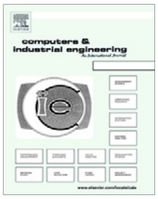
Computers & Industrial Engineering 61 (2011) 981–992

Contents lists available at ScienceDirect

Computers & Industrial Engineering

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



A constrained binary knapsack approximation for shortest path network interdiction

Justin Yates *, Kavitha Lakshmanan

Department of Industrial and Systems Engineering, Texas A&M University, United States

ARTICLE INFO

Article history:
Received 6 December 2010
Received in revised form 11 May 2011
Accepted 14 June 2011
Available online 17 June 2011

Keywords:
Network interdiction
Homeland security
Approximation techniques
Integer programming

ABSTRACT

A modified shortest path network interdiction model is approximated in this work by a constrained binary knapsack which uses aggregated arc maximum flow as the objective function coefficient. In the modified shortest path network interdiction problem, an attacker selects a path of highest non-detection probability on a network with multiple origins and multiple available targets. A defender allocates a limited number of resources within the geographic region of the network to reduce the maximum network non-detection probability between all origin-target pairs by reducing arc non-detection probabilities and where path non-detection probability is modeled as a product of all arc non-detection probabilities on that path. Traditional decomposition methods to solve the shortest path network interdiction problem are sensitive to problem size and network/regional complexity. The goal of this paper is to develop a method for approximating the regional allocation of defense resources that maintains accuracy while reducing both computational effort and the sensitivity of computation time to network/regional properties. Statistical and spatial analysis methods are utilized to verify approximation performance of the knapsack method in two real-world networks.

1. Introduction

Shortest path network interdiction may be considered as either a deterministic or stochastic attacker-defender game played with limited resources over a connected network with sequential movement. These games may be played with perfect, imperfect, or asymmetric knowledge, discrete or continuous interdiction, and have been applied to a wide array of applications in homeland security and defense which include but are not limited to port security, border patrol, and the protection of critical infrastructure. As focus on these interdiction problems has increased in recent years, so too has the desire to model more complex networks and interdiction scenarios. Such increases in complexity and scope have necessitated the examination of alternative solution and approximation approaches to the traditional shortest path network interdiction problem due to the inability of optimal solution techniques to maintain computational tractability with the added scope.

In order to effectively demonstrate the viability of alternate solution approaches to the shortest path network interdiction problem, it is necessary to examine not only the capability to approximate the computational solution but the spatial solution as well. The desire to closely approximate computational results is relatively obvious. Reliable solution techniques need to illustrate consistency in their ability to return optimal values and solutions that provide accurate numerical approximations. As an example, the probability of damage to critical infrastructure, the probability to detect a covert adversary, or the probability to identify illicit materials inside of a container, are all examples of computational metrics which would be used to evaluate the appropriateness of any proposed resource allocations or policy procedures. The desire to closely approximate spatial results, however, is arguably just as vital to the success and confidence of approximation procedures. When employing approximation models, there exists the real potential for multiple redundant solutions (naturally, this depends on the modelers' choices in formulation, network representation, network parameter assignment, etc.) which could yield the same optimal value through significantly different spatial resource allocations. Allocating resources to sub-optimal locations could lead to disastrous results including the loss of life and infrastructure, as well as large fiscal and psychological burdens for the attacked region and its population. It is imperative, therefore, that any developed approximate procedures for such scenarios be adequately vetted and tested to ensure their reliability and capability to produce results that are both computationally and spatially true.

Recognition of the need for competent approximation procedures in network interdiction has been directly stated (Church & Scaparra, 2007; Lim & Smith, 2007). Algorithmic/heuristic

---

* Corresponding author. Address: Department of Industrial and Systems Engineering, Texas A&M University, 237D Zachry Engineering Center, 3131 TAMU, College Station, TX 77843-3131, United States. Tel.: +1 979 845 1506.

E-mail addresses: jtyates@tamu.edu (J. Yates), klakshmanan@neo.tamu.edu (K. Lakshmanan).

0360-8352/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cie.2011.06.011

Nomenclature

A	set of suitable sensor locations
Λ	set of network arcs
α	weight of objective criterion where $0 \leqslant \alpha \leqslant 1$
B	total allowable defense budget
c_s	cost to locate sensor type $s \in S$
k_{ni}	binary variable where $k_{ni} = 1$ if arc $i \in \Lambda$ is incident to node $n \in N$, otherwise $k_{ni} = 0$
m_j	aggregate maximum flow over arc $j \in \Lambda$
N	set of network nodes
η_s	sensitivity of sensor s with $0 \leqslant \eta_s \leqslant 1$
p_j	number of network intersections separating arc $j \in \Lambda$ from its closest network origin
q_n	$\{1, -1, 0\}$ if node n is an {origin, destination, intermediate}
φ_b	objective function coefficient for atom $b \in A$
R^{as}	set of arcs falling within the range of influence of a type s sensor located at atom $a \in A$
r_i^{as}	binary variable representing whether an arc is capable of being covered $\left(r_i^{as} = 1\right)$ by a type s sensor located at atom a or not $\left(r_i^{as} = 0\right)$
S	set of sensor types available for location
ϕ^j	set of atoms covering arc $j \in \Lambda$
τ	maximum allowable sensor coverage
u_{ist}	non-detection probability for arc $i \in \Lambda$ under the coverage of t type s sensors

Decision variables

w_i	$w_i = 1$ if arc $i \in \Lambda$ used in the attacker path, otherwise $w_i = 0$
y_{as}	$y_{as} = 1$ if sensor type $s \in S$ located at $a \in A$, otherwise $y_{as} = 0$
x_{ist}	$x_{is} = 1$ if $i \in \Lambda$ covered by t type $s \in S$ sensors, otherwise $x_{ist} = 0$
v_b	$v_b = 1$ if atom $b \in A$ is used, otherwise $v_b = 0$

Acronyms

BD	benders decomposition
CIKR	critical infrastructure and key resources
KNAP	constrained knapsack approximation
GIS	geographic information system
DSPNI	discrete shortest path network interdiction problem

combinations as well as heuristic methods have been employed to obtain solutions to deterministic and stochastic network interdiction problems (Held & Woodruff, 2005; Royset & Wood, 2007; Salmeron, Wood, &Baldick,Bald). Within the current literature (including those papers cited above), focus on algorithmic/heuristic performance relies almost exclusively on a computational barometer. Often formulated as bi-level or multi-objective problems, the developed network interdiction approximation procedures work well to combat the computational time burden observed in obtaining an optimal solution. Even for small networks, the computational effort required to solve these problems can be significant.

A common approach in the literature to solve the network interdiction problems is to implement some form of Benders Decomposition, effectively sub-dividing the larger multi-objective problem into a master problem and sub problem which can then be solved iteratively to obtain an optimal solution. This approach can be observed in (Brown, Carlyle, Salmeron, & Wood, 2006; Israeli & Wood, 2002; Yates & Casas, 2010). In practice, the master problem tends to scale poorly with relation to increases in network size and complexity and, overall, tends to require the majority of computational effort (as an example, Brown et al., 2006, indicate up to 90% of computation time in obtaining an optimal interdiction solution was spent solving the master problem). Approximation procedures may attempt to reduce the number of Benders Decomposition iterations (and thus the number of times the master problem needs to be solved) through cut generation or the addition of other inequality constraints. For problems of the size typically considered in the literature, such approaches may be viable (e.g., 200 arcs, 50 nodes). For truly large-scale, regionally representative networks, however (e.g. 200,000 + arcs, 10,000 + nodes), even one iteration of the master problem may be computationally prohibitive. It is for this reason that reliable approximate procedures and methods which are not hindered by such combinatorial properties are sought and desired within the network interdiction domain.

This paper examines the discrete shortest path network interdiction problem (DSPNI) with perfect information in a two-player attacker-defender game and develops a knapsack-based solution approach for obtaining strong computational and spatial approximations to the optimal DSPNI solution. The motivation for this approach lies in the desire to accurately and consistently approximate both the optimal objective value and the spatial location of allocated resources in a single, simplistic model that does not suffer computationally from the same problems of scale observed in Benders Decomposition and other algorithmic/heuristic approaches. The DSPNI model used as a base-line in this paper was first introduced in (Yates & Casas, 2010) and modifies the traditional DSPNI by augmenting the spatial emphasis placed on resource allocation. The remainder of this paper is organized in the following way. Section 2 supports development of and presents a formulation for the knapsack approximation model, introduces terminology which will be used throughout the paper, and discusses the DSPNI problem examined. Section 3 introduces two test-case networks from Los Angeles County, California that will be examined within a structured experimental design to assess the computational and spatial performance of the proposed knapsack approximation. Sections 4 and 5 analyze the results of the experimental design computationally and spatially, respectively. Section 6 concludes this paper.

2. Approach and approximation

The goal of this paper is to develop a knapsack-based method for approximating computational and spatial solutions to the DSPNI. Motivating this work is the observation that current procedures for obtaining optimal solutions to DSPNI become computationally prohibitive as network size/complexity increases, inhibiting the ability of policy and decision makers to obtain solutions in a timely manner (or in the case of large-scale networks, obtain any solution at all). When interpreting the DSPNI in terms of public policy decisions, the primary objective is to effectively locate defense resources within the given region. Determining these resource locations is thus the primary concern and direct output of the developed approximation.

To develop a reliable approximation, the authors examine incorporation of maximum-flow/min-cut into a multi-objective, constrained knapsack formulation. This section introduces