Budget	Atom usage					Path usage				
Sensors only	\$800	52	131	159	167						
	\$1,600	20	62	131	134	154	172	186	201		
Both	\$800	52	117	131	172						
	\$1,600	20	35	131	154	172	201			1	2

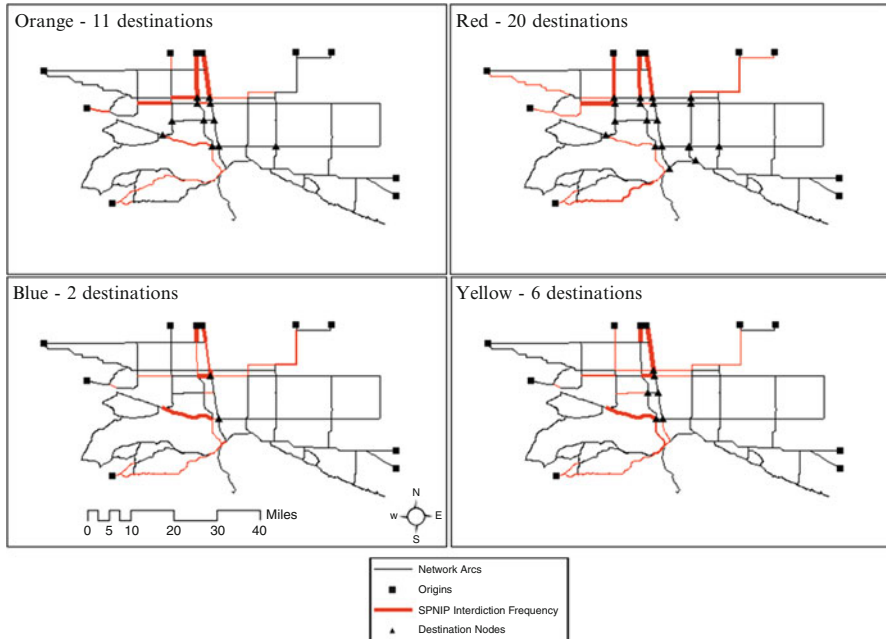


Fig. 13 Map of aggregate Lancaster SPNIP results at each destination level (Yates and Sanjeevi 2012)

spatial autocorrelation, LISA) on a network (Anselin 1995; Yamada and Thill 2010). With SPNIP-M and SPNIP-LB, there is an arc influence decision variable (x_{ist} and x_{ias} respectively) in addition to a variable indicating a sensor’s location at an atom (y_{as} in both models). While atom locations have a regular spatial pattern (to this point, all atom locations have been grid-structured), their independence from the road network itself enables the application LISA measures.

Figures 13 and 14 illustrate the aggregate results of solving a traditional arc-based SPNIP model such as Israeli and Wood (2002) and the aggregate atom solutions across all previously defined factor levels for SPNIP-M and SPNIP-LB in Lancaster and Northridge respectively.

Kernel density and map algebra techniques were implemented in an effort to better understand the observed similarity between the aggregated models of Figs. 13 and 14 (see ESRI 2009) for discussion on kernel density and map algebra). At a high

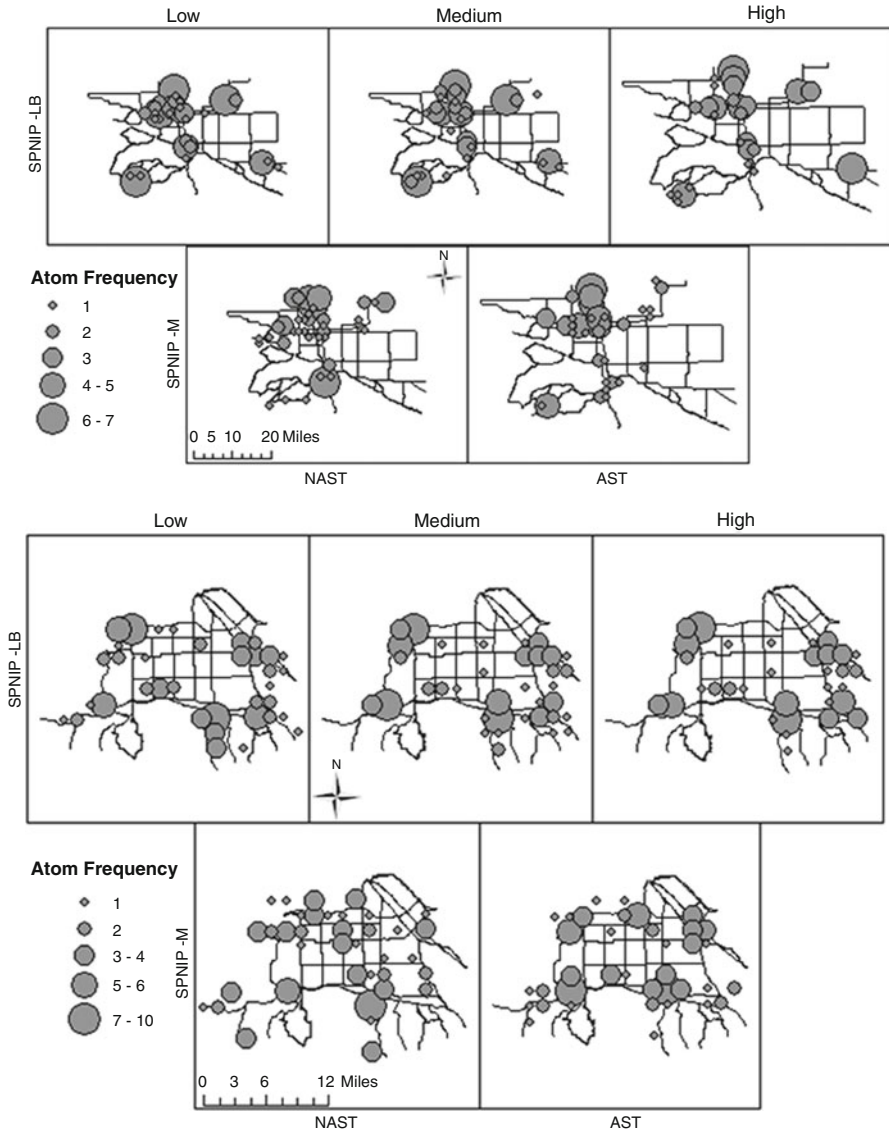


Fig. 14 Map of atom frequency in Lancaster-Palmdale (left) and Northridge (right) (Yates and Sanjeevi 2012)

level, kernel density is used to create a continuous-space image from the discrete atom frequencies that are obtained when SPNIP-M and SPNIP-LB solutions are aggregated. The continuous kernel density image is akin to a pixilated image and is different from the individual discrete point-based atom locations (all pixels are given a value through implementation of the kernel density and atom frequencies

are “smoothed” through the continuous space occupied by the atoms). Map algebra techniques are used to perform calculations on one or multiple continuous kernel density files. We use map algebra techniques here to define similarity metrics for the obtained kernel densities. Figure 15 illustrates the obtained kernel densities from the atom frequencies of Fig. 14.

We define two measures for comparing aggregated solutions. The first, Less-Than-Or-Equal-To (LessEQ), returns the percentage of individual pixels for kernel density input A that are less than or equal to the individual pixels for kernel density input B. The second, Equal-To (EQ), only returns the percentage of pixels for input A and input B that are identical. Both LessEQ and EQ are used to evaluate the similarity in aggregate coverage between SPNIP-M and SPNIP-LB. Table 12 provides the obtained similarity results using the kernel densities from Fig. 15 and the two raster similarity measures.

The motivation for this analysis stems from discussion in the previous section where the computational performance of SPNIP-M was more efficient in Lancaster than in Northridge. If it can be shown that results from the two formulations are similar, then they may be used interchangeably. This would provide flexibility for the modeler to choose or continue to use formulations exhibiting efficient performance. Additionally, such information on similarity can be useful in the development of approximation techniques to reformulate and solve interdiction problems (as will be discussed in the next section). In the case of Table 12, LB-3 exhibits strong similarity with M-NAST and M-AST, especially in Lancaster where average equality is between 63 and 70 %. Similarly, LessEQ demonstrates that both M-NAST and M-AST are capable of meeting or exceeding LB coverage in 85 % of the experimental runs.

Developing Interdiction Approximations and Heuristics

The previous section highlighted the computational performance and spatial characteristics of certain shortest path network interdiction problem variants. Though the aforementioned represents a small subsection of interdiction formulations, there were inherent trade-offs in computational performance across different formulations. A knowledgeable modeler or public policy maker could use these trade-offs to more effectively obtain information on the region and critical infrastructure being examined. While such gains would be beneficial to the modeler, the spatial similarities in solution characteristics support the assertion that there are inherent solution properties that may be replicable or decipherable either through alternative, approximate formulations or new solution techniques. This section is devoted to examining how the shortest path network interdiction problem can be re-modeled and re-evaluated for the purposes of developing faster, stronger approximation and solution techniques. We will begin by discussing a knapsack approximation to the SPNIP-M problem of the previous section. After the approximation is introduced, we will

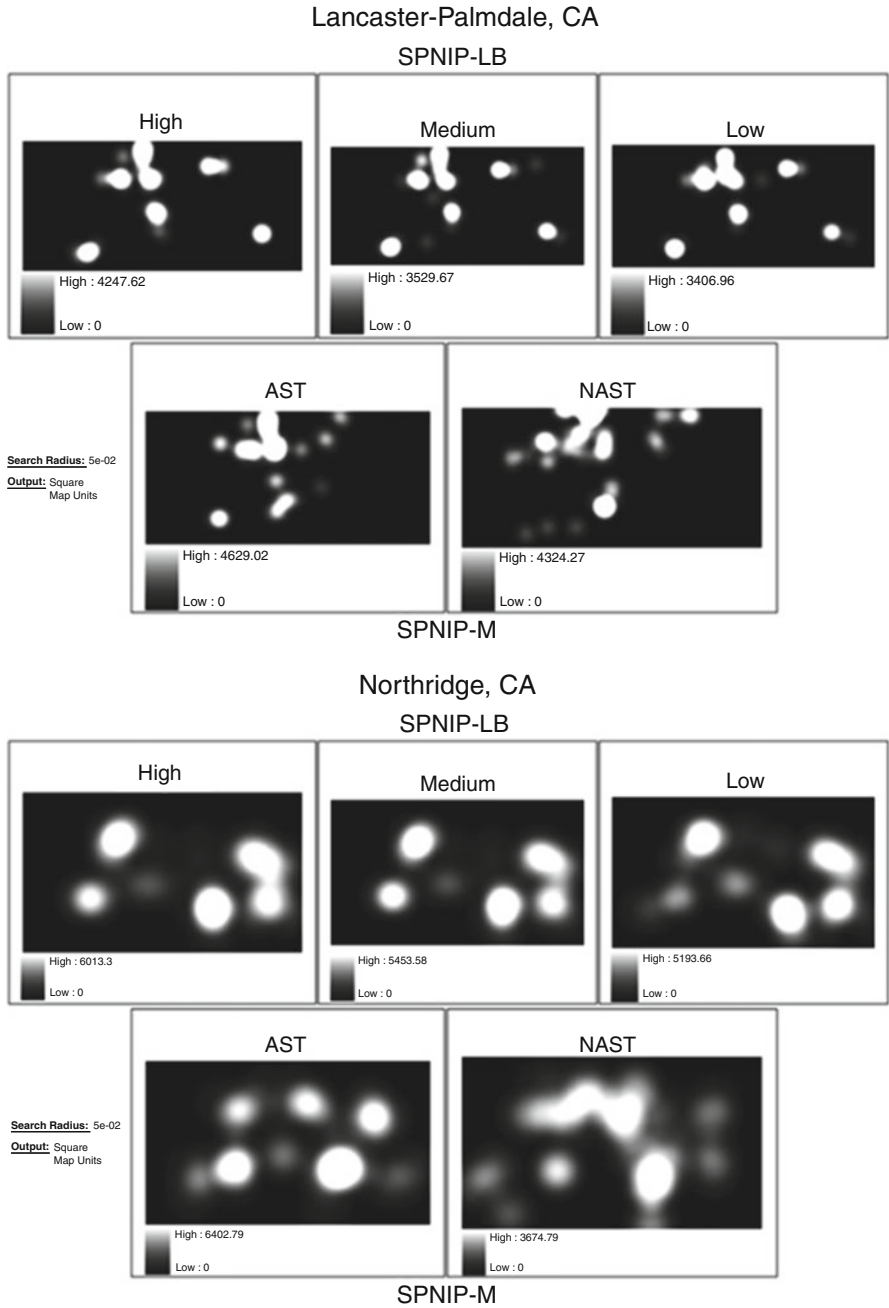


Fig. 15 Kernel density obtained from aggregate atom frequencies (Yates and Sanjeevi 2012)

Table 12 Spatial similarity of formulation results

First entry	Second entry	Raster	Lancaster		Northridge	
			Mean	Std dev.	Mean	Std dev.
LB-3	M-NAST	LessEQ	0.858	0.349	0.648	0.478
LB-3	M-AST	LessEQ	0.887	0.317	0.683	0.465
LB-1	M-NAST	LessEQ	0.838	0.369	0.630	0.483
LB-1	M-AST	LessEQ	0.859	0.348	0.601	0.490
LB-2	M-NAST	LessEQ	0.826	0.379	0.636	0.481
LB-2	M-AST	LessEQ	0.836	0.370	0.665	0.472
LB-3	M-NAST	EQ	0.665	0.472	0.168	0.374
LB-3	M-AST	EQ	0.705	0.456	0.224	0.417
LB-1	M-NAST	EQ	0.640	0.480	0.156	0.362
LB-1	M-AST	EQ	0.685	0.465	0.194	0.396
LB-2	M-NAST	EQ	0.629	0.483	0.151	0.364
LB-2	M-AST	EQ	0.658	0.474	0.212	0.409

examine ways to increase the performance of Bender’s Decomposition and conclude with provocation of a new, heuristic approach to solving interdiction problems.

A Knapsack Approximation

Within an interdiction problem, the primary concern of the defender is to identify arcs and/or nodes that are most critical to the protection of critical infrastructure and protect, reinforce, or otherwise deter an attacker from using those arcs. The Bender’s Decomposition approach to solving interdiction models is essentially an iterative approach that uses an attacker-based sub-problem to build a set of likely attacker paths through the network. These attacker paths contain what can be considered the critical arcs. Severing or preventing the attacker from using these critical arcs by allocating regional resources is the primary defender concern.

Identifying critical, vulnerable, or salient network arcs is not a new problem. Many approaches use a cut-set mentality to identify arcs whose absence will cut off or extremely inhibit flow between origins and destinations. A classic application of such an approach is given in Matisziw et al. (2007). Many interdiction models, especially those in early hazardous materials literature, are predicated on the maximum flow-minimum cut paradigm, using a minimum cut as the primary method to identify critical network arcs. The following list contains such max flow-min cut incorporated models: Burch et al. (2003), Corley and Chang (1974), Cunningham (1985), Ghare et al. (1971), Phillips (1993), Ratliff et al. (1975), Wollmer (1964), and Wood (2003).

The approximation technique discussed here is essentially a constrained knapsack optimization problem that identifies the attacker's critical network arcs, again relying on the max flow-min cut property as its foundation. The major premise of the approximation is to consider minimum capacity cuts in the network as a means to identify likely attacker critical arcs. In doing so, the following lemma guides the approximation (the proof for this lemma is by contradiction and may be found in Yates and Lakshmanan (2011)). The knapsack approximation formulation [KNAP] follows the lemma.

Lemma *For any given network $G(N, \Lambda)$ having probability of non-detection as its flow metric, the maximum flow in any path is an upper bound on the total path non-detection probability.*

$$\begin{aligned}
 & z^* = \max \sum_b \varphi_b v_b && \text{[KNAP]} \\
 & \text{s.t. } \sum_b c_1 v_b \leq B && \varphi_b = \sum_{j \in R^{bl}} \left(\alpha m_j + \frac{1-\alpha}{p_j} \right) \\
 & \sum_{b \in \phi^j} v_b \leq \tau \quad \forall j \in \Lambda \\
 & v \in \{0, 1\}
 \end{aligned}$$

z^* is the weighted objective utility for KNAP and contains two components. The first, m_j , is the aggregated maximum flow for arc j considering all origin and critical infrastructure pairs. The second, $\frac{1}{p_j}$ is the inverse of the node count between arc j and its closest origin. α Determines the emphasis placed on the objective with the goal of KNAP to locate sensor resources at atoms of the network such that z^* is maximized. In addition to the standard knapsack budgetary constraint, KNAP also constrains the amount of tolerable sensor overlap within a sensor allocation scheme in the same way that DSPNI used the subscript index t to control the degree to which sensor overlap was counted when calculating z .

When examining solutions to the knapsack approximation, it is import to note that only defender allocation schemes are determined under this method (i.e. no attacker path information is provided). As a method for defender's to gain useful information on situational awareness, the knapsack approximation provides a fast and reliable approximation to defender sensor location. Figures 16 and 17 and in Table 13 provide computational results of the knapsack and SPNIP-M formulation solutions on the Lancaster and Northridge networks and using the same experimental design discussed in the previous section. In Figs. 16 and 17, z is the optimal objective value for SPNIP-M and z' is the objective value obtained when the KNAP sensor solution is evaluated for the SPNIP-M objective. Also in the figures, KNAP parameters were set at $B = \$3,600$, $\alpha = 0.02$ and $\tau = 3$.

Comparing the computational results of the knapsack approximation illuminates a few important trends. First, the approximation reliably captures the form of the SPNIP-M objective function through a simple approximation based on a well-

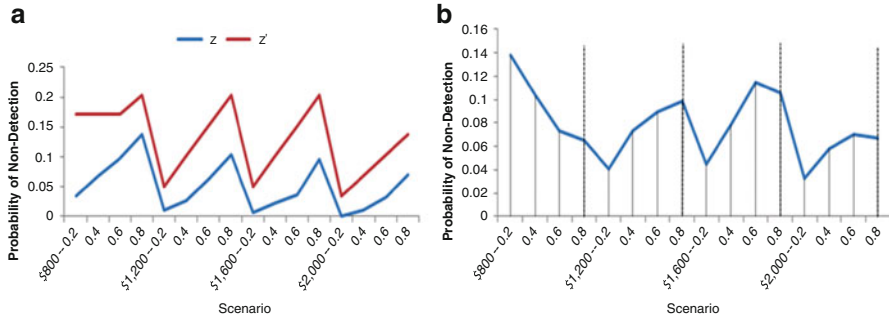


Fig. 16 Lancaster-Palmdale, random initial non-detection probability (Yates and Lakshmanan 2011)

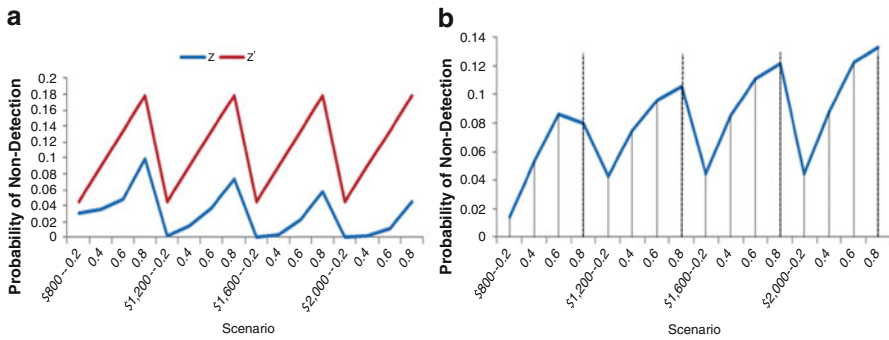


Fig. 17 Northridge, random initial non-detection probability (Yates and Lakshmanan 2011)

known and understood optimization principle, in this case maximum flow-minimum cut. Second, the approximation demonstrates insensitivity to network choice. Third, the approximation demonstrates computational insensitivity to changes in SPNIP-M problem parameters. Computationally, the knapsack approximation performs well for the cases examined and appears to be a well suited alternative to model defender sensor location in SPNIP-M. We now introduce and discuss the knapsack’s ability to spatially approximate SPNIP-M solutions. To do this, the same spatial analysis techniques (kernel density and map algebra) were applied as in the previous section. Figure 18 illustrates the obtained kernel densities while Table 14 gives the LessEQ and EQ values.

The approximation’s spatial performance is promising, though not as strong as its computational capabilities. With roughly 75 % similarity to the SPNIP-M solution, the approximation performs well in Lancaster and appears to increase its performance as overlap (τ) increases. While the approximation does not perform as well in Northridge, only a small number of possible parameter combinations are provided in Table 14 and it is highly probable that the knapsack approximation could be strengthened through a more comprehensive pareto analysis.

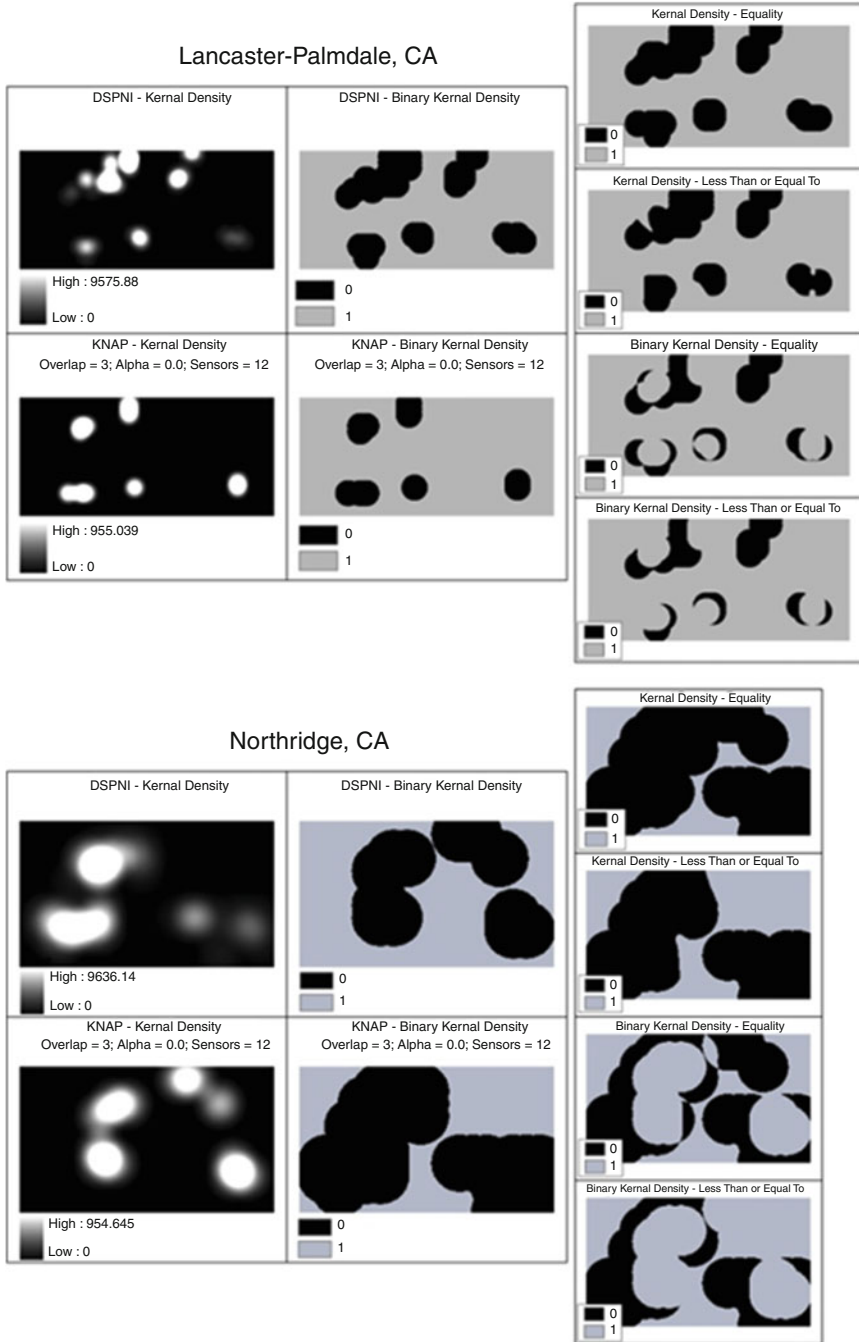


Fig. 18 Kernel and binary kernel density and comparison for the Lancaster-Palmdale and Northridge case study regions (Yates and Lakshmanan 2011)

Table 14 EQ and LessEQ similarity values for Lancaster and Northridge under varying K NAP parameters

	Overlap	Type	Alpha = 0.0		Alpha = 0.50		Alpha = 1.0	
			Mean	Std dev.	Mean	Std dev.	Mean	Std dev.
Lancaster	1	EQ	0.684	0.465	0.667	0.471	0.664	0.472
		LessEQ	0.762	0.426	0.759	0.428	0.761	0.426
	2	EQ	0.740	0.439	0.710	0.454	0.710	0.454
		LessEQ	0.758	0.428	0.760	0.427	0.761	0.426
	3	EQ	0.738	0.440	0.701	0.458	0.701	0.458
		LessEQ	0.764	0.425	0.759	0.428	0.760	0.427
	4	EQ	0.742	0.437	0.724	0.447	0.703	0.457
		LessEQ	0.764	0.425	0.761	0.426	0.762	0.426
Northridge	1	EQ	0.182	0.386	0.187	0.390	0.187	0.390
		LessEQ	0.429	0.495	0.434	0.496	0.429	0.495
	2	EQ	0.208	0.406	0.227	0.419	0.227	0.419
		LessEQ	0.399	0.490	0.408	0.492	0.408	0.492
	3	EQ	0.248	0.432	0.217	0.412	0.217	0.412
		LessEQ	0.381	0.486	0.393	0.489	0.393	0.489
	4	EQ	0.248	0.432	0.221	0.415	0.221	0.415
		LessEQ	0.384	0.486	0.399	0.490	0.399	0.490

The knapsack approximation demonstrates how an entirely new formulation can be developed to take advantage of the unique structure of the network interdiction problem. With a relatively simplistic formulation capable of being solved efficiently, close approximations to the SPNIP-M formulation’s optimal solutions were obtained with significantly less computational effort. The next section will discuss how a similarly simple idea can be used to eliminate costly Bender’s Decomposition iterations in solving SPNIP-M.

Approximating with k-Shortest Paths

In lieu of redefining a new optimization problem for network interdiction or reformulating an existing one, this section will discuss the benefits of modifying the interdiction solution approach. For this discussion, the same basic experimental design introduced in section “[Formulating Interdiction Models](#)” will be used and applied to the Northridge network. Recalling that SPNIP-M is solved by implementing Bender’s Decomposition, the iterative attacker-defender sub-problem format is revised in an effort to decrease overall computation time. Additionally, this work nicely complements the knapsack approximation approach by enabling modelers a quick and easy approach to obtaining quality attacker paths (recall that the knapsack approximation only provided defender resource allocation solutions. [Figure 19](#) illustrates the original Bender’s Decomposition structure and the suggested revision to be examined here.

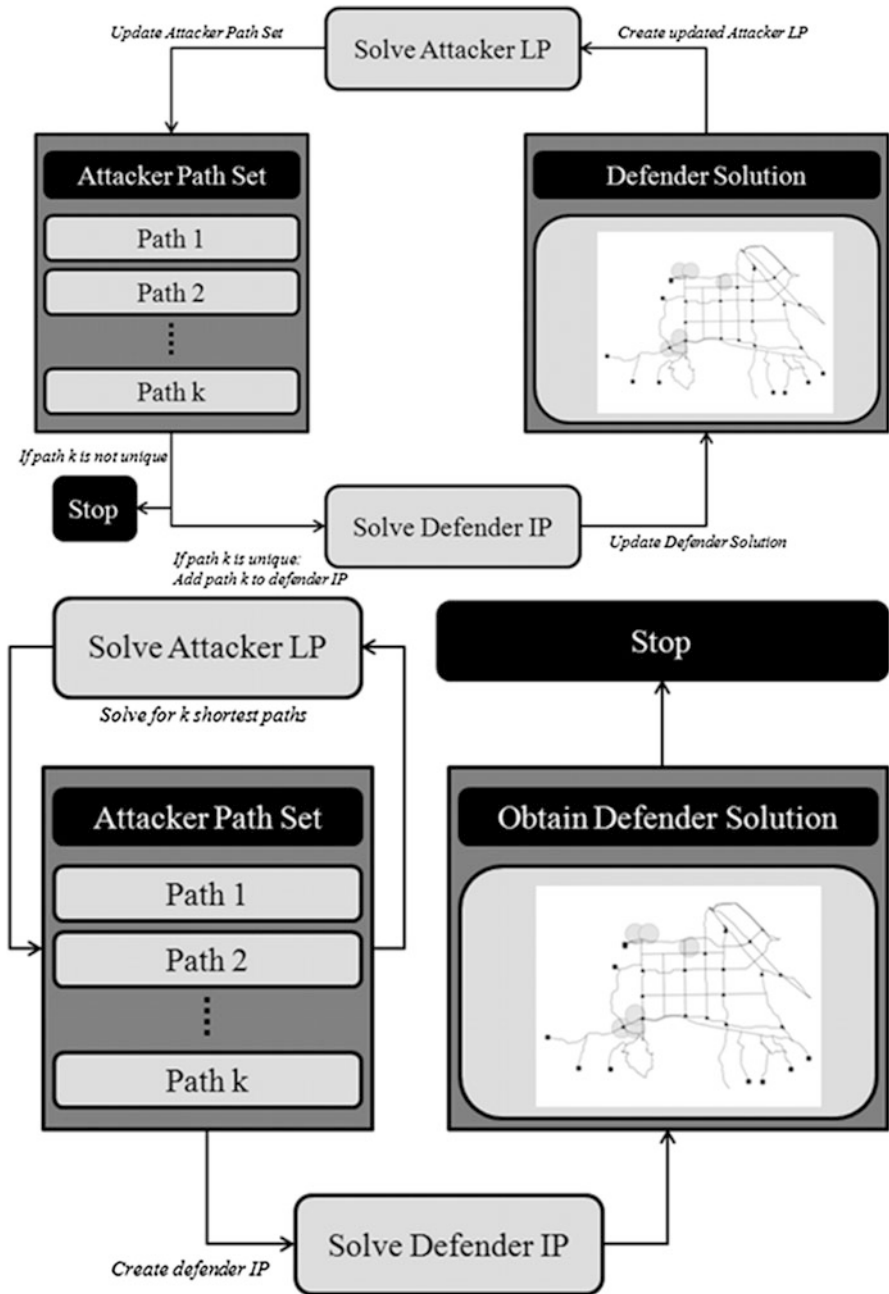


Fig. 19 Illustration of the original and modified Bender's decomposition (Yates et al. in submission)

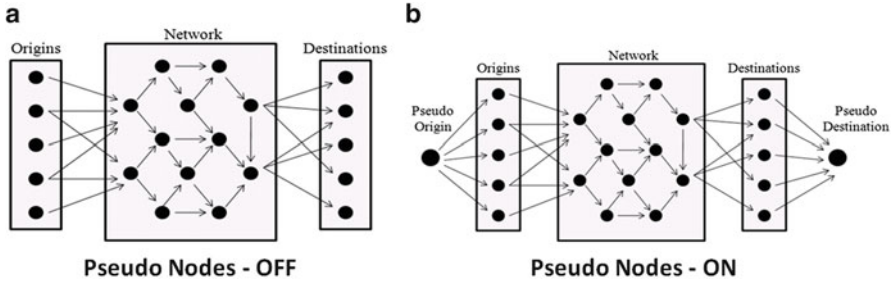


Fig. 20 Illustration of the exclusion and inclusion of pseudo nodes to solve for the k -shortest paths (Yates et al. in submission)

The traditional Bender’s Decomposition approach decomposes the SPNIP-M into attacker and defender sub-problems which are then iteratively solved until an equilibrium point has been reached, signifying an optimal solution. In this approach, the defender sub-problem is a complex mixed integer problem that accounts for a majority of the computational effort. In the revised method, it is surmised that gains in computational performance can be achieved by solving the defender problem only once instead of iteratively and repeatedly. In Fig. 19, this method is illustrated on the right-hand-side, where the attacker sub-problem is looped, essentially solving a k -Shortest path problem to identify the k paths of high non-detection given the initial, random arc non-detection metrics (see Yen 1971) for discussion on the k shortest path problem). Each of the individual k paths then becomes a constraint in the defender sub-problem of SPNIP-M and the defender sub-problem is solved once to determine an acceptable defense allocation. At its core, this approach essentially asks “what is the appropriate k value to capture the optimal attacker path in SPNIP-M?”

To assert whether there is an acceptable k value, a modified experimental design approach was developed. First, a global origin and target set were identified within Northridge. Four levels were used to dictate the origin set size [2,4,6,8] and target set size [3,9,15,21], within which five random origin and destination sets were generated. When calculating the k shortest paths, pseudo nodes were either included or not included, resulting in two additional experimental levels (Fig. 20 illustrates these two levels). Lastly, the value of k was set to [1,2,3,5] when pseudo nodes were off and [5,10,15,20] when pseudo nodes were on. In the Northridge network, initial arc non-detection values were assigned randomly using a *Uniform*[0.3, 0.7] distribution.

To analyze and compare the solutions obtained using the k -Shortest approach with the SPNIP-M optimal, *Gap V%*, *Gap T%*, *% Under* and *% Over* are used. *Gap V%* is the percentage difference in the k -Shortest solution from the SPNIP-M optimal while *Gap T%* measures the difference in computational time (in CPU seconds). *% Under* and *% Over* are spatial metrics to assess coverage similarity as a function of length-of arc covered and are aggregated over all network arcs

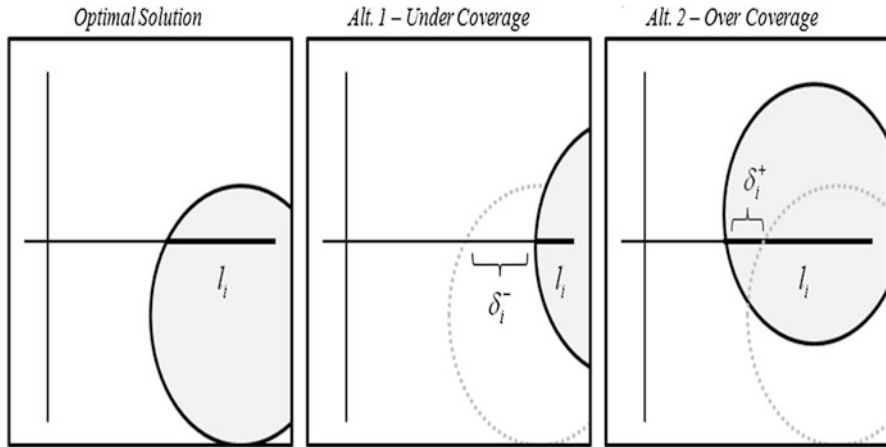


Fig. 21 Illustration of under coverage and over coverage in the calculation of % Under and % Over (Yates et al. in submission)

for a given experimental run. In this way, the k -Shortest path solution may either exactly replicate SPNIP-M arc coverage, under-cover and arc, or over-cover an arc. Figure 21 illustrates the later two cases. Table 15 provides information on the comparative performance of the k -Shortest path approach.

Table 15 provides the obtained averages from the five random experimental instances at each origin-target level. From the table, there are observable benefits in adapting traditional Bender’s Decomposition with a k -Shortest path approach. First, the k -Shortest approach identified the optimal SPNIP-M solution in at least one of the five random replications at each origin-target level (as indicated in Table 15 by a minimum *Gap V%* of “-”). In all but two levels, computational effort was also saved. Spatially, the ability of the k -Shortest approach to identify optimal SPNIP-M solutions is acceptable (~5 % under coverage with pseudo nodes off and 15 % with pseudo nodes on). Over coverage is relatively consistent in cases, with an average of 5 %.

Figure 22 visualizes two select, comparative cases between the optimal SPNIP-M solution and the obtained solution based on the k -Shortest path approach. In the figure, the left-hand case demonstrates an instance of strong computational and spatial coverage. In this case, the optimal SPNIP-M solution was obtained through the k -Shortest approach with a 23 % time savings. The right-hand case, however, illustrates a scenario where k -Shortest fails to perform. With 33 % under coverage and a 45 % optimality gap, the SPNIP-M optimal solution was not well approximated. The latter case signifies that the choice of k , in this case $k = 5$, was not high enough to adequately capture any attacker path trends.

The simplicity of this k -Shortest approach can be a huge advantage in decision-making and public policy, where modelers would desire the ability to test large numbers of scenarios and network compositions repeatedly. Though the Northridge

Table 15 Summary statistics of computational performance for the k-shortest approximation

Level	Gap V%				Gap T%				% Under				% Over			
	Avg.	Std dev.	Min	Max	Avg.	Std dev.	Min	Max	Avg.	Std dev.	Min	Max	Avg.	Std dev.	Min	Max
Off 1	1.788	3.530	-	9.569	65.108	42.575	-90.960	93.764	0.087	0.097	-	0.308	0.023	0.030	-	0.131
2	1.229	3.270	-	14.183	8.597	64.795	-124.812	79.724	0.039	0.040	-	0.127	0.020	0.025	-	0.089
3	-	-	-	0.000	-208.038	272.568	-960.824	47.464	0.055	0.059	-	0.204	0.048	0.045	-	0.145
4	-	-	-	0.000	-443.798	461.330	-1,391.150	7.908	0.082	0.088	-	0.245	0.023	0.021	-	0.058
On 1	8.742	12.537	-	31.360	38.907	53.681	-136.874	92.306	0.179	0.221	-	0.573	0.040	0.042	-	0.131
2	26.488	27.271	-	68.591	65.623	22.462	21.882	94.724	0.221	0.214	-	0.651	0.033	0.024	-	0.081
3	23.017	31.230	-	97.515	43.124	42.471	-65.230	93.829	0.098	0.095	-	0.327	0.053	0.066	-	0.253
4	26.034	33.593	-	143.604	51.555	33.229	-9.090	94.241	0.140	0.130	-	0.522	0.047	0.038	-	0.111

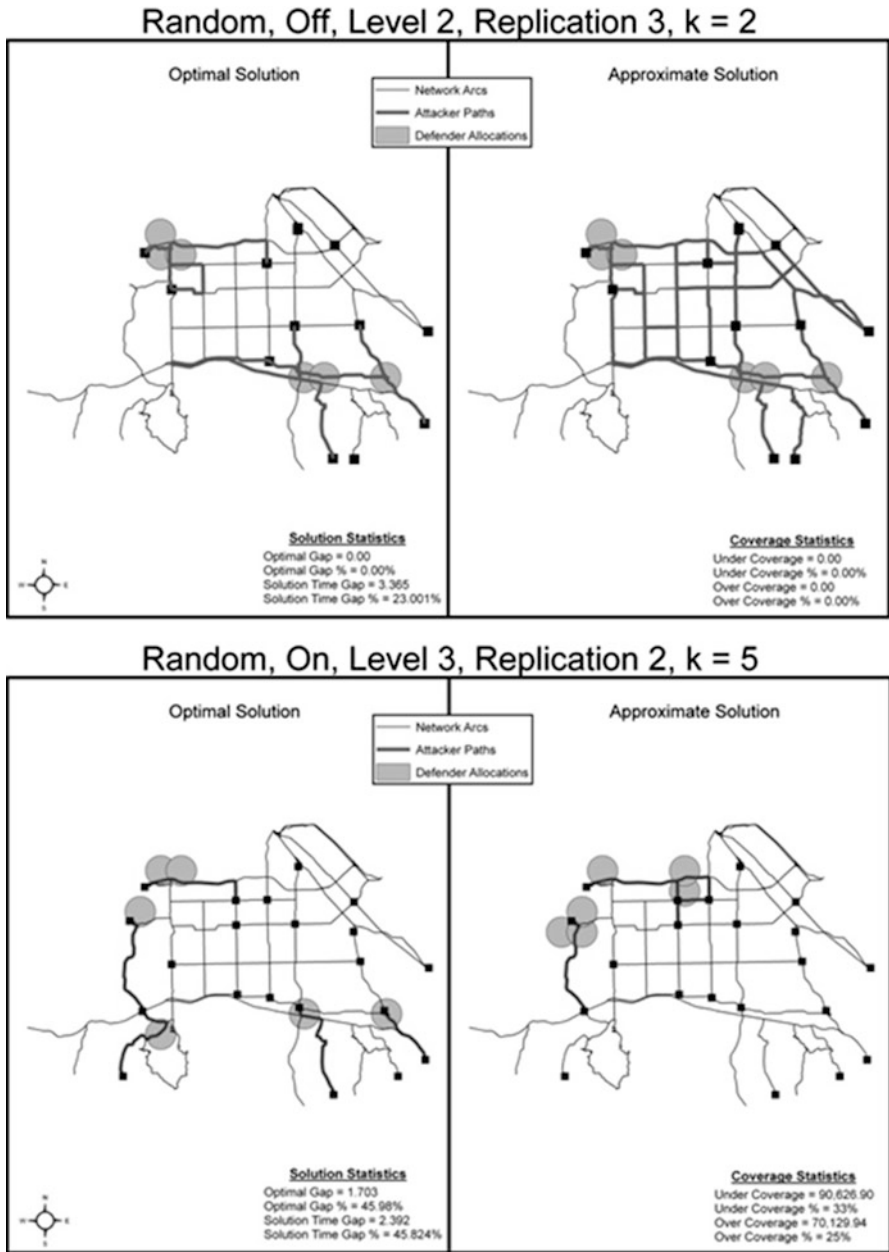


Fig. 22 Example of poor spatial performance by the approximation (Yates et al. in submission)

case is decidedly small, the SPNIP-M formulation grows exponentially with the size of a network. In Northridge (384 directed arcs), SPNIP-M was formulated with 3,437 constraints while a network of 1,000 directed arcs and 500 nodes produces 8,869 SPNIP-M constraints. Increasing network size by a factor of 10, a 100,000 direct arc network with 1,000 nodes has nearly 100 times the number of SPNIP-M constraints at 801,369. Using the entire Los Angeles County road network (U.S. Census Bureau 2008) easily leads to 2,000,000+ constraints. While the complexity of these problems may lead to elongated solution times and the necessity to include more advanced and strategic computational techniques, known k -shortest path algorithms enable this simple solution approach to handle problems of realistic scale without significant alteration. Stated previously, such a tool would be invaluable to emergency planners, responders and public policy makers alike when analyzing network performance/vulnerability/accessibility as they could test a plethora of event scenarios.

Additionally, the k -shortest approximation approach preserved much of the spatial integrity of SPNIP-M solutions (i.e. small under and over coverage measures), implying that this simple approximation approach could be used as a capable technique for other modified shortest path network interdiction models. As an example, the under and over coverage values indicate that quality SPNIP-LB solutions, where arc length was used directly in the determination of non-detection probability (Przemieniecki 2000) could be well approximated by this approach.

Identifying Basic Network Trends

The knapsack and k -Shortest path approximations previously discussed illustrate how simple concepts and applications in the optimization of network interdiction can be used to develop alternative techniques in obtaining interdiction solutions. Additionally, the similarity between solutions of the SPNIP-M and SPNIP-LB problems in “[Formulating interdiction models](#)” combined with the approximation accuracy of the knapsack and k -Shortest approaches implies that there are certain problem properties and parameters (e.g. network complexity/structure and atom set composition) that have a high level of impact in determining defender and attacker interdiction solutions. Specifically pertaining to the SPNIP-M and SPNIP-LB, four problem properties were identified and tested to determine their significance in influencing the corresponding interdiction solutions. An experimental design similar to those already used was developed and tested within three real-world network: New York City, Boston and Houston. These networks were chosen because of their diverse network structure and were tested in combination with three distinct atom sets (Casas et al. 2012). The atom sets used maintain uniform, grid-like spacing between atoms but change density to increase the number of potential sensor locations.

To test whether a given problem property was influential or not, a Negative Binomial Regression (NBR) was used. The NBR was chosen instead of other

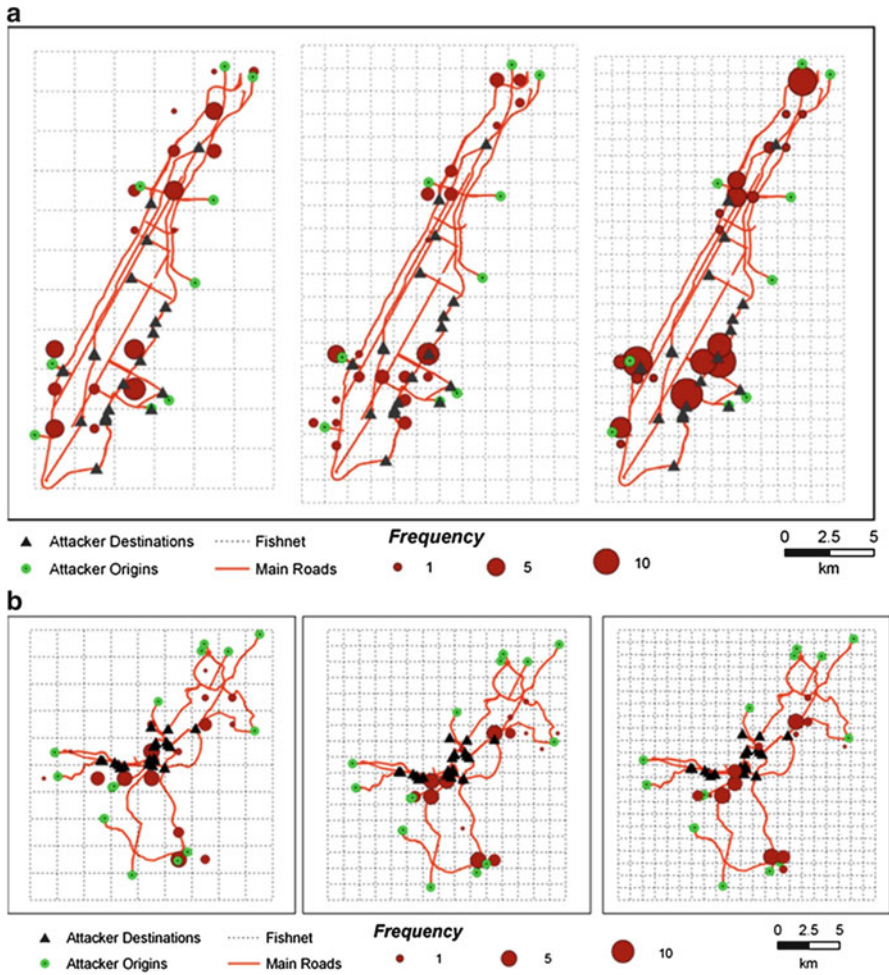


Fig. 23 Cumulative atom usage frequency from SPNIP-M experimental design for NYC (a) and Boston (b) (Casas et al. 2012)

regressions such as OLS or Poisson Regression due to the fact that most available atoms in SPNIP-M and SPNIP-LB are not used to locate sensors in the final solution. This creates sparse solution sets that NBR is better adept to evaluate. For information on NBR, please see Hilbe (2007). When implementing NBR to assess correlation, the frequency of atom use in aggregated SPNIP-M optimal solutions across the experimental design is used as the measuring variable.

Figure 23 illustrates the SPNIP-M optimal solutions for NYC and Boston while Fig. 24 illustrates the solutions for Houston. In the figures, frequency of use represents the cumulative number of sensors located at the particular atom across

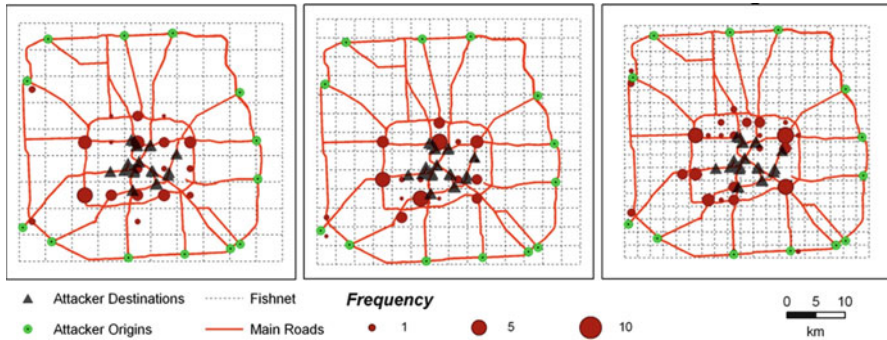


Fig. 24 Cumulative atom usage frequency from SPNIP-M experimental design for Houston (Casas et al. in submission)

all experimental runs. Atom density increases from left-to-right in each figure, with the three atom levels being low, med, and high.

Table 16 provides the statistical results from the NBR for all three networks under all three atom density sets. Again, we assume here that only one type of sensor is being allocated within the region. The four variables examined included *Coverage* (the total network distance covered by a sensor located at a given atom), *Count* (the number of arcs covered by locating a sensor at an atom), *Min Dist to Origin* (the distance from any given atom to its closest origin) and *Min Dist to Target* (the distance from any given atom to its closest target).

Highlighting the main points of interest (detailed discussion can be found in Casas et al. (in submission)), *Min Dist to Origin* plays an important role in determining whether an atom is used frequently in the various SPNIP-M experimental design cases. The closer an atom is to an identified origin, the higher its usage in SPNIP-M solutions. The NBR analysis also shows that *Min Dist to Target* is the least influential of the four variables examined. Simply stated, a defender in SPNIP-M creates a more influential detection system when they focus on early detection rather than target-specific sensor allocation. If the defender focuses on covering critical infrastructure independently, there is a “one-to-one” effect while a defender focusing on the coverage of origins experiences a “one-to-many” impact (many destinations are potentially covered or protected by the allocation of a single sensor). Additionally, the coverage capability of a sensor (*Count* in Table 16) is a quintessential factor in determine sensor location. The frequency of atom use is positively related to the number of arcs a sensor placed at that atom covers.

This last relationship is used to discuss the final interdiction-related problem of this chapter. Knowing that *Count* acts an indicator of atom usage, three strategic atom allocation schemes will be examined for New York City, Boston and Houston. These schemes will be developed using network topology and connectivity to create the atom set that guides sensor location. Using these intelligently created atom sets, the SPNIP-M optimal solutions will be examined and compared to the standard grid-like atom sets used in the previous analysis. The goal of this analysis is to determine

Table 16 Regression results for NYC, Boston and Houston at each atom density level

	New York City				Boston				Houston			
	Estimate	Std error	Pr (> z)		Estimate	Std error	Pr (> z)		Estimate	Std error	Pr (> z)	
	(Intercept)	3.006	1.086	0.00564	3.11E+00	1.21E+00	0.009902	Low density	-0.4703	1.652	0.7759	Low density
Coverage	1.331e-0.6	6.88E-07	0.05299	2.37E-06	1.42E-06	0.094174		6.83E-07	1.03E-07	3.51E-11		
Count	0.009112	0.4175	0.98259	-2.11E-02	2.89E-01	0.941637		-0.1295	0.06834	0.0581		
Min dist to origin	-0.000233	8.50E-05	0.00606	-1.00E-03	2.75E-04	0.000271		-1E-06	3.12E-05	0.9744		
Min dist to target	-0.000217	9.48E-05	0.02214	-2.78E-04	1.75E-04	0.113408		-4.5E-05	2.79E-05	0.1036		
(Intercept)	2.86	1.12E+00	0.0103	2.32E+00	1.24E+00	0.06213	Med density	1.438	1.868	0.44116	Med density	
Coverage	1.462e-0.5	2.17E-06	1.63E-12	2.68E-05	5.81E-06	3.99E-06		2.6E-06	3.67E-07	1.3E-12		
Count	-1.426	5.24E-01	0.006499	-1.44E+00	4.98E-01	0.00394		-0.2472	0.1274	0.0524		
Min dist to origin	-3.000412	1.08E-04	0.000133	-801E-04	3.33E-04	0.0163		-3.8E-05	3.56E-05	0.28488		
Min dist to target	-0.252	1.01E-04	0.013031	-5.77E-04	1.77E-04	0.00112		-0.00011	3.74E-05	0.00221		
(Intercept)	-1.052	1.05E+00	0.31685	-1.19E+00	8.63E-01	0.1679	High density	-0.7876	1.518	0.6038	High density	
Coverage	0.0000377	6.44E-06	4.85E-09	1.32E-04	1.84E-05	7.58E-13		5.92E-06	6.06E-07	<2e-16		
Count	2.897	6.64E-01	1.28E-05	-3.94E+00	1.01E+00	9.14E-05		-0.336	0.153	0.0281		
Min dist to origin	-0.000276	1.05E-04	0.00893	-8.07E-04	3.24E-04	0.0128		-1.2E-05	2.86E-05	0.683		
Min dist to target	-8.29E-05	1.01E-04	0.41022					-7E-05	2.74E-05	0.0104		

the effect that atom location sets have on optimal SPNIP-M sensor locations and to evaluate computational and spatial trade-offs in determining whether the additional fidelity obtained from intelligent atom locations provides significantly improved or diverse defender sensor schemes.

Intelligently Locating Atoms

The problem of locating atoms intelligently is motivated by the observation that not all networks are created equal and that not all uniform, grid-based atom allocations are capable of providing an adequate set of sensor location points for network interdiction. The hypothesis of intelligent atom design is that atom allocations that are derived based on individual network properties will provide higher fidelity, more accurate solutions to network interdiction problems. Given that network structure is relatively unique, devising intelligent atom sets will give more sensor location options in areas that are denser, or which have a higher concentration of arcs with low initial detection probabilities.

Observing that analyzers have different interests in network features, we develop three methods to add atoms intelligently. For the network interdiction problem, methods are based on the initial arc non-detection values, the density of arcs in a pre-defined space and the number of arcs in a pre-defined space. The algorithmic approach to creating these atom structures is executed using ESRI ArcGIS 10 and is now provided. Figure 25 illustrates algorithmic implementation for the Boston network.

Intelligent atom algorithm

1. Determine the geographic area the network occupies (x , y or latitude, longitude coordinates).
2. Build an initial grid-based structure (user decided initial grid size).
3. For each grid, calculate the {average arc non-detection, arc density, number of arcs}.
4. If the grid value exceeds the decision threshold, further decompose grid into quarters.
5. Stopping criteria.
 - (a) If the iteration number is pre-determined and has been reached, STOP.
 - (b) If the iteration number is not pre-determined and no existing grids require decomposition, STOP.
 - (c) If at least one grid was decomposed in Step 4, return to Step 3.

Figure 25d illustrates the final atom set for Boston using the number of arcs within a grid as the decomposition measure. Locating atoms intelligently, the atom set is clearly more contoured to the individual structure of the Boston network. To examine whether the increased complexity of an intelligent atom set is useful from a modeling standpoint, an experimental design similar to those previously discussed is invoked. The individual solutions from the experimental design runs are aggregated

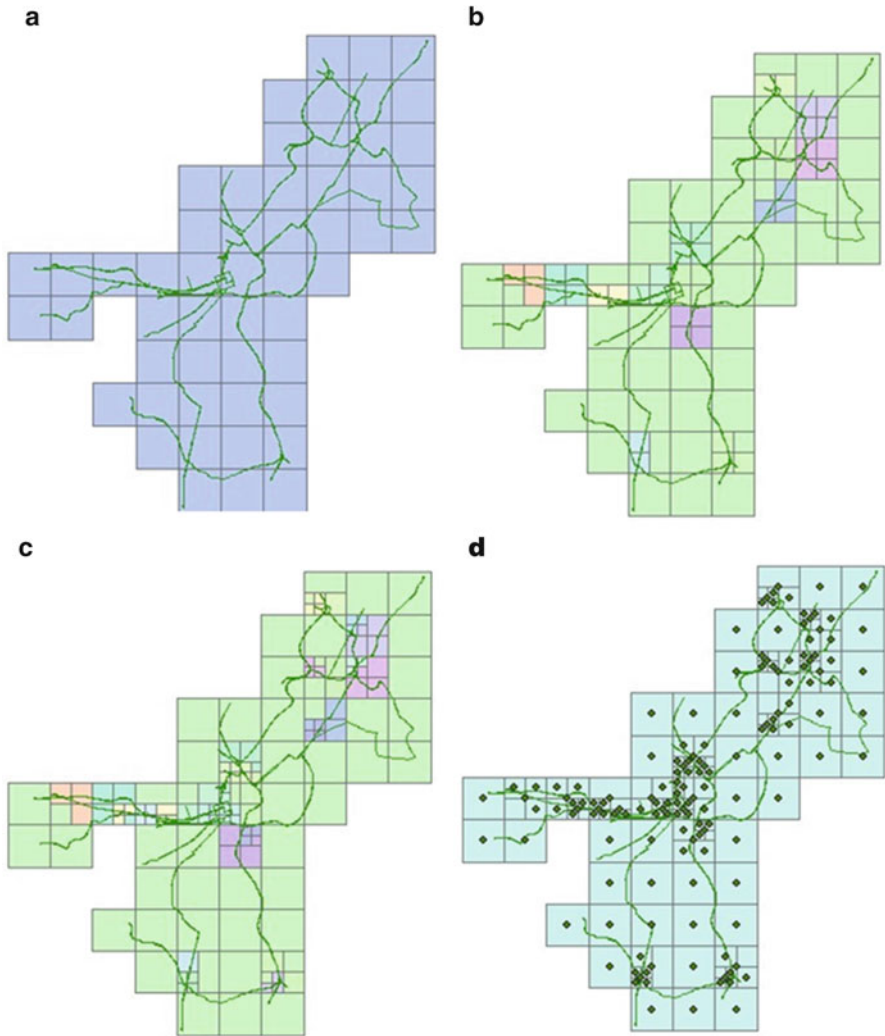


Fig. 25 Using the arc number to intelligently locate atoms

and used to obtain average computational information for road networks in New York City (NYC), Washington DC (DC), Boston, MA and Houston, TX. In total six atom allocations were considered and compared. They are: low resolution grid-based (low), med resolution grid-based (med), high resolution grid-based (high), arc length intelligent (length), arc number intelligent (number) and arc non-detection intelligent (non-det). For each network, 15 randomly generated origin-target pairs were identified with each origin and target being pulled from a pre-defined origin and destination set (origin and target size for each of the 15 pairs was also randomly generated using a uniform distribution between one and the corresponding

Table 17 Better caption

		Grid allocations			Intelligent allocations		
		Low	Med	High	Length	Number	Vulnerability
NYC	Objective	0.23	0.21	0.23	0.21	0.22	0.22
	No. paths	9.79	10.98	8.17	11.32	11.45	10.92
	Sol. time	28.70	76.40	39.05	748.00	717.00	753.00
DC	Objective	0.16	0.18	0.22	0.06	0.06	0.06
	No. paths	30.48	21.51	14.12	11.10	10.06	11.26
	Sol. time	269.70	268.30	373.60	877.00	572.00	2, 188.00
Boston	Objective	0.18	0.19	0.18	0.13	0.14	0.13
	No. paths	12.56	10.60	10.73	21.97	22.37	25.68
	Sol. time	27.99	25.58	27.31	216.60	205.90	326.00
Houston	Objective	0.11	0.24	0.20	0.14	0.12	0.11
	No. paths	18.35	19.11	17.12	14.06	15.84	13.02
	Sol. time	584.70	281.40	646.00	402.00	1, 431.00	103.30

origin/target set size). Four budget levels enabled the allocation of 4, 6, 8 and 10 sensors within the region. The computational results from this experimental design are given in Table 17, with each experimental design case being solved to optimality using Bender's Decomposition.

From Table 17, it can be shown that the computational comparison between the standard grid-based atom sets and intelligent atom sets is inconclusive at best. In certain networks like NYC and Boston, there is little different in the optimal objective values of grid and intelligent atom sets but a great gain in solution time. Though the actual number of Bender's Decomposition iterations does not increase dramatically, the intelligent atom allocations create a substantial rise in defender sub-problem solution times. With intelligent atom location, many individual atoms will have similar coverage schemes, especially in SPNIP-M where coverage is binary and the actual length of coverage is not counted. This similarity extends the amount of branching required to solve the defender sub-problem, increasing its solution time. For the DC and Houston networks, Table 17 shows that there is more significant dissimilarity between objective function values, though the intelligent atom allocations actually reduce the number of Bender's Decomposition iterations. In all, it appears that there may be some usefulness to an intelligent atom design, though in those network cases examined to date, the increased computational effort does not appear to be worth the limited fidelity gained over a grid-based approach.

Conclusions

In this chapter, we began by discussing the hazardous materials transportation problem as it is addressed in optimization. We saw how traditional hazardous

materials modeling in the 1970s and 1980s transitioned towards and motivated development of the network interdiction problem in the mid-1990s and early 2000s. Focusing on the network interdiction problem, discussion was provided on the standard shortest path network interdiction formulation and two initial variations (one modified and one length-based shortest path network interdiction problem). In the modified problem (SPNIP-M), we saw how sensor location could be separated from the network, with sensors instead located at geographic points called atoms. Examples were provided on the computational and spatial performance of SPNIP-M and SPNIP-LB, with various measures of spatial similarity introduced to compare and contrast the solutions of these models.

In the later part of this chapter, we used the obtained knowledge from SPNIP-M and SPNIP-LB to develop approximations with the goal of reducing computation time while maintaining a similar spatial distribution of sensors. We saw how the max flow-min cut theorem could be used to motivate development of a constrained knapsack approximation. This approximation was able to maintain consistent computational solution times across each of the two networks examined while reasonably replicating spatial sensor locations. In addition to the knapsack model, we pursued a spatially-based regression study which used a detailed experimental design to statistically identify two spatial properties which were shown to be pertinent factors in allocating defender resources. Lastly, used one of these properties (the number of arcs within a sensor's range) to motivate development of an algorithm to strategically determine potential sensor locations for a given network. Computational results from this intelligent atom location show that the more simplistic grid-based solutions to provide a strong base-line for sensor allocation strategies with increased fidelity in defender sensor solutions from the intelligent atom allocations coming at a steep computational price.

Acknowledgements Special acknowledgement is given to Christopher Hill and Nannan Chen, who contributed in the development and analysis of select sections in this work while students at Texas A&M University.

References

- Anselin L (1995) Local indicators of spatial association – LISA. *Geogr Anal* 27:93–115
- Bard J (1998) *Practical bilevel optimization; algorithms and applications*. Kluwer Academic Publishers, Boston
- Batta R, Chiu S (1998) Optimal obnoxious paths on a network: transportation of hazardous materials. *Oper Res* 36(1)
- Brown G et al (2006) Defending critical infrastructure. *Interfaces* 36(6):530–544
- Burch C et al (2003) A decomposition-based approximation for network inhibition. *Network interdiction and stochastic programming*. Kluwer, Boston, pp 51–69
- Casas et al. (Louisiana Tech University, 2012, unpublished)
- U.S. Census Bureau (2008) TIGER/line and TIGER-related products. <http://www.census.gov/geo/www/tiger/>. Accessed 1 Aug 2008

- Church R, Scaparra M (2007) Protecting critical assets: the r-interdiction median problem with fortification. *Geogr Anal* 39:129–146
- Church R, Scaparra M, Middleton S (2004) Identifying critical infrastructure: the median and covering facility interdiction problems. *Ann Assoc Am Geogr* 94(3):491–502
- Corley HW, Chang H (1974) Finding the n most vital nodes in a flow network. *Manage Sci* 21:362–364
- Cova T, Conger S (2003) Transportation hazards. In: Kutz M (ed) *Handbook of transportation engineering*. McGraw Hill, New York, pp 17.1–17.24
- Cunningham WH (1985) Optimal attack and reinforcement of a network. *J Assoc Comput Mach* 32:549–561
- Department of Homeland Security (2009) Critical infrastructure and key resources. http://www.dhs.gov/files/programs/gc_1189168948944.shtm. Accessed 7 Jul 2009
- Erkut E, Verter V (1998) Modeling of transport risk for hazardous materials. *Oper Res* 46(5)
- ESRI (2009) ArcGIS: a complete integrated system. <http://www.esri.com/software/arcgis/index.html>. Accessed 10 Feb 2010
- Federal Emergency Management Agency (2006) Software program for estimating potential losses from disasters. <http://www.fema.gov/plan/prevent/hazus>. Accessed 25 May 2006
- Field M (2004) Highway security and terrorism. *Rev Policy Res* 21(3):71–91
- Ghare P, Montgomery D, Turner WC (1971) Optimal interdiction policy for a flow network. *Nav Res Logist Q* 18:37–45
- Gopalan R et al (1990) Modeling equity of risk in the transportation of hazardous materials. *Oper Res* 38(6)
- Grubestic T, Murray A (2006) Vital nodes, interconnected infrastructures, and the geographies of network survivability. *Ann Assoc Am Geograph* 96(1):64–83
- Hilbe JM (2007) *Negative binomial regression*. Cambridge University, Cambridge
- Huang B, Cheu RL, Liew YS (2004) GIS and genetic algorithms for HazMat route planning with security considerations. *Int J Geogr Inf Sci* 18(8):769–787
- Israeli E, Wood K (2002) Shortest-path network interdiction. *Networks* 40(2):97–111
- Jenelius E, Petersen T, Mattsson LG (2006) Importance and exposure in road network vulnerability analysis. *Transp Res A* 40:537–560
- Jin H, Batta R (1996) On the analysis of two new models for transporting hazardous materials. *Oper Res* 44(5)
- Jin H, Batta R, Karwan M (1996) On the analysis of two new models for transporting hazardous materials. *Oper Res* 44(5)
- Kara B, Verter V (2004) Designing a road network for hazardous materials transportation. *Transp Sci* 38(2):188–196
- Laefer D, Pradhan A (2006) Evacuation route selection based on tree-based hazards using light detection and ranging and GIS. *J Transp Eng* 132(4):312–320
- Lim C, Smith JC (2007) Algorithms for discrete and continuous multicommodity flow network interdiction problems. *IIE Trans* 39:15–26
- List G et al (1991) Modeling and analysis for hazardous materials transportation: risk analysis, routing/scheduling and facility location. *Transp Sci* 25(2)
- Luedtke J, White C (2002) *HazMat transportation and security: survey and directions for future research*. Department of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta, GA
- Matisziw T, Murray A, Grubestic T (2007) Bounding network interdiction vulnerability through cut-set identification. *Adv Spat Sci* 61:243–255
- Matisziw T, Murray A (2009) Modeling s-t path availability to support disaster vulnerability assessment of network infrastructure. *Comput Oper Res* 36:16–26
- MCEER (2006) REDARS 2 methodology and software for seismic risk analysis of highway systems. <http://mceer.buffalo.edu>. Accessed 25 May 2006
- Morton D, Pan F, Saeger K (2007) Models for nuclear smuggling interdiction. *IIE Trans* 39:3–14
- Murray A, Matisziw T, Grubestic T (2007) Critical network infrastructure analysis: interdiction and system flow. *J Geogr Syst* 9:103–117

- National Highway Institute (1996) Highway routing of hazardous materials, guidelines for applying criteria. The Institute, USA, p 123
- Nemhauser G, Wolsey L (1999) Integer and combinatorial optimization. Wiley-Interscience, New York
- Phillips (1993) The network inhibition problem. Proceedings of the 25th annual ACM symposium on the theory of computing (STOC), May 1993, pp 776–785
- Przemieniecki JS (2000) Mathematical methods in defense analyses. AIAA Education Series, Reston, Virginia
- Qiao J et al (2007) Allocating security resources to a water supply network. IIE Trans 39:95–109
- Ratliff HD, Sicilia G, Lubore S (1975) Finding the n most vital links in flow networks. Manage Sci 21:631–639
- Scaparra M, Church R (2008) A bilevel mixed-integer program for critical infrastructure protection planning. Comput Oper Res 35:1905–1923
- Southworth F (2008) Multi-criteria sensor placement for emergency response. Appl Spatial Anal 1:37–58
- Texas Transportation Institute (2011) The 2011 urban mobility report. Texas A&M University, College Station
- Transportation Research Board (2002) Deterrence, protection, and preparation: the new transportation security imperative – special report 270
- Transportation Security Administration (2012) Highway and motor carrier division. http://www.tsa.gov/what_we_do/tsnm/highway/index.shtm. Accessed 10 Jan 2012
- US Department of Transportation (2006) Biennial report on hazardous materials transportation. Washington, DC. Report (obtained online). Accessed 12 Aug 2012
- US Department of Transportation (2012) PHMSA: pipeline and hazardous materials safety administration. <http://www.phmsa.dot.gov/>. Accessed 10 Jan 2012
- Wein L, Atkinson M (2007) The last line of defense: designing radiation detection-interdiction systems to protect cities from a nuclear terrorist attack. IEEE Trans Nucl Sci 54:654–669
- Wollmer R (1964) Removing arcs from a network. Oper Res 12:934–940
- Wood K (1993) Deterministic network interdiction. Math Comput Model 17(2):1–18
- Wood RK (2003) Deterministic network interdiction. Math Comput Model 17(2):1–18
- Yamada I, Thill JC (2010) Local indicators of network-constrained clusters in spatial patterns represented by a link attribute. Ann Assoc Am Geogr 100(2):269–285
- Yates J, Sanjeevi S (2013) A length-based multiple resource type approach to shortest path network interdiction. *Int J Crit Infrastruct Protect* (Spring)
- Yates J, Wang X, Chen N (2013) Assessing k-Shortest approximation accuracy for shortest path network interdiction. *Optimiz Eng* (Summer)
- Yates J, Casas I (2010) Role of spatial data in the protection of critical infrastructure and homeland defense. *Appl Spat Anal Policy* 5:1–18
- Yates J, Lakshmanan K (2011) A constrained binary knapsack approximation for shortest path network interdiction. *Comput Ind Eng* 61:981–992
- Yates J, Sanjeevi S (2012) Assessing the impact of vulnerability modeling in the protection of critical infrastructure. *J Geogr Syst* 14:415–435
- Yen J (1971) Finding the k shortest loopless paths in a network. *Manage Sci* 17(11):712–716