Computers and Operations Research 98 (2018) 56–68

Contents lists available at ScienceDirect

Computers and Operations Research

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

A bilevel exposure-oriented sensor location problem for border security

Aaron M. Lessin*, Brian J. Lunday, Raymond R. Hill

Department of Operations Research, Air Force Institute of Technology, 2950 Hobson Way, Wright-Patterson AFB, OH 45433, USA

ARTICLE INFO

Article history:
Received 1 December 2017
Revised 26 March 2018
Accepted 16 May 2018
Available online 17 May 2018

Keywords:
Bilevel programming
Minimal exposure path
Wireless Sensor Networks
Border surveillance
Barrier coverage

ABSTRACT

We propose a bilevel math programming model for locating a heterogeneous set of sensors to maximize the minimum exposure of an intruder's penetration path through a defended region. Our formulation also allows a defender to specify minimum probabilities of coverage for a subset of the located sensors (e.g., the most valuable sensors) and for high-value asset locations in the defended region. We reformulate the bilevel program to a single-level optimization problem for which instances can be readily solved using a commercial solver. Given the locations of a defender's sensors, we additionally formulate three alternative path identification models corresponding to conceptually-motivated intrusion-path metrics. We examine a test instance for the air defense of a border region against intrusion by an enemy aircraft; upon identifying the optimal, respective defender asset location and intruder routing solutions, we examine the intruder-optimal solutions corresponding to each of three alternative metric-specific paths, illustrating the relative impact of an intruder choosing an inappropriate metric. Sensitivity analyses are conducted to examine the effect of several model parameters on solution quality and required computational effort.

Published by Elsevier Ltd.

1. Introduction

National, group, and individual sovereignty requires protection against threats. At the national level, potential threats include the illegal or unauthorized movement of people, weapons, or drugs. At the group level, corporations seek to defend their computer networks against malicious code. Individual sovereignty concerns include protection of a residence against burglary. The defense against such threats begins at a border or boundary of the region under a defender's control, whether it be physical or virtual. Moreover, the defense against threats occurs within a *border region*, wherein a defender will locate and use assets to detect and/or interdict a would-be intruder.

Evidence of the growing requirement for border security can be seen in a 2017 memorandum from the U.S. Department of Homeland Security (DHS) which indicates "the surge of illegal immigration at the southern border has overwhelmed federal agencies and resources and has created a significant national security vulnerability to the United States" (Kelly, 2017). As a result, the U.S. House of Representatives Homeland Security Committee passed a $10 billion bill (McCaul, 2017) to "deter, impede, and detect illegal activity" through the use of integrated surveillance and intrusion detection assets such as the Integrated Fixed Tower (IFT) System and the Remote Video Surveillance System (RVSS). IFTs are fixed sensors that provide long-range, persistent surveillance by automatically detecting and tracking targets of interest. Similarly, RVSS assets are fixed sensors that use cameras, radio, and microwave transmitters to "provide short-, medium-, and long-range persistent surveillance mounted on stand-alone towers, or other structures" (Alles et al., 2016). The bill also sets aside $10 million to implement Vehicle and Dismount Exploitation Radars (VADER) in border security operations (McCaul, 2017). Since 2006, unmanned systems equipped with VADER sensors have been credited with interdicting over "13,144 pounds of cocaine and 321,330 pounds of marijuana worth an estimated $1.8 billion" (Alles et al., 2016).

Oriented against aerial threats to border security, ground-based air defense weapons are emplaced as part of an antiaccess/area-denial (A2/AD) strategy to defend against enemy aircraft attempting to penetrate a country's border region during active conflict. Many countries have adopted A2/AD strategies (Schmidt, 2016) and significantly advanced their Surface to Air Missile (SAM) technology. Over the last 10 years, Russia has developed and fielded the S-400 Triumf air defense weapon system which can destroy aerial targets at ranges of 40–400 km (Foss and O'Halloran, 2014). This highly-effective SAM system is capable of engaging the world's most premier aircraft, as well as cruise missiles and ballistic missiles. Recent reports indicate the Russian military currently operates 39 S-400 battalions, with each battalion consisting of eight

* Corresponding author.
E-mail addresses: aaron.lessin@afit.edu (A.M. Lessin), brian.lunday@afit.edu (B.J. Lunday), rayrhill@gmail.com (R.R. Hill).

https://doi.org/10.1016/j.cor.2018.05.017
0305-0548/Published by Elsevier Ltd.

launchers and up to 112 missiles, along with radar systems and a command post (Gady, 2017). China, Turkey, India, and Saudi Arabia have all signed contracts for the purchase of multiple S-400 systems from Russia (TAS, 2017). Motivated by this trend in air defense posturing, in this study we construct an air defense test instance as an illustrative border security application.

Border security is no longer limited to physical borders but now includes virtual, software-defined borders, creating vulnerabilities from the economic market to the energy sector. Due to recent threats "targeting government entities and organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors" the DHS and the Federal Bureau of Investigation (FBI) released an alert "to educate network defenders and enable them to identify and reduce exposure to malicious activity" (DHS, 2017). This emerging threat is not simply a U.S. problem; in December 2015, a cyberattack on the Ukrainian power grid left over 225,000 people without power (Lee et al., 2016). Daniel Tobok, CEO and co-owner of Toronto-based Cytelligence, estimates that cyberattacks "cost Canada $3 billion to $5 billion per year in proceeds to criminals, adding one Calgary energy company was forced to pay $200,000 in ransom three years ago to regain control of its corrupted digital production systems" (Healing, 2017). In his 2017 State of the Union Address, European Commission President Jean-Claude Juncker said that "cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks" (Juncker, 2017).

Common to each of these border security applications is that a defender must decide where to locate a set of assets to prevent an adversary from traversing through a region; the defender's assets may also have differing capabilities to detect or engage the adversary; some defensive assets may be important enough to the defender because of their high cost or limited supply to warrant protection, once emplaced; specific locations of the defended region may require preferential coverage due to their importance; and an adversary will be able to observe the location of defender assets and select a route through the border region to minimize their likelihood of detection.

1.1. Literature review

Our modeling efforts for this research focus on implementing and extending previous work in facility location. Schilling et al. (1993) presented a detailed overview of covering problems in facility location. They classified models as either a Set Covering Problem (SCP) or a Maximal Covering Location Problem (MCLP), where coverage is either required or optimized, respectively. The MCLP was first introduced by Church and ReVelle (1974) to maximize the amount of demand covered within a specified service distance by locating a fixed number of facilities. White and Case (1974) extended the work of Church and ReVelle (1974) by considering equal weights on all demand points. Church (1984) later introduced the MCLP on a planar surface using Euclidean and rectilinear distance measures, where potential facility locations are no longer discrete (and finite).

One of the main assumptions of the MCLP is that coverage is binary. That is, a demand point is either fully covered or not covered at all by a located facility. However, this assumption is often unrealistic. Berman and Krass (2002) extended the MCLP to the Generalized Maximal Covering Location Problem (GMCLP), allowing for "partial coverage of customers, with the degree of coverage being a non-increasing step function of the distance to the nearest facility." Additionally, Berman et al. (2003) extended the GMCLP by way of a gradual covering decay model. Drezner et al. (2004) also solved the gradual covering problem on a planar surface.

Traditional facility location models do not address the need to prevent the passage of an adversary into friendly territory, which is the main concern for border security applications. However, a related field of research pertaining to the location of sensors in a Wireless Sensor Network (WSN) presents coverage models designed specifically for such a purpose. One of the three main coverage problems discussed in WSNs is *barrier coverage* (Cardei and Wu, 2006). In the context of WSNs, "a given belt region is said to be *k-barrier covered* with a sensor network if all crossing paths through the region are *k-covered*, where a crossing path is any path that crosses the width of the region completely" (Kumar et al., 2005). A path is said to be *k-covered* if it intersects at least k sensors' sensing ranges (Huang and Tseng, 2005).

As the defender, the goal of a barrier coverage model is to locate a set of sensors S such that some chosen measure of coverage is maximized. Alternatively, an attacker seeks to interdict or locate areas of the region where the value of the coverage measure is minimized. One such measure of coverage often used in WSN models is *exposure*. First introduced by Meguerdichian et al. (2001b), exposure can informally be thought of as the "expected average ability of observing a target in the sensor field." More formally, exposure is defined as "an integral of a sensing function that generally depends on distance from sensors on a path from a starting point p_S to destination point p_D" (Meguerdichian et al., 2001b). Unlike some coverage metrics, the element of time is important for exposure, since the ability of a sensor to detect a target can improve as the sensing time (i.e., exposure) increases.

For a sensor s, the general sensing model S at an arbitrary point p is:

$$S(s, p) = \frac{\lambda}{[d(s, p)]^K}, \tag{1}$$

where $d(s, p)$ is the Euclidean distance between the sensor s and the point p, and positive constants λ and K are technology-dependent parameters (Meguerdichian et al., 2001b). The parameter λ can be thought of as the energy emitted by a target, and K is an energy decay factor, typically ranging from 2 to 5 (Amaldi et al., 2008).

The *exposure* of an object in the sensor field during the interval $[t_1, t_2]$ along the path $p(t)$ is defined by Meguerdichian et al. (2001b) as:

$$E(p(t), t_1, t_2) = \int_{t_1}^{t_2} I\Big(F, p(t)\Big)\left|\frac{dp(t)}{dt}\right| dt, \tag{2}$$

wherein the sensor field intensity $I(F, p(t))$ is implemented using an *All-Sensor Field Intensity* model or a *Closest-Sensor Field Intensity* model, depending on the application and types of sensors used. The *All-Sensor Field Intensity* model is a summation of the sensing function values (1) from target p to *all* sensors in the sensor network, defined as $I_A(F, p) = \sum_{i=1}^{n} S(s_i, p)$, whereas the *Closest-Sensor Field Intensity* model only utilizes the sensing function value of the *closest* sensor to the target (Meguerdichian et al., 2001b).

Using the definition of exposure, Meguerdichian et al. (2001b) presented an algorithm to find the *minimal exposure path* in a sensor network. The algorithm first transforms the problem into a discrete domain utilizing a generalized grid approach and then creates an edge-weighted graph. The algorithm then applies Dijkstra's single-source shortest-path algorithm (Dijkstra, 1959) to find the minimal exposure path from the source point p_S to the destination point p_D. Meguerdichian et al. (2001c) also extended this initial work by developing a localized minimal exposure path algorithm using Voronoi diagrams.

Understanding that signals traveling from a target to a sensor are often corrupted by noise, Clouqueur et al. (2002) added an Adaptive White Gaussian Noise term $N_i, i = 1, \ldots, n$, to the initial sensor model in Eq. (1). Clouqueur et al. (2002) also pre-