Transport Policy 24 (2012) 109–117

Contents lists available at SciVerse ScienceDirect

Transport Policy

journal homepage: www.elsevier.com/locate/tranpol

Establishing public policy to protect critical infrastructure: Finding a balance between exposure and cost in Los Angeles County

Justin Yates [a,*], Rajan Batta [b], Mark Karwan [b], Irene Casas [c]

[a] Department of Industrial and Systems Engineering, Texas A&M University, 4079 Emerging Technologies Building, College Station, TX 77843-3131, USA
[b] Department of Industrial and Systems Engineering, University at Buffalo (State University of New York), 432 Bell Hall, Buffalo, NY 14260, USA
[c] Department of Social Sciences, Louisiana Tech University, PO Box 9988, Ruston, LA 71272, USA

ARTICLE INFO

Available online 8 September 2012

Keywords:
Sensor location
Homeland security
Critical infrastructure protection
Bi-level programming

ABSTRACT

This paper examines the problem of critical infrastructure protection in urban environments and provides a mechanism for evaluating the performance allocated resources on defense of the region. In the devised formulation, a bi-level mixed integer program and hypercube queuing model compose the mathematical model used to represent the concept of critical infrastructure protection between an attacker and a defender operating within the urban environment and an experimental design is used as the basis for observing salient properties and trends. Applying the model within Los Angeles County, California, results demonstrate the trade-offs observed in various protection schemes and illustrate how continuously increasing defense resources does not guarantee a safer region. The implication of detection strategy on response capability is also assessed through the case study, illustrating the importance of balance when deriving solutions. We also show how the mathematical model may be used to support research and development in defense technologies by identifying resource characteristics that strongly influence infrastructure protection.

Published by Elsevier Ltd.

1. Introduction

This paper addresses the location of detection sensors and interception units for the protection of critical infrastructure and key resources connected via network. Determination of optimal detection sensor locations in scenarios of defense/homeland security is not new to the optimization field. A summary of some typically applied network and facility location models can be found in Daskin (1995). Recently, the shortest path network interdiction problem (SPNIP) introduced by Israeli and Wood (2002) has been extensively applied to the domain of homeland defense. The traditional SPNIP is a two player (leader and follower) problem with competing objectives. The follower operates within the network such that the shortest path between an origin (set of possible origins) and destination (set of possible destinations) minimized. The leader "interdicts" network arcs subject to a given budget such that this minimum shortest path is maximized. In this paper, a modified SPNIP determines detection sensor allocation given a similar two-player structure (in this case, an attacker and a defender). In the modified shortest path network interdiction problem (SPNIP-M), the attacker seeks a path of maximum non-detection through the network from an origin (set of possible origins) to a destination (set of possible destinations) while the defender allocates detection sensors such that the path of maximum non-detection is minimized (sensors reduce arc and subsequently path, non-detection probabilities). Defender allocation is subject to a restrictive budget. Contrary to the traditional SPNIP, the SPNIP-M does not necessitate that sensors be allocated directly to network arcs/nodes and it allows for the influence of multiple network arcs by a single sensor. Variants of the SPNIP have been used in border patrol, port security, wireless network protection and extreme events scenarios, but none incorporate the SPNIP-M modifications (Brown et al., 2006; Wein and Atkinson, 2007; Doerner et al., 2009).

In many papers evoking the SPNIP model, the concept of a secure network stops at successful detection (Bayrak and Baily, 2008; Morton et al., 2007; Southworth, 2008). Realistically, detection is only the first step in securing a network/critical infrastructure with the second being the capability to successfully intercept sensor alarms. While interception may not be as physically burdensome in wireless network security, critical infrastructure protection, border patrol and port security all require the physical movement of persons, vehicles, and weaponry to successfully stop or mitigate malicious adversarial advances. In this paper, interception unit location is modeled as a *p*-Median problem where the obtained optimal sensor allocation determines demand. A hybercube queuing model incorporates sensor allocation and interception unit location to ascertain individual and team interception performance metrics

* Corresponding author. Tel.: +1 979 458 2337.
E-mail addresses: jtyates@tamu.edu (J. Yates), batta@eng.buffalo.edu (R. Batta), mkarwan@eng.buffalo.edu (M. Karwan), icasas@latech.edu (I. Casas).

0967-070X/$ - see front matter Published by Elsevier Ltd.
http://dx.doi.org/10.1016/j.tranpol.2012.08.003

(e.g. unit/team utilization rates, average response time, etc.). The proposed integration of sensor location and interception unit location/evaluation helps to ensure that decisions of defense and public policy are capable of representing dependencies reflected in real-world homeland security (i.e. budget levels and allocation of sensors may be determined at the federal level through the Department of Homeland Security or another governmental agency while the duty to intercept any triggered alarms often rests with local law enforcement). Such directive dichotomy is pervasive in current defense and critical infrastructure protection policies (Lewis, 2006).

This paper is divided into four major sections. The first introduces the SPNIP-M and illustrates its distinction from the traditional SPNIP model. The second section describes the interception unit components of location (p-Median) and evaluation (hypercube queue) and defines the linkage between defense sensor location and interception location/evaluation. The third section studies an example case of critical infrastructure protection using road network and critical infrastructure location data from Los Angeles County, California. The final section of this paper summarizes the obtained results and discusses the successes and limitations of the integrated sensor and interception location model.

2. Sensor location

We begin by defining a network of interest as a set of connected nodes $n \in N$ and directed arcs $i \in \Lambda$, $G(N,\Lambda)$. The node set may be subdivided into entry points ($o \in N^O$) and targets ($d \in N^D$) such that $N^O \subset N$, $N^D \subset N$ and $N^O \cap N^D = \phi$. A set of locatable sensor types S is given where $S=\{0,1\} \cup \{0,1,2,...,\omega\}$, $\omega \in Z^+$ depending on whether the model considers only a single sensor type or a set of sensor types for allocation ($s=0$ represents the base/null case). A sensor $s \in S$ is identified by the parameters f_s^+ (false positive rate), η_s (sensitivity/strength), c_s (cost) and r_s (range).

To remove sensor location dependency on the network, the geographic region where the network resides is discretized into a series of individual atoms a at which sensors are located. An atom may be coincident to any node or arc of the network or may be disjoint such that there is no spatial dependency on the given network for sensor location. The set A of atoms contains all possible sensor locations within the region. The set of network arcs influenced by a sensor of type s located at atom a is given as R^{as} (if any portion of an arc i falls within the range of sensor s at atom a, then $i \in R^{as}$). Path non-detection probability is the product of individual arc non-detection probabilities for arcs on the given path (independence of arc non-detection probabilities is assumed).

In the traditional SPNIP, there exists one decision variable for the leader representing the arcs comprising the shortest path through the network and one decision variable for the follower representing those arcs selected for interdiction. Allowing sensor locations to be disjoint from the network in the SPNIP-M necessitates the definition of a third decision variable representing the relationship between sensor location and network arc influence. As a result, there are two binary defender decision variables (sensor location at atoms and sensor influence of network arcs) and one binary attacker decision variable (the arcs comprising the path of maximum non-detection through the network). The original SPNIP-M formulation is now presented.

[SPNIP-M]

Parameters:
$k_{ni}=1$ if node n is incident to arc i, $k_{ni}=0$ otherwise
$qn=\{1,-1,0\}$ if node n is an {origin, intermediate, destination}
$r_i^{as}=1$ if a sensor of type s at atom a influences arc i, 0 otherwise
$B=$ the total defense budget for sensor allocation

Variables:
$w_i=1$ if arc i is used by the attacker, $w_i=0$ otherwise
$y_{as}=1$ if sensor type s is allocated to atom a, $y_{as}=0$ otherwise
$x_{is}=1$ if arc i is covered by a type s sensors, $x_{is}=0$ otherwise

Formulation:

$$z = \min_{x,y} \max_{w} \prod_{i,s} u_{is}^{w_i x_{is}} \tag{1}$$

$$\text{s.t.} \quad \sum_i k_{ni} w_i \le q_n \quad \forall n \tag{2}$$

$$x_{is} - \sum_a r_i^{as} y_{as} \le 0 \quad \forall i,s \tag{3}$$

$$\sum_s x_{is} = 1 \quad \forall i \tag{4}$$

$$\sum_a \sum_s c_s y_{as} \le B \tag{5}$$

$$w,x,y \in Binary$$

In SPNIP-M, (1) represents the competing defender and attacker objective function with z yielding the min max network non-detection probability. Objective function (1) may be converted into a linear objective function through logarithmic transformation. Constraint (2) ensures conservation of flow through the network as the attacker selects the maximum non-detection path. Constraint (3) has the following interpretation: "a sensor may not be considered to be influenced by a type s sensor unless it falls within the detection range r_s of a located sensor." Constraint (4) ensures that all arcs are covered, either by the null sensor ($s=0$) or one of the available sensor types. Constraint (5) limits defender sensor allocation to a maximum budget B.

Optimal solutions to SPNIP-M are obtained using Benders Decomposition, viable because the defender and attacker decision variables do not appear together in any single set of constraints. This enables the problem to be subdivided into an attacker sub-problem and a defender master problem. Benders Decomposition is an iterative approach that successively solves the sub and master-problems by adding solutions from the sub-problem as constraints to the master. The procedure ceases when a constraint generated via the sub-problem already exists in the master constraint set, yielding a provably optimal solution (Bard, 1998).

SPNIP-M is capable of modeling scenarios to locate sensors of only one type, or of multiple types. SPNIP-M is not, however, capable of addressing situations of multiple or overlapping coverage. By definition of (4) and the binary conditions, one and only one $x_{is}=1$ for all arcs. In the case where (3) allows multiple x_{is} to be positive, (1) ensures that the highest impact (i.e. strongest) sensor will be chosen to influence that arc (recall that x_{is} determines which sensor influences an arc, not the sensor location which is determined by y_{as}). A more realistic sensor location model should be capable of quantifying the combined effect on non-detection probability of an arc residing within multiple located sensor ranges. By redefining x_{is} and altering (1), (3) and (4), the SPNIP-M formulation may be further generalized to account for the additive influence of an arc covered by multiple sensors. This model was first proposed in Yates et al. (2010). The following substitutions enable transition to an additive model (all other SPNIP-M definitions remain).