Transportation Research Part E 93 (2016) 71–94

Contents lists available at ScienceDirect

Transportation Research Part E

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

Optimal placement of multiple types of detectors under a small vessel attack threat to port security

Xihong Yan [a], Xiaofeng Nie [b,*]

[a] Higher Education Key Laboratory of Engineering and Scientific Computing, Taiyuan Normal University, Taiyuan 030012, China
[b] School of Mechanical and Aerospace Engineering, Nanyang Technological University, Singapore 639798, Singapore

ARTICLE INFO

Article history:
Received 14 January 2015
Received in revised form 5 May 2016
Accepted 7 May 2016
Available online 30 May 2016

Keywords:
Port security
Small vessel attack
Detector deployment
Exact algorithms

ABSTRACT

We focus on a threat scenario where a terrorist would utilize a small vessel to attack a maritime target. We consider how to place multiple types of detectors to protect maritime targets from such an attack. Detectors are not perfectly reliable. The resulting detector placement problem is formulated as a nonlinear binary integer program such that the expected damage cost caused by the small vessel attack is minimized. Two exact algorithms and a greedy adding heuristic are proposed. Moreover, we conduct a detailed computational study and provide a case study in New York Harbor.

1. Introduction and literature review

Driven by the economic boom in emerging markets, global maritime trade has grown significantly over the years. According to the Review of Maritime Transport 2011 of the United Nations, more than 80% of international trade in goods is being carried by sea and the 2010 international sea-borne trade was estimated to be 8.41 billion tons of goods (United Nations, 2011). As gateways for the movement of such a huge amount of goods, ports play critical roles to facilitate the flow. Since many manufacturing companies use just-in-time distribution systems to lower inventory holding costs, port shutdowns may have catastrophic economic impacts. For example, the closure of 29 U.S. West Coast ports in 2002 was estimated to cost the U.S. economy $1 billion to $2 billion per day (Gaudette, 2002). It was estimated that a nine-month labor dispute at the same 29 ports in 2014–2015 costed Honda 25,000 vehicles in February 2015 (Trott, 2015).

After the tragic terrorist attacks of September 11, 2001, homeland security became a top priority in the U.S. Ports are extremely vulnerable to terrorist attacks due to their characteristics: size, open accessibility by water and land, location in metropolitan areas, the amount of materials being transported, and the ready transportation links to many locations (U.S. GAO, 2002). Because of their strategic importance and criticalness to economy, ports may become potential terrorist targets. Providing an effective and efficient port security system has become one of the primary tasks to safeguard the nation.

One critical threat to port security comes from small vessels. Terrorists have shown a great interest in conducting attacks using small boats. Recently, the small boat threat has regained a lot of media attention, see, for example, USA Today (Frank, 2007), CBS News (CBS News, 2008), and GlobalPost (Neild, 2011). In April 2008, the U.S. Department of Homeland Security (DHS) announced the Small Vessel Security Strategy. In the report, the DHS identified four serious concerns associated with

* Corresponding author.
E-mail address: xiaofengnie@ntu.edu.sg (X. Nie).

http://dx.doi.org/10.1016/j.tre.2016.05.003
1366-5545/

using small vessels in terrorist-related activities: using small vessels as water-borne improvised explosive devices, to smuggle weapons, to smuggle terrorists, and as water-borne platforms to carry out stand-off attacks (U.S. DHS, 2008).

In this paper, we concentrate on the threat scenario where a terrorist would utilize a small vessel as a water-borne improvised explosive device to attack a maritime target (for example, a military vessel, a cruise ship, a passenger ferry, and an oil tanker). Many up-to-date technologies are available to detect the presence of small amounts of radiological, chemical, and biological materials from hundreds of meters away. These devices include fixed-position detectors and mobile sensors. A detailed description of sensors to detect the presence of illicit materials on small boats is provided by Hill (2009). These devices are small and technologically advanced enough to be utilized at ports. For example, the DHS has announced a West Coast Maritime pilot program that involves developing a detection architecture to reduce the risk of threats transported on small vessels (U.S. DHS, 2007). The program is currently underway in Washington's Puget Sound and California's San Diego areas. We consider the situation where the government has collected intelligence information regarding the potential small vessel attack and plans to locate detectors to interdict the small vessel attack. As for the terrorist, he/she subsequently conducts the small vessel attack without knowing detector placement.

Since various technologies (for example, electro-optical, electro-magnetic, radar, and seismic technologies) are involved, different types of detectors have their own costs and detection characteristics (for example, detection rate and effective detection radius). Our paper focuses on how to cost-effectively place multiple types of fixed-position detectors to help protect maritime targets in a port area from a terrorist attack using a small vessel. We assume that detectors are not perfectly reliable and the probability of detection depends not only on the type of the detector but also on how long the small vessel would stay in the detector's effective detection area. The expected damage cost caused by the small vessel attack is minimized while keeping the cost of detectors within a budget limit. The resulting optimization problem is formulated as a nonlinear binary integer program.

In the homeland security literature, many quantitative studies have focused on improving security from different domains, for example, aviation security and border security. In the aviation security domain, Nie et al. (2009a) incorporate joint responses of devices into passenger grouping strategies based on classification theory. Nie et al. (2009b) propose a mixed integer linear program to study how to group passengers with different risk levels. McLay et al. (2010) formulate a sequential stochastic multi-level passenger screening problem as a Markov decision process. Lee and Jacobson (2011) propose three probability-based performance measures for assessing sequential passenger assignment policies. Nie (2011) investigate risk-based grouping for a checked baggage screening system through a cost-effectiveness model. Nikolaev et al. (2012) consider dynamic passenger risk updates in a multi-stage sequential passenger screening problem. Lee and Jacobson (2012) propose three types of estimators for exploring passenger risk uncertainty. Nie et al. (2012) construct a simulation-based selectee lane queueing design framework to determine how to assign passengers with different risk characteristics to a selectee lane. In the border security domain, Morton et al. (2007) propose two types of stochastic network interdiction models for placing radiation sensors at border crossings. For the type under asymmetric information, Sullivan et al. (2014) introduce a smaller and tighter formulation on a bipartite network. Wein et al. (2009) introduce a mathematical optimization model for resource allocation such that a terrorist's likelihood of successfully crossing the U.S.–Mexico border is minimized. Zhang et al. (2011) model a security-check queue at a U.S.–Canada border crossing as a two-stage queueing model.

Most port security literature concentrates on container inspection. A container inspection system consists of a sequence of inspection sensors with different capabilities. Elsayed et al. (2009) focus on determining the threshold levels of inspection sensors and their corresponding sequence simultaneously. The objective is to minimize the overall system cost which includes both inspection and misclassification costs. Young et al. (2010) extend the model to incorporate the time required to complete inspection as another objective. Boros et al. (2009) consider finding container inspection strategies (represented as decision trees) such that the expected per-container-inspection cost is minimized. They develop a large-scale linear programming model based on the polyhedral description of the decision trees. Several evolutionary algorithms are proposed by Ramirez-Marquez (2008), Concho and Ramirez-Marquez (2010), and Van Weele and Ramirez-Marquez (2011). Merrick and McLay (2010) use multiple-objective decision analysis to examine whether screening cargo containers for smuggled nuclear threats is worthwhile. They conclude that the result relies on some key inputs. McLay et al. (2011) propose a risk-based framework to investigate how to define a system alarm. They develop a container reliability knapsack problem which decides what fractions of high-risk and low-risk containers undergo secondary screening. Gaukler et al. (2012) investigate two container inspection policies (a hardness control policy and a hybrid inspection policy) for detecting nuclear materials smuggling. Both policies are shown to perform better than the existing Automated Targeting System based system in most realistic situations. McLay and Dreiding (2012) introduce two linear programming models (a multi-level knapsack screening model and a multi-level threshold knapsack screening model) for detecting nuclear materials in cargo containers. Some structural properties for both models are provided and it is shown through a computational example that enforcing a threshold policy may not result in significant differences.

Some related literature deals with the deployment of detectors in monitoring environments. Chakrabarty et al. (2002) consider determining the placement and type of sensors in a surveillance region such that the cost is minimized while achieving the desired coverage. An integer linear programming model is formulated and a divide-and-conquer approach is proposed for solving large problem instances. Kaplan and Kress (2005) study the operational effectiveness of suicide-bomber detector schemes in two urban environments: a grid model and a plaza model. They conclude that even though suicide bomber sensors could play an important role in the defense of known targets, they may not be effective in random