Ann Oper Res (2011) 187:5–22
DOI 10.1007/s10479-010-0793-z

A Stackelberg game model for resource allocation in cargo container security

Niyazi Onur Bakır

Published online: 22 September 2010

Abstract This paper presents a game theoretic model that analyzes resource allocation strategies against an adaptive adversary to secure cargo container transportation. The defender allocates security resources that could interdict an unauthorized weapon insertion inside a container. The attacker observes the defender's security strategy and chooses a site to insert the weapon. The attacker's goal is to maximize the probability that the weapon reaches its target. The basic model includes a single container route. The results in the basic model suggest that in equilibrium the defender should maintain an equal level of physical security at each site on the cargo container's route. Furthermore, the equilibrium levels of resources to interdict the weapon overseas increase as a function of the attacker's capability to detonate the weapon remotely at a domestic seaport. Investment in domestic seaport security is highly sensitive to the attacker's remote detonation capability as well. The general model that includes multiple container routes suggests that there is a trade-off between the security of foreign seaports and the physical security of sites including container transfer facilities, container yards, warehouses and truck rest areas. The defender has the flexibility to shift resources between non-intrusive inspections at foreign seaports and physical security of other sites on the container route. The equilibrium is also sensitive to the cost effectiveness of security investments.

Keywords Container security · Port security · Border security · Game theory · Risk analysis · Terrorism

1 Introduction

The attacks of September 11, 2001 changed the perception of terrorism risk along the United States (U.S.) borders. Since disrupting economy is a stated goal of al-Qa'ida (see Hoffman 2006), protection of critical nodes of the economy located along the borders has become a priority. U.S. seaports that handle more than 10 million incoming overseas cargo containers

N.O. Bakır (✉)
Department of Industrial Engineering, Bilkent University, Ankara, Turkey 06800
e-mail: nonur@bilkent.edu.tr

each year (see GAO 2008a) are considered to be potential targets of a terrorist attack. As a result, cargo containers that are indispensable conveyors of overseas trade have drawn extra scrutiny during inspections at domestic seaports. However, protection of seaports requires a system-wide approach that allocates security resources at multiple nodes of container movement cutting across international borders. With this recognition, the Department of Homeland Security (DHS) adopted a multi-layered approach to counter terrorism. In this paper, a game theoretic model is discussed to gain insights about how best to allocate resources to protect U.S. seaports against a containerized weapon threat.

1.1 Background

Concerns about a containerized nuclear weapon or a dirty bomb attack are shared among many academic scholars and security experts. The technology curve for building a nuclear weapon may not be high enough to dissuade determined terrorists from building one (see Bunn and Wier 2006; Martin 2007; Allison 2004, 2006; Cooper 2004; Langewiesche 2007; Ferguson 2006 and Maerli et al. 2003). Material to build such weapons of mass disruption are illicitly available as evidenced by International Atomic Energy Agency (IAEA) reports of nuclear smuggling around the globe (IAEA 2006). As described in the Department of Homeland Security National Planning Scenarios released in April 2005 (see DHS 2005), the weapon could be shipped in a container and detonated in a port complex.

Cargo transportation system involves multiple points where containers stop before the delivery at destination. Various programs and initiatives have been developed by the U.S. federal government to reduce the vulnerability at these points and deter terrorists from weaponizing cargo containers. A brief summary of these programs and initiatives is in order. In an effort to bolster security of cargo during loading and transportation phases, the U.S. Bureau of Customs and Border Protection (CBP) introduced the Customs-Trade Partnership against Terrorism initiative. This initiative offers private companies expedited inspections at U.S. borders in return for improving security of their supply-chains. A parallel initiative by CBP, the Container Security Initiative (CSI), deploys non-intrusive inspection and radiation detection equipment at foreign seaports that ship U.S.-bound cargo. Currently, 58 foreign seaports that together handle 86% of inbound overseas cargo (GAO 2008a) are CSI participants. The goal is to examine high risk cargo overseas by non-intrusive technology in the presence of U.S. Customs personnel. The Department of Energy contributes to the overseas non-intrusive inspection activities through its Megaports Initiative in which radiation portals are deployed. The capabilities of Megaports Initiative and CSI were combined in 2006 to meet the goal of scanning 100% of U.S.-bound cargo under the Secure Freight Initiative.

In this paper, 'inspections' refer to the sequence of activities performed at U.S. or international customs to check the contents of cargo containers for discovering illegal radioactive or nuclear material transported over the borders. Inspections include initial screening of cargo manifests and other critical information to assign a risk score to a container, scanning of containers by non-intrusive equipment and physical examinations carried out if the results of the non-intrusive inspections raise suspicion that a threat item is transported. All cargo security initiatives and programs have been introduced to inspect a higher percentage of cargo containers. However, the time required for physical examination of each cargo container renders it impossible to open 100% of all containers. Therefore, the backbone of cargo security initiatives and programs is new security technology. Non-intrusive inspections are made possible by radiation portals, gamma-ray and X-ray scanners, personal radiation detectors and handheld radioactive isotope identification devices. Most cargo containers are scanned by radiation portal monitors at domestic seaports. In addition, high risk cargo is identified by the Automated Targeting System (ATS) that utilizes a complex algorithm and assigns a risk score for each incoming cargo container. ATS uses cargo manifest information submitted 24 hours before the ship leaves the foreign seaport. If a container is identified as high risk, then it goes through X-ray imaging to determine whether a threat item is transported.

1.2 Purpose and past related work

Despite all efforts to improve security of incoming containers at U.S. seaports, vulnerabilities exist. The goal of this paper is to understand how system-wide resource allocation for container security could be improved in an attacker-defender game setting. The interaction between the attacker and the defender is modeled as a Stackelberg game where the defender moves first to allocate security resources followed by an attacker move to send a weapon. Since a single attack scenario is considered, the game ends after the attacker's move. The attacker may exploit the vulnerabilities to the risk of unauthorized tampering or insider help when a container makes a stop at a warehouse, a container yard or a truck rest area. The attacker may choose to insert a weapon at any one of these points in transportation. Under such a scenario, the major policy question from the perspective of the defender is when to interdict the attacker's attempt if the target is a U.S. seaport.

There is a very rich body of literature applying game theory to homeland security problems (see for instance Kardeş 2007 for a review). Only the most recent and relevant work will be mentioned here. Most studies address how the defender should allocate resources among multiple targets to reduce the vulnerability to an attack (see for example Bier et al. 2007; Powell 2007; Golany et al. 2009 and Bier et al. 2008). Vulnerability is defined as the probability of success to the attacker if an attack attempt is made. In Bier et al. (2007), the defender allocates resources under uncertainty about the attacker's valuation of targets whereas in Powell (2007) the defender considers layered defense strategies with complete information about the attacker's payoff. Other studies allow attacker's effort to have impact on targets' vulnerability as well (see Zhuang and Bier 2007 and Major 2002). On the other hand, some Stackelberg game applications focus on protection of a single target through randomized security layers (see Pita et al. 2008 and Paruchuri et al. 2008), and on protection of multiple domains in which multiple attackers may operate (see Paruchuri et al. 2006a, 2006b, 2007).

The rest of this paper is organized as follows. The next section analyzes a simple version of the model where the attacker could attack on a single container route with n sites. Section 3 generalizes this analysis to multiple container routes each with a different number of sites and characterizes some of the important properties of the equilibrium. Some policy implications and further discussion are presented in Sect. 4.

2 Single container route

2.1 The model

Containers move through multiple modes of transportation and are handled by multiple parties before they reach their final destination, which in this paper is a U.S. seaport. They make multiple stops at foreign locations during their transport on highways, railroads or even sea routes. They are vulnerable to tampering at sites on their route where they make stops. Typical sites where containers stop en route are warehouses, container yards, intermodal transfer facilities and truck rest areas. It is incumbent upon the defender, who is the leader

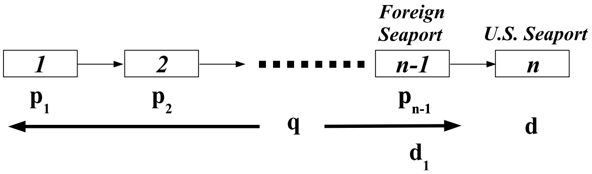

Fig. 1 Container movement and system parameters in a single container route model

in the Stackelberg game considered here, to improve physical security at these sites and to reduce the likelihood of unauthorized tampering. Furthermore, the defender could allocate resources to install in-box sensors that could detect threat items inside containers and to enhance non-intrusive weapon interdiction capabilities at seaports. Each security investment decision introduces another layer of security. The follower in the game is the attacker who can observe the defender's actions and chooses a vulnerable site where a container of choice is tampered. The attacker plans to ship a nuclear weapon targeting a major U.S. seaport. If the nuclear weapon reaches its final target and is successfully detonated, the defender incurs a loss of $e \in \mathbb{R}_+$. A loss of $e \in \mathbb{R}_+$ represents the economic consequences that the defender suffers after a successful attack. The attacker's gain from a successful attack is equal to the defender's loss.

The entire cargo container movement realm is represented as a discrete set of sites where each site is a candidate location for weapon insertion. Figure 1 represents the model for a single container route. A summary of the game based on a single container route is given in Fig. 2. On their route, containers move sequentially starting from site 1 and ending at site n, which a U.S. seaport. Sites 1 to $n-2$ represent warehouses, container yards, intermodal transfer facilities and truck rest areas where each container makes a stop. The last two sites ($n-1$ and n) are the foreign seaport and the domestic seaport, respectively. The single container route model essentially represents the cargo container movement system assuming that every container arriving at the U.S. seaport visits the same sites abroad. It does not represent a system in which only one container moves. Instead, multiple containers move on the same route, and any one of these containers could be selected for weapon insertion by the attacker while it visits some site $i' \in \{1, \dots, n-1\}$. In other words, the attacker can choose to insert the weapon into an arbitrary container at one of the sites from 1 to $n-1$. The defender, in a leader role, does not observe the choice of i'. Hence, the defender implements physical security measures (i.e., install video cameras, build fences or employ guards) at each site $i \in \{1, \dots, n-1\}$ to interdict the attacker if an attempt to insert the weapon is made at site i. In Fig. 1, p_i is the probability that the attacker's attempt to insert a weapon at site i is interdicted with physical security measures implemented at the site.

Physical security at sites 1 to $n-1$ is the first layer of security. The second layer is in-box sensor technology. The defender could equip all cargo containers with in-box sensor technology as discussed in Cohen (2006). Even if the attacker successfully inserts the weapon into a container, the attempt could later be detected with sensor technologies installed inside this container. The probability of interdiction with sensor technology is q. Note that, q does not depend on where the weapon is inserted. Non-intrusive technology deployed at foreign and domestic seaports constitute the third and fourth layers of security, respectively. Non-intrusive equipment deployed at seaports include gamma-ray and X-ray scanners, radiation portal monitors, personal radiation detectors and other handheld detection devices. This paper does not focus on optimal inspection strategies employed at seaports. Other studies discuss optimal inspection strategies that utilize a series of non-intrusive scanners (see Elsayed et al. 2007; Boros et al. 2006 and Wein et al. 2006), and their operational impacts (see Bakshi et al. 2009). At a foreign seaport, the probability of interdiction is d_1. On the

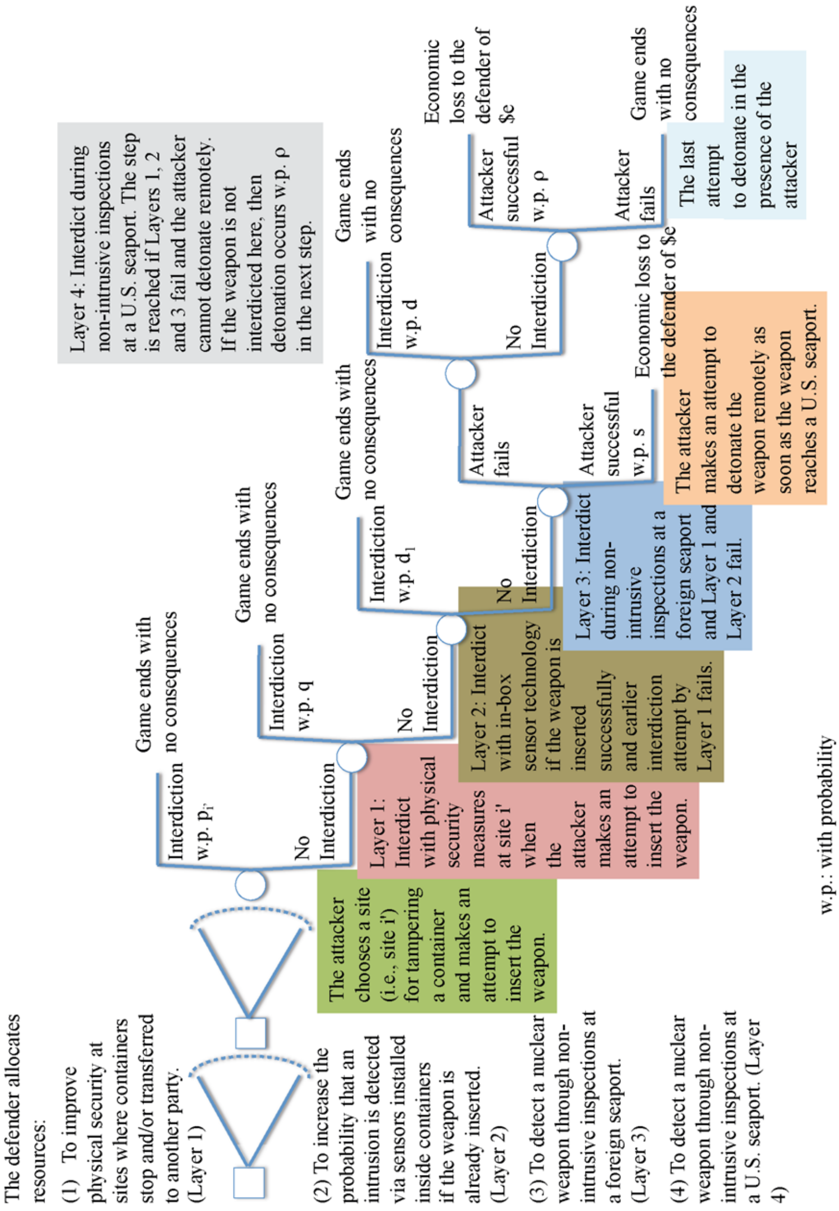
The defender allocates resources:
(1) To improve physical security at sites where containers stop and/or transferred to another party. (Layer 1)
(2) To increase the probability that an intrusion is detected via sensors installed inside containers if the weapon is already inserted. (Layer 2)
(3) To detect a nuclear weapon through non-intrusive inspections at a foreign seaport. (Layer 3)
(4) To detect a nuclear weapon through non-intrusive inspections at a U.S. seaport. (Layer 4)
The attacker chooses a site (i.e., site i') for tampering a container and makes an attempt to insert the weapon.
Interdiction w.p. $p_{i'}$
Game ends with no consequences
No Interdiction
Layer 1: Interdict with physical security measures at site i' when the attacker makes an attempt to insert the weapon.
Interdiction w.p. q
Game ends with no consequences
No Interdiction
Layer 2: Interdict with in-box sensor technology if the weapon is inserted successfully and earlier interdiction attempt by Layer 1 fails.
Interdiction w.p. d_1
Game ends with no consequences
No Interdiction
Layer 3: Interdict during non-intrusive inspections at a foreign seaport and Layer 1 and Layer 2 fail.
Attacker fails
Attacker successful w.p. s
Economic loss to the defender of $e
The attacker makes an attempt to detonate the weapon remotely as soon as the weapon reaches a U.S. seaport.
Interdiction w.p. d
Game ends with no consequences
No Interdiction
Layer 4: Interdict during non-intrusive inspections at a U.S. seaport. The step is reached if Layers 1, 2 and 3 fail and the attacker cannot detonate remotely. If the weapon is not interdicted here, then detonation occurs w.p. ρ in the next step.
Attacker successful w.p. ρ
Economic loss to the defender of $e
Attacker fails
Game ends with no consequences
The last attempt to detonate in the presence of the attacker
w.p.: with probability

Fig. 2 A summary of the player moves and the events in the Stackelberg game in the case of a single container route

other hand, the parameter d is defined for the probability of interdiction at a domestic seaport.

The weapon can reach its target at a U.S. seaport if and only if interdiction through the first three security layers fail. When the weapon reaches a U.S. seaport, the attacker makes an attempt to detonate the weapon remotely before inspections take place. This attempt succeeds with probability s. In case the remote detonation attempt fails, the attacker makes a second attempt after the inspections and this attempt is assumed to succeed with probability ρ. The second attempt is assumed to be made in the presence of the attacker. Hence, $\rho > s$. As such, π_i, the probability that the attacker successfully executes the attack after inserting the weapon at site i is calculated as:

$$\begin{aligned}\pi_i &= P(\text{Weapon inserted at site } i) \cdot P(\text{No detection by in-box sensor technology})\\ &\quad \cdot P(\text{No detection at a foreign seaport}) \cdot \big[P(\text{Successful remote detonation})\\ &\quad + P(\text{Remote detonation fails}) \cdot P(\text{No detection at a U.S. seaport})\\ &\quad \cdot P(\text{Successful detonation in the presence of an attacker})\big]\\ &= (1-p_i)\cdot(1-q)\cdot(1-d_1)\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big].\end{aligned}$$

Better security does not come free to the defender. The defender incurs a cost $c(p_i)$ to maintain an interdiction probability p_i at site i. Hence, we assume that the probability of success to the attacker solely depends on the defender's effort to improve security at site i. Bier et al. (2007) uses a logarithmic function to express this relationship (i.e. $c(p_i) = -\ln(1-p_i)$). For analytical convenience, we use a reciprocal function for the cost of improving physical security at site i, which is $c(p_i) = (1/(1-p_i)^{\alpha_i}) - 1$. This reciprocal function captures some of the nice properties of the logarithmic function used in Bier et al. (2007) such as

$$c(0) = 0, \qquad c' > 0, \qquad c'' > 0 \quad \text{and} \quad \lim_{p_i \to 1} c(p_i) = +\infty.$$

The condition on c'' is a mathematical statement of the assumption that it should get more difficult to increase p_i further at higher values of p_i. In addition, the parameter α_i is introduced to model the impact of technology. Through parameter α_i, we establish the relationship between the marginal cost of maintaining an interdiction probability p_i based on the effectiveness of the technology in use. Note that, $c'(p_i) = \alpha_i/(1-p_i)^{(\alpha_i+1)}$ which is increasing in α_i. The higher the value of α_i is, the higher is the cost of maintaining p_i and the marginal cost of increasing p_i. Therefore, a high value of α_i models a rather ineffective technology where the defender should incur a high cost of maintaining p_i. Another convenience of the reciprocal function is that the empirical estimation of α_i can be made through linear regression. Estimation of p_i is more difficult because it may require an extensive evaluation by the subject matter experts on the potential ways to breach a given level of physical security.

The reciprocal function is used for modeling the cost for other layers as well. The cost of installing in-box sensor technology is $c(q) = (1/(1-q)^{\beta}) - 1$. Non-intrusive technology cost has different technology parameters for the foreign and the domestic seaport. In particular, $c(d_1) = (1/(1-d_1)^{\gamma_1}) - 1$ and $c(d) = (1/(1-d)^{\gamma}) - 1$. In response to the defender resource allocation strategy, the attacker chooses to insert the weapon at site i' where $\pi_{i'} = \max_{i\in\{1,\dots,n-1\}} \pi_i$. Then, by multiplying $\pi_{i'}$ with e, the economic consequences after a successful attack, we compute the expected payoff to the risk neutral attacker by choosing site i' as $\pi_{i'} \cdot e$. The defender knows the attacker's objective as well and chooses the

Table 1 Summary of notation

p_i	The probability that the attacker's attempt to insert a weapon at site i is interdicted.
q	The probability that the weapon is detected by in-box sensor technology.
d_1	The probability that non-intrusive inspections at a foreign seaport detect the weapon.
d	The probability that inspections at a domestic seaport detect the weapon.
e	Loss incurred by the defender if the weapon is detonated.
$c(p_i)$	Cost of maintaining p_i at site i.
$c(q)$	Cost of maintaining q through in-box sensors.
$c(d_1)$	Cost of maintaining d_1 at a foreign seaport.
$c(d)$	Cost of maintaining d at a domestic seaport.
α_i	Technology parameter in $c(p_i)$.
β	Technology parameter in $c(q)$.
γ_1	Technology parameter in $c(d_1)$.
γ	Technology parameter in $c(d)$.
π_i	The probability that the attacker successfully executes the attack after inserting the weapon at site i.
s	The probability that the weapon is successfully detonated remotely at a U.S. seaport.
ρ	The probability that the weapon is successfully detonated in the presence of the attacker at a U.S. seaport.

resource allocation strategy to minimize the sum of the total cost of technology and the expected attack consequences

$$L(p_1, p_2, \dots, p_{n-1}, q, d_1, d) = \sum_{j=1}^{n-1} c(p_i) + c(q) + c(d_1) + c(d) + \pi_{i'} \cdot e. \tag{1}$$

Since it is easy to characterize the attacker's strategy, the rest of the discussion focuses on the defender's objective function in (1). Note that, $\pi_z \geq \pi_l$ if $(1 - p_z) \geq (1 - p_l)$, or $p_l \geq p_z$. Table 1 lists the notation that has been introduced so far in the context of a single container route. In what follows, we focus first on the analysis of the problem with a single container route including n sites (see Fig. 1). In Sect. 3, the model is generalized to include multiple container routes, all leading to a target U.S. seaport.

2.2 Characterization of the equilibrium

In the single container route case, the defender's problem can be written as,

$$\begin{aligned} &L(p_1, p_2, \dots, p_{n-1}, q, d_1, d) \\ &\quad = \sum_{j=1}^{n-1} \frac{1}{(1-p_j)^{\alpha_i}} + \frac{1}{(1-q)^{\beta}} + \frac{1}{(1-d_1)^{\gamma_1}} + \frac{1}{(1-d)^{\gamma}} \\ &\qquad + (1-p_{i'}) \cdot (1-q) \cdot (1-d_1) \cdot \big[s + (1-s) \cdot (1-d) \cdot \rho\big] \cdot e, \\ &\qquad \text{s.t.} \quad p_j \geq p_{i'} \quad \forall j \neq i' \text{ and } j \in \{1, \dots, n-1\}. \end{aligned} \tag{2}$$

It is possible to obtain an analytical solution to this non-linear problem, albeit without any closed-form expressions for the optimal levels of decision variables. The first derivatives of $L(\cdot)$ with respect to the decision variables are,

$$
\begin{aligned}
\frac{\partial L}{\partial p_j} &= \alpha_j \cdot (1-p_j)^{-(\alpha_j+1)} \quad \forall j \neq i' \text{ and } j \in \{1,\dots,n-1\},\\
\frac{\partial L}{\partial p_{i'}} &= \alpha_{i'} \cdot (1-p_{i'})^{-(\alpha_{i'}+1)} - (1-q)\cdot(1-d_1)\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]\cdot e,\\
\frac{\partial L}{\partial q} &= \beta \cdot (1-q)^{-(\beta+1)} - (1-p_{i'})\cdot(1-d_1)\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]\cdot e,\\
\frac{\partial L}{\partial d_1} &= \gamma_1 \cdot (1-d_1)^{-(\gamma_1+1)} - (1-p_{i'})\cdot(1-q)\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]\cdot e,\\
\frac{\partial L}{\partial d} &= \gamma \cdot (1-d)^{-(\gamma+1)} - (1-p_{i'})\cdot(1-q)\cdot(1-d_1)\cdot(1-s)\cdot\rho\cdot e.
\end{aligned}
\tag{3}
$$

First order conditions imply $\frac{\partial L}{\partial p_{i'}} = \frac{\partial L}{\partial q} = \frac{\partial L}{\partial d_1} = \frac{\partial L}{\partial d} = 0$ at equilibrium. Since $\frac{\partial L}{\partial p_j} > 0 \; \forall j \neq i'$ and $j \in \{1,\dots,n-1\}$, the unconstrained optimum is $p_j = 0$. However, the constraint dictates $p_j = p_{i'}$. The next proposition proves that the solution characterized by these properties is indeed the equilibrium.

Proposition 1 *Let $(p^*_{i'}, p^*_j \; \forall j \neq i', q^*, d^*_1, d^*)$ denote the equilibrium values of the associated decision variables. Then, the equilibrium in the Stackelberg game between the attacker and the defender in the case of a single container route satisfies,*

$$
\begin{gathered}
\alpha_{i'} \cdot \big(1-p^*_{i'}\big)^{-\alpha_{i'}} = \beta \cdot \big(1-q^*\big)^{-\beta} = \gamma_1 \cdot \big(1-d^*_1\big)^{-\gamma_1},\\
\gamma \cdot \big(1-d^*\big)^{-(\gamma+1)} = \big(1-p^*_{i'}\big)\cdot\big(1-q^*\big)\cdot\big(1-d^*_1\big)\cdot(1-s)\cdot\rho\cdot e,\\
p^*_j = p^*_{i'} \quad \forall j \neq i' \textit{ and } j \in \{1,\dots,n-1\},
\end{gathered}
\tag{4}
$$

Proof The optimal solution to the non-linear optimization problem in (2) is the equilibrium solution to the Stackelberg game, and the first order conditions of the problem imply the functional relationships in (4). Hence, the proof requires the second-order sufficiency condition that the Hessian of the objective function is positive definite. Since the objective function is separable in $p_{i'}$ and p_j's where $j \neq i'$ and $j \in \{1,\dots,n-1\}$, the Hessian includes only the second-order derivatives with respect to variables $p_{i'}$, q, d_1 and d. Hence, the Hessian H is

$$
\begin{bmatrix}
\partial^2 L/\partial p^2_{i'} & \partial^2 L/\partial p_{i'}\partial q & \partial^2 L/\partial p_{i'}\partial d_1 & \partial^2 L/\partial p_{i'}\partial d\\
\partial^2 L/\partial q\partial p_{i'} & \partial^2 L/\partial q^2 & \partial^2 L/\partial q\partial d_1 & \partial^2 L/\partial q\partial d\\
\partial^2 L/\partial d_1\partial p_{i'} & \partial^2 L/\partial d_1\partial q & \partial^2 L/\partial d^2_1 & \partial^2 L/\partial d_1\partial d\\
\partial^2 L/\partial d\partial p_{i'} & \partial^2 L/\partial d\partial q & \partial^2 L/\partial d\partial d_1 & \partial^2 L/\partial d^2
\end{bmatrix}.
$$

There are several ways to prove that Hessian is positive definite. The particular method here is to show that all the upper left submatrices have positive determinants. First, $\partial^2 L/\partial p^2_{i'} = \alpha_{i'} \cdot (1+\alpha_{i'}) \cdot (1-p_{i'})^{-(\alpha_{i'}+2)} > 0$. Second, the 2×2 upper left submatrix determinant is

$$\begin{aligned}&\partial^2 L/\partial p_{i'}^2 \cdot \partial^2 L/\partial q^2 - \left(\partial^2 L/\partial p_{i'}\partial q\right)^2\\ &\quad = \alpha_{i'} \cdot (1+\alpha_{i'}) \cdot (1-p_{i'})^{-(\alpha_{i'}+2)} \cdot \beta \cdot (\beta+1) \cdot (1-q)^{-(\beta+2)}\\ &\qquad - (1-d_1)^2 \cdot \left[s + (1-s)\cdot(1-d)\cdot\rho\right]^2 \cdot e^2\\ &\quad = (1-d_1)^2 \cdot \left[s+(1-s)\cdot(1-d)\cdot\rho\right]^2 \cdot e^2 \cdot \left((\alpha_{i'}+1)\cdot(\beta+1)-1\right) > 0.\end{aligned}$$

Since the computation of the determinant of the 3 × 3 upper left submatrix and the entire Hessian matrix is long, it is presented in the Appendix. Both determinants are positive. Hence the stationary point as described by the first order conditions is a minimizer. This completes the proof. □

The result in Proposition 1 has interesting implications. First, it states that in equilibrium the probability of successful weapon insertion should be the same at each site. If unequal security standards are implemented, then the attacker should exploit the vulnerabilities at the least secure site (for example a cargo transfer facility) to insert the weapon rendering the security measures at other sites ineffective. As discussed in Sect. 1, the Department of Homeland Security introduced the Customs-Trade Partnership against Terrorism (C-TPAT) initiative to incentivize companies to improve physical supply-chain security by offering less scrutinized inspections at the border. The program was criticized in 2005 by the Government Accountability Office due to weaknesses in validation of security profiles submitted by the participating companies (see GAO 2005b and GAO 2005a). In particular, it was reported that the site visits which are required to validate the implementation of security measures are challenged by staffing shortages and lack of criteria to determine the relevance of selected sites for the security of container movement. While a later report in 2008 (GAO 2008b) praises the Customs and Border Protection (CBP) agency for the improvements made, weaknesses still exist in validating security measures at supply-chain sites. The result in Proposition 1 strongly recommends equal security standards at sites where containers are loaded and transported. Hence, CBP should continue its efforts to visit foreign sites on a regular basis to ensure a minimum level of security.

The equilibrium results of the model recommend balanced spending on each layer of security. However, there is a trade-off between dollars spent on each layer. For example, in comparing the value of physical security of supply-chain sites and in-box sensor technology, the technology effectiveness parameters $\alpha_{i'}$ and β are crucial. If $\alpha_{i'} > \beta$, then in equilibrium,

$$\left(1-q^*\right)^{-\beta} > \left(1-p_{i'}^*\right)^{-\alpha_{i'}}$$

which implies $1-p_{i'}^* > 1-q^*$, or $q^* > p_{i'}^*$. As such, in equilibrium the defender maintains a higher probability of interdiction using in-box sensor technology when $\alpha_{i'} > \beta$. This follows because the marginal cost of improving interdiction capability in any security layer is increasing in the value of the technology parameter.

Another major implication is on the effectiveness of non-intrusive inspection technology. The value of non-intrusive technology at domestic seaports depends largely on the attacker choice of a target. If the attacker chooses to detonate the weapon at a major seaport, then there is a chance that the detonation occurs before the non-intrusive inspections. This reduces the value of non-intrusive inspections at domestic seaports. In equilibrium of this model we have,

$$\gamma \cdot \left(1-d^*\right)^{-(\gamma+1)} = \left(1-p_{i'}^*\right) \cdot \left(1-q^*\right) \cdot \left(1-d_1^*\right) \cdot (1-s) \cdot \rho \cdot e. \tag{5}$$

If the probability of detonation before inspections at a domestic seaport is high (i.e., s is high on the right hand side of (5)), then the corresponding solution to d^* in (5) is low. In other words, the defender should focus on non-intrusive technology at domestic seaports if the attacker's remote detonation capability is not sophisticated enough to pose a high threat to national security. Conversely, the first order conditions for other major parameters are,

$$\begin{aligned}
&\alpha_{i'} \cdot \left(1-p_{i'}^*\right)^{-(\alpha_{i'}+1)} = \left(1-q^*\right)\cdot\left(1-d_1^*\right)\cdot\left[s+(1-s)\cdot\left(1-d^*\right)\cdot\rho\right]\cdot e,\\
&\beta \cdot \left(1-q^*\right)^{-(\beta+1)} = \left(1-p_{i'}^*\right)\cdot\left(1-d_1^*\right)\cdot\left[s+(1-s)\cdot\left(1-d^*\right)\cdot\rho\right]\cdot e,\\
&\gamma_1 \cdot \left(1-d_1^*\right)^{-(\gamma_1+1)} = \left(1-p_{i'}^*\right)\cdot\left(1-q^*\right)\cdot\left[s+(1-s)\cdot\left(1-d^*\right)\cdot\rho\right]\cdot e.
\end{aligned} \tag{6}$$

In (6), the right hand sides of all the equations are increasing in s. Similarly, the left sides are increasing in the model's decision variables (i.e., the left hand side of the first equation in (6) is increasing in $p_{i'}^*$, the second equation is increasing in q^* and the third equation is increasing in d_1^*). This indicates an opposite relationship between the attacker's capability of remote detonation and the probability of detection at earlier stages of container movement. If the attacker is believed to have a high remote detonation capability, then more emphasis should be placed on interdiction before the weapon reaches U.S. shores.

Finally, a similar analysis of (5) and (6) suggest that the defender should maintain a higher level of security at each layer if the expected economic consequences of a terrorist attack are high. The sensitivity of the equilibrium probability of interdiction at each layer to perturbations in expected economic consequences depend on the level of security at other layers. If the security level at other layers is already high, then sensitivity to a change in expected economic consequences is relatively low.

3 The general model

Suppose now that there are an arbitrary number of container routes in the system (see Fig. 3) all ending at one U.S. seaport. Similar to the single container route case, there are multiple containers moving through the system. However, in this section we drop the assumption that all containers move on the same route visiting the same sites. We should restate one modeling assumption here, though. Terrorists make an attempt to insert one nuclear device in a container transported to a U.S. seaport at a site of their choice where containers en route to the U.S. make a stop. The defender's goal is to interdict the tampered container. However, the defender does not know a priori the site of weapon insertion and thus the route the tampered container uses to arrive at U.S. Hence, the defender has to consider improving security at all the sites where containers en route to the U.S. make stops.

Containers may arrive at the U.S. seaport from one of the t foreign seaports. Associated with each foreign seaport $i \in \{1,\dots,t\}$, there are a total of $m(i)$ separate container routes. As such, a container may use either one of the $m(i)$ routes to arrive at foreign seaport i. Each route is identified with the two-tuple (j,i) where $j \in \{1,\dots,m(i)\}$ and $i \in \{1,\dots,t\}$. Similar to the single container route case, on each route (j,i), there are a total of $n(j,i)$ sites that a container makes stops and hence is vulnerable to tampering. The attacker can choose to insert the weapon at any site (k,j,i), where $k \in \{1,\dots,n(j,i)\}$, $j \in \{1,\dots,m(i)\}$ and $i \in \{1,\dots,t\}$. In addition, the attacker has the option to insert the weapon at one of the t seaports. In Fig. 3, the notation used to identify a foreign seaport $i \in \{1,\dots,t\}$ is $(k,j,i) = (0,0,i)$.

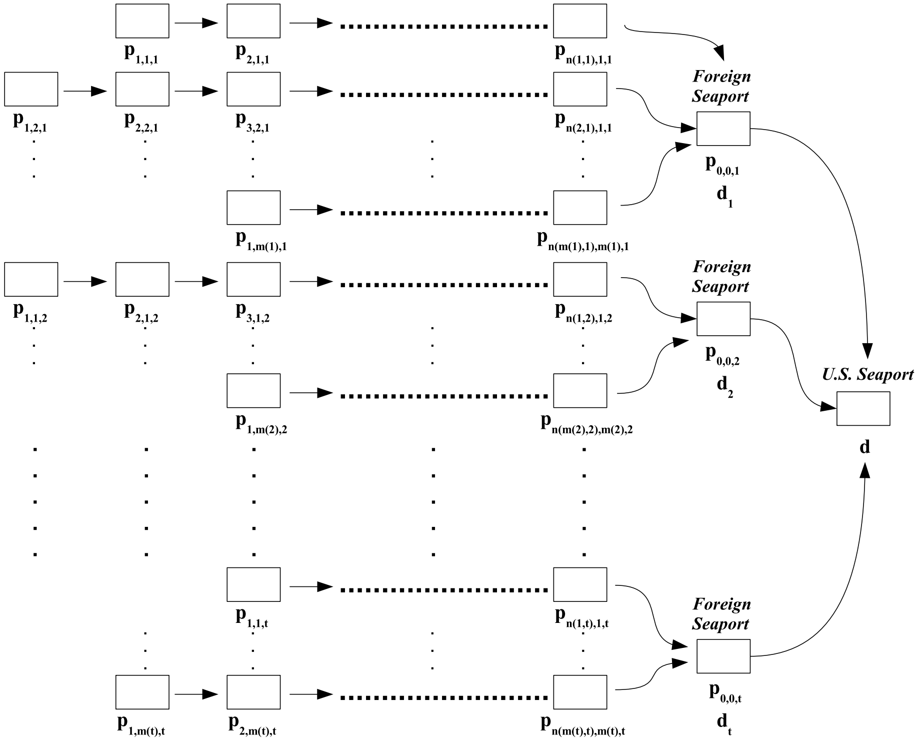

Fig. 3 Container movement and system parameters in a model with multiple container routes

The probability of interdicting the attacker's attempt to insert a weapon at site (k, j, i) is denoted by p_{kji}. In plain words, p_{kji} is the probability of interdicting an attacker attempt to insert the weapon at the kth stop that the container makes as it is transported on the jth route that eventually leads to foreign seaport i. When $k, j = 0$, the interpretation is much simpler. Then, p_{00i} is the probability of interdicting weapon insertion while a container makes a stop at foreign seaport i. Parallel to the single container route case, the cost of improving physical security at site (k, j, i) is expressed as a function of p_{kji} as $c(p_{kji}) = (1/(1-p_{kji})^{\alpha_{kji}}) - 1$. Again, the parameter α_{kji} models the impact of technology. At a foreign seaport i, $1 \le i \le t$, the cost of non-intrusive technology is $c(d_i) = (1/(1-d_i)^{\gamma_i}) - 1$ where d_i is the probability of interdiction and γ_i is the technology parameter. The cost functions for layers 2 and 4 are exactly the same under this case. The attacker has a strategy in equilibrium to maximize the probability of a successful attack by selecting an arbitrary container for weapon insertion and tampering this container at site (k^o, j^o, i^o) where,

$$\pi_{k^o j^o i^o} = \max_{\substack{k^o \in \{0,\ldots,n(j^o,i^o)\} \\ j^o \in \{0,\ldots,m(i^o)\}, i^o \in \{1,\ldots,t\}}} \pi_{kji}.$$

The expected payoff to the risk neutral attacker by choosing site (k^o, j^o, i^o) is $\pi_{k^o j^o i^o} \cdot e$. The defender knows the attacker's objective as well and allocates resource to minimize the probability of success to the attacker. Despite the generalization, the defender's problem is quite similar to (2),

$$\begin{aligned}L(p_{kji}, q, d_i, d) = {} & \sum_{i=1}^{t}\left[\left[\sum_{j=0}^{m(i)}\sum_{k=0}^{n(j,i)}\frac{1}{(1-p_{kji})^{\alpha_{kji}}}\right]+\frac{1}{(1-d_i)^{\gamma_i}}\right] \\ & + \frac{1}{(1-q)^{\beta}}+\frac{1}{(1-d)^{\gamma}}+(1-p_{k^o j^o i^o})\cdot(1-q)\cdot(1-d_{i^o}) \\ & \cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]\cdot e, \\ \text{s.t.}\quad & \pi_{k^o j^o i^o} \ge \pi_{kji} \quad \forall(k,j,i)\ne\big(k^o,j^o,i^o\big),\ i\in\{1,\dots,t\}, \\ & j\in\big\{0,\dots,m(i)\big\},\ k\in\big\{0,\dots,n(j,i)\big\}.\end{aligned} \tag{7}$$

Parameters q and d denote exactly the same quantities as in the previous section. The attacker strategy to insert the weapon at site (k^o, j^o, i^o) renders non-intrusive inspections at the foreign seaport i^o critical. In equilibrium, d_{i^o} is the detection probability during non-intrusive inspections at the foreign seaport that is on the weaponized container's route. The problem in the general multiple container route case is quite similar except the probability constraint. The first order derivatives are

$$\begin{aligned}\frac{\partial L}{\partial p_{kji}} &= \alpha_{kji}\cdot(1-p_{kji})^{-(\alpha_{kji}+1)} \quad \forall(k,j,i)\ne\big(k^o,j^o,i^o\big),\ i\in\{1,\dots,t\}, \\ & \qquad j\in\big\{0,\dots,m(i)\big\},\ k\in\big\{0,\dots,n(j,i)\big\}, \\ \frac{\partial L}{\partial p_{k^o j^o i^o}} &= \alpha_{k^o j^o i^o}\cdot(1-p_{k^o j^o i^o})^{-(\alpha_{k^o j^o i^o}+1)}-(1-q)\cdot(1-d_{i^o}) \\ & \quad \cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]\cdot e, \\ \frac{\partial L}{\partial q} &= \beta\cdot(1-q)^{-(\beta+1)}-(1-p_{k^o j^o i^o})\cdot(1-d_{i^o})\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]\cdot e, \\ \frac{\partial L}{\partial d_{i^o}} &= \gamma_{i^o}\cdot(1-d_{i^o})^{-(\gamma_{i^o}+1)}-(1-p_{k^o j^o i^o})\cdot(1-q)\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]\cdot e, \\ \frac{\partial L}{\partial d_i} &= \gamma_i\cdot(1-d_i)^{-(\gamma_i+1)} \quad \forall i\ne i^o, \\ \frac{\partial L}{\partial d} &= \gamma\cdot(1-d)^{-(\gamma+1)}-(1-p_{k^o j^o i^o})\cdot(1-q)\cdot(1-d_{i^o})\cdot(1-s)\cdot\rho\cdot e.\end{aligned} \tag{8}$$

The equilibrium values for decision variables are given in the next proposition.

Proposition 2 *Let* $(p^*_{k^o j^o i^o}, p^*_{kji}\ \forall(k,j,i)\ne(k^o,j^o,i^o), q^*, d^*_{i^o}, d^*_i\ \forall i\ne i^o, d^*)$ *denote the equilibrium values of the associated decision variables. The equilibrium in the Stackelberg game between the attacker and the defender in the general case satisfies*,

$$\begin{aligned}& \alpha_{k^o j^o i^o}\cdot\big(1-p^*_{k^o j^o i^o}\big)^{-\alpha_{k^o j^o i^o}} = \beta\cdot\big(1-q^*\big)^{-\beta} = \gamma_{i^o}\cdot\big(1-d^*_{i^o}\big)^{-\gamma_{i^o}}, \\ & \gamma\cdot\big(1-d^*\big)^{-(\gamma+1)} = \big(1-p^*_{k^o j^o i^o}\big)\cdot\big(1-q^*\big)\cdot\big(1-d^*_{i^o}\big)\cdot(1-s)\cdot\rho\cdot e, \\ & \big(1-p^*_{k^o j^o i^o}\big)\cdot\big(1-d^*_{i^o}\big)\ge\big(1-p^*_{kji}\big)\cdot\big(1-d^*_i\big) \quad \forall i\ne i^o, \\ & p^*_{kji^o}\ge p^*_{k^o j^o i^o}, p^*_{k^o ji^o}\ge p^*_{k^o j^o i^o}, p^*_{kj^o i^o}\ge p^*_{k^o j^o i^o} \quad \forall(k,j,i)\ne\big(k^o,j^o,i^o\big),\ i\in\{1,\dots,t\}, \\ & \quad j\in\big\{0,\dots,m(i)\big\},\ k\in\big\{0,\dots,n(j,i)\big\}.\end{aligned} \tag{9}$$

Proof The proof for the equilibrium values of $p_{k^o j^o i^o}$, d_{i^o}, q and d is similar to the proof of Proposition 1. These are the only parameters for which the first order derivatives in (8) are equal to zero in equilibrium. Therefore, the major step in this proof is to show the positive definiteness of the 4 × 4 Hessian for four variables as in the proof of Proposition 1,

$$\begin{bmatrix} \partial^2 L/\partial p^2_{k^o j^o i^o} & \partial^2 L/\partial p_{k^o j^o i^o}\partial q & \partial^2 L/\partial p_{k^o j^o i^o}\partial d_{i^o} & \partial^2 L/\partial p_{k^o j^o i^o}\partial d \\ \partial^2 L/\partial q\partial p_{k^o j^o i^o} & \partial^2 L/\partial q^2 & \partial^2 L/\partial q\partial d_{i^o} & \partial^2 L/\partial q\partial d \\ \partial^2 L/\partial d_{i^o}\partial p_{k^o j^o i^o} & \partial^2 L/\partial d_{i^o}\partial q & \partial^2 L/\partial d^2_{i^o} & \partial^2 L/\partial d_{i^o}\partial d \\ \partial^2 L/\partial d\partial p_{k^o j^o i^o} & \partial^2 L/\partial d\partial q & \partial^2 L/\partial d\partial d_{i^o} & \partial^2 L/\partial d^2 \end{bmatrix}.$$

Positive definiteness of this Hessian is proved similarly as in the Appendix.

For other variables, we use the constraints $\pi_{k^o j^o i^o} \geq \pi_{kji}$ $\forall(k,j,i) \neq (k^o, j^o, i^o)$, $i \in \{1,\dots,t\}$, $j \in \{0,\dots,m(i)\}$ and $k \in \{0,\dots,n(j,i)\}$. As in the proof of Proposition 1, the unconstrained minimum of variables such as p_{kji}, $\forall(k,j,i) \neq (k^o, j^o, i^o)$, $i \in \{1,\dots,t\}$, $j \in \{0,\dots,m(i)\}$, $k \in \{0,\dots,n(j,i)\}$ and d_i, $i \neq i^o$ is zero. However, since $\pi_{k^o j^o i^o} \geq \pi_{kji}$ $\forall(k,j,i) \neq (k^o, j^o, i^o)$, $i \in \{1,\dots,t\}$, $j \in \{0,\dots,m(i)\}$ and $k \in \{0,\dots,n(j,i)\}$, their respective equilibrium values have to satisfy the constraints given in (9). Note that the constraints in (9) should be satisfied to ensure that the attacker does not deviate from the equilibrium strategy of inserting the weapon at site (k^o, j^o, i^o). In other words, the probability of success to the attacker after inserting the weapon at site (k^o, j^o, i^o) should be greater or equal to the probability of success after inserting the weapon elsewhere. □

In the general model, the physical security of sites on each container route is not necessarily at a uniform level. When there is a single container route, the probability of interdiction at each site is the same. With multiple container routes, we observe that a similar result holds on container routes leading to the foreign seaport that the weaponized container visits. On other parallel routes, the physical security level is dependent on the status of non-intrusive inspection capabilities at the foreign seaport. For example, consider the site (k,j,i), $i \neq i^o$. Any container that visits site (k,j,i) arrives at the foreign seaport i by definition. Then, p_{kji} and d_i satisfy,

$$\left(1 - p^*_{k^o j^o i^o}\right) \cdot \left(1 - d^*_{i^o}\right) \geq \left(1 - p^*_{kji}\right) \cdot \left(1 - d^*_i\right)$$

in equilibrium. This inequality is satisfied in equilibrium because, by definition, inserting the weapon at (k^o, j^o, i^o) should maximize the probability of success to the attacker. If this condition is not imposed, then both p_{kji} and d_i would be zero in equilibrium. It suggests a trade-off between the physical security of sites on the container route and non-intrusive inspection capabilities at a foreign seaport. If non-intrusive inspection technology is used effectively at a foreign seaport i (i.e., d_i is high), then physical security of sites that lead into i should be less of a concern and vice versa (i.e., p_{kji} is relatively low).

The general model confirms the insights gained in the single container route problem as well. The original single container route model and its expanded version discussed in this section do not fully identify the site chosen by the attacker for weapon insertion. Further assumptions have to be made on technology parameters of the model to completely identify the equilibrium strategies. Such an attempt is not made here because precise estimates of these parameters which could help determine the exact functional relationships are difficult to obtain. Most relevant information is classified. Bakır (2008) provides some estimates and ranges based on open source information without defining any functional relationships, albeit for southwestern border crossings. Nevertheless, the results of the paper provide a very good sketch of what the equilibrium should look like.

4 Conclusion

Port security has been a major theme in homeland security since the attacks upon the World Trade Center and the Pentagon. Terrorists may target ports mainly because of their economic significance as well as their close proximity to urban centers. Unfortunately, terrorists have a variety of options to carry out an attack. The Department of Homeland Security has been doing its part to reduce the likelihood of such a successful attack by enhancing cargo and physical security. Despite significant progress since September 11, loopholes are still reported to exist. This paper addresses cargo related aspects of port security and analyzes the resource allocation problem across various layers of the container transportation.

The results of the general model provide some insights about an effective defense against an adaptive adversary. The attacker's strategy is to maximize the probability of a successful attack. Hence, the choice of location for weapon insertion should be where the physical security could be breached most easily. In response, the defender has to maintain an equal security level at container transfer facilities, loading stations, warehouses and truck rest areas on the most vulnerable container route to maximize the return on investment. Security on other container routes should be balanced between non-intrusive inspections at foreign seaports and physical security. In this regard, the defender has some flexibility in allocating security resources as well. If increasing non-intrusive inspection capability overseas is an effective way to detect weapons of mass disruption, physical security of sites visited during land transportation may receive less emphasis. However, if the implementation of non-intrusive inspections overseas face challenges due to local concerns of slower port operations, physical security in land transportation becomes crucial to cargo container security.

The model accounts for the possibility of an attack before the authorities get a chance to inspect the container at the domestic port. This reduces the effectiveness of domestic seaport security. The value of improving security at domestic ports depends on the probability that the attacker can detonate the weapon remotely soon after the containerized weapon reaches its target. A higher probability of success for the attacker reduces equilibrium probability of interdiction maintained at a domestic seaport. In this case, the defender should shift resources to improve early interdiction capabilities.

Vulnerability of each location on the container route and the change in the probability of interdiction for a given amount of security spending vary. Nevertheless, the results provide valuable insights. The Department of Homeland Security recognizes the adaptive nature of terrorists. With this recognition, various programs and initiatives have been introduced over the years. However, high number of inbound containers and the difficulty in enforcing security standards at foreign sites may in practice make it difficult to implement optimal resource allocation decisions. A coordinated and a sincere effort by all nations and the private sector is required to implement high security standards to reduce the threat.

Acknowledgements The author thanks Garrett Asay, Erim Kardeş and Heather Rosoff for insightful discussions on the topic of the paper. The author also thanks the anonymous reviewers and the editors. This research was supported in part by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number 2007-ST-061-000001. However, any opinions, findings and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security.

Appendix

Proof of Proposition 1 The determinant of the 3 × 3 upper left submatrix and the entire Hessian is computed as follows. First, the 3 × 3 upper left submatrix is

$$\begin{bmatrix} \partial^2 L/\partial p_{i'}^2 & \partial^2 L/\partial p_{i'}\partial q & \partial^2 L/\partial p_{i'}\partial d_1 \\ \partial^2 L/\partial q\partial p_{i'} & \partial^2 L/\partial q^2 & \partial^2 L/\partial q\partial d_1 \\ \partial^2 L/\partial d_1\partial p_{i'} & \partial^2 L/\partial d_1\partial q & \partial^2 L/\partial d_1^2 \end{bmatrix}.$$

The determinant is

$$\begin{aligned}
&\partial^2 L/\partial p_{i'}^2 \cdot \big[\partial^2 L/\partial q^2 \cdot \partial^2 L/\partial d_1^2 - \big(\partial^2 L/\partial q\partial d_1\big)^2\big] - \partial^2 L/\partial p_{i'}\partial q \cdot \big[\partial^2 L/\partial q\partial p_{i'} \cdot \partial^2 L/\partial d_1^2 \\
&\quad - \partial^2 L/\partial q\partial d_1 \cdot \partial^2 L/\partial d_1\partial p_{i'}\big] + \partial^2 L/\partial p_{i'}\partial d_1 \cdot \big[\partial^2 L/\partial q\partial p_{i'} \cdot \partial^2 L/\partial d_1\partial q \\
&\quad - \partial^2 L/\partial q^2 \cdot \partial^2 L/\partial d_1\partial p_{i'}\big] \\
&\ = \alpha_{i'} \cdot (\alpha_{i'} + 1) \cdot (1 - p_{i'})^{-(\alpha_{i'}+2)} \cdot \big[\beta \cdot (\beta + 1) \cdot (1 - q)^{-(\beta+2)} \\
&\quad \cdot \gamma_1 \cdot (\gamma_1 + 1) \cdot (1 - d_1)^{-(\gamma_1+2)} - (1 - p_{i'})^2 \cdot \big[s + (1 - s) \cdot (1 - d) \cdot \rho\big]^2 \cdot e^2\big] \\
&\quad - (1 - d_1) \cdot \big[s + (1 - s) \cdot (1 - d) \cdot \rho\big] \cdot e \cdot \big[(1 - d_1) \cdot \big[s + (1 - s) \cdot (1 - d) \cdot \rho\big] \cdot e \cdot \gamma_1 \\
&\quad \cdot (\gamma_1 + 1) \cdot (1 - d_1)^{-(\gamma_1+2)} - (1 - p_1) \cdot \big[s + (1 - s) \cdot (1 - d) \cdot \rho\big]^2 \cdot e^2 \cdot (1 - q)\big] \\
&\quad + (1 - q) \cdot \big[s + (1 - s) \cdot (1 - d) \cdot \rho\big] \cdot e \cdot \big[(1 - d_1) \cdot \big[s + (1 - s) \cdot (1 - d) \cdot \rho\big]^2 \\
&\quad \cdot e^2 \cdot (1 - p_{i'}) - \beta \cdot (\beta + 1) \cdot (1 - q)^{-(\beta+1)} \cdot \big[s + (1 - s) \cdot (1 - d) \cdot \rho\big] \cdot e\big].
\end{aligned}$$

Using first order conditions $\frac{\partial L}{\partial p_{i'}} = \frac{\partial L}{\partial q} = \frac{\partial L}{\partial d_1} = \frac{\partial L}{\partial d} = 0$, and simplifying the expression

$$\begin{aligned}
&= (1 - d_1) \cdot (1 - q) \cdot (1 - p_{i'}) \cdot \big[s + (1 - s) \cdot (1 - d) \cdot \rho\big]^3 \cdot e^3 \\
&\quad \cdot [\alpha_{i'}\beta\gamma_1 + \alpha_{i'}\beta + \alpha_{i'}\gamma_1 + \beta\gamma_1],
\end{aligned}$$

which is positive. Next, the determinant of the entire Hessian is

$$\begin{aligned}
&\frac{\partial^2 L}{\partial p_{i'}^2} \cdot \frac{\partial^2 L}{\partial q^2} \cdot \left(\frac{\partial^2 L}{\partial d_1^2} \cdot \frac{\partial^2 L}{\partial d^2} - \left(\frac{\partial^2 L}{\partial d_1\partial d}\right)^2\right) \\
&\quad - \frac{\partial^2 L}{\partial p_{i'}^2} \cdot \frac{\partial^2 L}{\partial q\partial d_1} \cdot \left(\frac{\partial^2 L}{\partial d_1\partial q} \cdot \frac{\partial^2 L}{\partial d^2} - \frac{\partial^2 L}{\partial d_1\partial d} \cdot \frac{\partial^2 L}{\partial d\partial q}\right) \\
&\quad + \frac{\partial^2 L}{\partial p_{i'}^2} \cdot \frac{\partial^2 L}{\partial q\partial d} \cdot \left(\frac{\partial^2 L}{\partial d_1\partial q} \cdot \frac{\partial^2 L}{\partial d_1\partial d} - \frac{\partial^2 L}{\partial d_1^2} \cdot \frac{\partial^2 L}{\partial d\partial q}\right) \\
&\quad - \left(\frac{\partial^2 L}{\partial p_{i'}\partial q}\right)^2 \cdot \left(\frac{\partial^2 L}{\partial d_1^2} \cdot \frac{\partial^2 L}{\partial d^2} - \left(\frac{\partial^2 L}{\partial d_1\partial d}\right)^2\right) \\
&\quad + \frac{\partial^2 L}{\partial p_{i'}\partial q} \cdot \frac{\partial^2 L}{\partial q\partial d_1} \cdot \left(\frac{\partial^2 L}{\partial d_1\partial p_1} \cdot \frac{\partial^2 L}{\partial d^2} - \frac{\partial^2 L}{\partial d_1\partial d} \cdot \frac{\partial^2 L}{\partial d\partial p_1}\right) \\
&\quad - \frac{\partial^2 L}{\partial p_{i'}\partial q} \cdot \frac{\partial^2 L}{\partial q\partial d} \cdot \left(\frac{\partial^2 L}{\partial d_1\partial p_{i'}} \cdot \frac{\partial^2 L}{\partial d\partial d_1} - \frac{\partial^2 L}{\partial d_1^2} \cdot \frac{\partial^2 L}{\partial d\partial p_{i'}}\right)
\end{aligned}$$

$$\begin{aligned}
&+\frac{\partial^2 L}{\partial p_{i'}\partial d_1}\cdot\frac{\partial^2 L}{\partial q\partial p_{i'}}\cdot\left(\frac{\partial^2 L}{\partial d_1\partial q}\cdot\frac{\partial^2 L}{\partial d^2}-\frac{\partial^2 L}{\partial d_1\partial d}\cdot\frac{\partial^2 L}{\partial d\partial q}\right)\\
&-\frac{\partial^2 L}{\partial p_{i'}\partial d_1}\cdot\frac{\partial^2 L}{\partial q^2}\cdot\left(\frac{\partial^2 L}{\partial d_1\partial p_{i'}}\cdot\frac{\partial^2 L}{\partial d^2}-\frac{\partial^2 L}{\partial d_1\partial d}\cdot\frac{\partial^2 L}{\partial d\partial p_{i'}}\right)\\
&+\frac{\partial^2 L}{\partial p_{i'}\partial d_1}\cdot\frac{\partial^2 L}{\partial q\partial d}\cdot\left(\frac{\partial^2 L}{\partial d_1\partial p_{i'}}\cdot\frac{\partial^2 L}{\partial d\partial q}-\frac{\partial^2 L}{\partial d_1\partial q}\cdot\frac{\partial^2 L}{\partial d\partial p_{i'}}\right)\\
&-\frac{\partial^2 L}{\partial p_{i'}\partial d}\cdot\frac{\partial^2 L}{\partial q\partial p_{i'}}\cdot\left(\frac{\partial^2 L}{\partial d_1\partial q}\cdot\frac{\partial^2 L}{\partial d\partial d_1}-\frac{\partial^2 L}{\partial d_1^2}\cdot\frac{\partial^2 L}{\partial d\partial q}\right)\\
&+\frac{\partial^2 L}{\partial p_{i'}\partial d}\cdot\frac{\partial^2 L}{\partial q^2}\cdot\left(\frac{\partial^2 L}{\partial d_1\partial p_{i'}}\cdot\frac{\partial^2 L}{\partial d\partial d_1}-\frac{\partial^2 L}{\partial d_1^2}\cdot\frac{\partial^2 L}{\partial d\partial p_{i'}}\right)\\
&-\frac{\partial^2 L}{\partial p_{i'}\partial d}\cdot\frac{\partial^2 L}{\partial q\partial d_1}\cdot\left(\frac{\partial^2 L}{\partial d_1\partial p_{i'}}\cdot\frac{\partial^2 L}{\partial d\partial q}-\frac{\partial^2 L}{\partial d_1\partial q}\cdot\frac{\partial^2 L}{\partial d\partial p_{i'}}\right).
\end{aligned}$$

Using $f(p_{i'})=(1-p_{i'})^{-(\alpha_{i'}+2)}$, $g(q)=(1-q)^{-(\beta+2)}$, $h(d_1)=(1-d_1)^{-(\gamma_1+2)}$, and $t(d)=(1-d)^{-(\gamma+2)}$, the determinant expression is

$$\begin{aligned}
&=\alpha_{i'}\cdot(\alpha_{i'}+1)\cdot f(p_{i'})\cdot\beta\cdot(\beta+1)\cdot g(q)\cdot\gamma_1\cdot(\gamma_1+1)\cdot h(d_1)\cdot\gamma\cdot(\gamma+1)\cdot t(d)\\
&\quad+2\cdot\alpha_{i'}\cdot(\alpha_{i'}+1)\cdot f(p_{i'})\cdot(1-p_{i'})^3\cdot(1-s)^2\cdot\rho^2\cdot(1-q)\cdot(1-d_1)\\
&\quad\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]\cdot e^3\\
&\quad+2\cdot\gamma\cdot(\gamma+1)\cdot t(d)\cdot(1-p_{i'})\cdot(1-q)\cdot(1-d_1)\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]^3\cdot e^3\\
&\quad+2\cdot\gamma_1\cdot(\gamma_1+1)\cdot h(d_1)\cdot(1-p_{i'})\cdot(1-s)^2\cdot\rho^2\cdot(1-q)\cdot(1-d_1)^3\\
&\quad\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]\cdot e^3\\
&\quad+2\cdot\beta\cdot(\beta+1)\cdot g(q)\cdot(1-p_{i'})\cdot(1-s)^2\cdot\rho^2\cdot(1-q)^3\cdot(1-d_1)\\
&\quad\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]\cdot e^3\\
&\quad-3\cdot(1-p_{i'})^2\cdot(1-s)^2\cdot\rho^2\cdot(1-q)^2\cdot(1-d_1)^2\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]^2\cdot e^4\\
&\quad-\alpha_{i'}\cdot(\alpha_{i'}+1)\cdot f(p_{i'})\cdot\beta\cdot(\beta+1)\cdot g(q)\cdot(1-p_{i'})^2\cdot(1-s)^2\cdot\rho^2\cdot(1-q)^2\cdot e^2\\
&\quad-\alpha_{i'}\cdot(\alpha_{i'}+1)\cdot f(p_{i'})\cdot\gamma\cdot(\gamma+1)\cdot t(d)\cdot(1-p_{i'})^2\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]^2\cdot e^2\\
&\quad-\alpha_{i'}\cdot(\alpha_{i'}+1)\cdot f(p_{i'})\cdot\gamma_1\cdot(\gamma_1+1)\cdot h(d_1)\cdot(1-p_{i'})^2\cdot(1-s)^2\cdot\rho^2\cdot(1-d_1)^2\cdot e^2\\
&\quad-\gamma_1\cdot(\gamma_1+1)\cdot h(d_1)\cdot\gamma\cdot(\gamma+1)\cdot t(d)\cdot(1-d_1)^2\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]^2\cdot e^2\\
&\quad-\beta\cdot(\beta+1)\cdot g(q)\cdot\gamma\cdot(\gamma+1)\cdot t(d)\cdot(1-q)^2\cdot\big[s+(1-s)\cdot(1-d)\cdot\rho\big]^2\cdot e^2\\
&\quad-\beta\cdot(\beta+1)\cdot g(q)\cdot\gamma_1\cdot(\gamma_1+1)\cdot h(d_1)\cdot(1-q)^2\cdot(1-s)^2\cdot\rho^2\cdot(1-d_1)^2\cdot e^2.
\end{aligned}$$

Beyond this point, major steps of this computation include the use of first order conditions to simplify the expression to obtain,

$$\begin{aligned}
\det(H)&=(\alpha_{i'}\gamma_1\beta\gamma+\alpha_{i'}\gamma_1\beta+\alpha_{i'}\gamma_1\gamma+\alpha_{i'}\beta\gamma+\gamma_1\beta\gamma)\cdot(1-p_{i'})^2\cdot(1-q)^2\\
&\quad\cdot(1-d_1)^2\cdot(1-s)\cdot\rho\cdot\Big(\big[s+(1-s)\cdot(1-d)\cdot\rho\big]^3/(1-d)\Big)\cdot e^4
\end{aligned}$$

$$+ (\alpha_{i'}\beta + \alpha_{i'}\gamma_1 + \gamma_1\beta) \cdot \big[(1-p_{i'})^2 \cdot (1-q)^2 \cdot (1-d_1)^2 \cdot (1-s) \cdot \rho \\ \cdot \big(\big[s + (1-s) \cdot (1-d) \cdot \rho\big]^3/(1-d)\big) \cdot e^4 - (1-p_{i'})^2 \cdot (1-q)^2 \\ \cdot (1-d_1)^2 \cdot (1-s)^2 \cdot \rho^2 \cdot \big[s + (1-s) \cdot (1-d) \cdot \rho\big]^2 \cdot e^4\big].$$

The first term is positive. The second term is also positive if and only if the term in brackets is also positive. One can rewrite the term in the brackets as,

$$(1-p_{i'})^2 \cdot (1-q)^2 \cdot (1-d_1)^2 \cdot (1-s) \cdot \rho \cdot \big[s + (1-s) \cdot (1-d) \cdot \rho\big]^2 \cdot e^4 \\ \cdot \big(\big(\big[s + (1-s) \cdot (1-d) \cdot \rho\big]/(1-d)\big) - (1-s) \cdot \rho\big). \tag{10}$$

It is easy to see that (10) is also positive because $([s + (1-s) \cdot (1-d) \cdot \rho]/(1-d)) > (1-s) \cdot \rho$. This proves that the Hessian is positive definite. □

References

Allison, G. (2004). *Nuclear terrorism*. New York: Times Books.

Allison, G. (2006). The will to prevent. *Harvard International Review*, *28*(3), 50–55.

Bakır, N. O. (2008). A decision tree model for evaluating countermeasures to secure cargo at United States southwestern ports of entry. *Decision Analysis*, *5*(4), 230–248.

Bakshi, N., Flynn, S. E., & Gans, N. (2009). *Estimating the operational impact of container inspections at international ports* (Working Paper No. 2009-05-01). The Wharton School Risk Management and Decision Processes Center.

Bier, V. M., Oliveros, S., & Samuelson, L. (2007). Choosing what to protect: Strategic defensive allocation against an unknown attacker. *Journal of Public Economic Theory*, *9*(4), 563–587.

Bier, V. M., Haphuriwat, N., Menoyo, J., Zimmerman, R., & Culpen, A. M. (2008). Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Analysis*, *28*(3), 763–770.

Boros, E., Fedzhora, L., Kantor, P. B., Saeger, K., & Stroud, P. (2006). *Large scale LP model for finding optimal container inspection strategies* (Rutcor Research Report No. RRR-26-2006).

Bunn, M., & Wier, A. (2006). Terrorist nuclear weapon construction: How difficult? *The Annals of the American Academy of Political and Social Science*, *607*(1), 133–149.

Cohen, S. S. (2006). Boom boxes: Containers and terrorism. In J.D. Haveman & H.J. Shatz (Eds.), *Protecting the nation's seaports: Balancing security and cost* (pp. 91–128).

Cooper, M. H. (2004). Nuclear proliferation and terrorism. *CQ Researcher*, *14*(13), 297–320.

DHS (2005). National planning scenarios: Executive summaries. http://cees.tamiu.edu/covertheborder/TOOLS/NationalPlanningSen.pdf.

Elsayed, E. A., Young, C. M., Xie, M., Zhang, H., & Zhu, Y. (2007). *Port-of-entry inspection: Sensor deployment policy optimization* (Rutgers IE Working Paper 07-012).

Ferguson, C. D. (2006). *Preventing catastrophic nuclear terrorism*. Council on Foreign Relations Special Report, Washington, DC.

GAO (2005a). *Cargo security: Partnership program grants importers reduced scrutiny with limited assurance of improved security*. U.S. Government Accountability Office, GAO-05-404, Washington, DC.

GAO (2005b). *Homeland security: Key cargo security programs can be improved*. U.S. Government Accountability Office, GAO-05-466T, Washington, DC.

GAO (2008a). *Supply chain security: Examinations of high-risk cargo at foreign seaports have increased, but improved data collection and performance measures are needed*. U.S. Government Accountability Office, GAO-08-187, Washington, DC.

GAO (2008b). *U.S. customs and border protection has enhanced its partnership with import trade sectors, but challenges remain in verifying security practices*. U.S. Government Accountability Office, GAO-08-240, Washington, DC.

Golany, B., Kaplan, E. H., Marmur, A., & Rothblum, U. G. (2009). Nature plays with dice—terrorists do not: Allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research*, *192*(1), 198–208.

Hoffman, B. (2006). *The use of the Internet by Islamic extremists*. RAND Testimony, Santa Monica, CA.

IAEA (2006). *Illicit trafficking and other unauthorized activities involving nuclear and radioactive materials*. IAEA 2005 Fact Sheet.

Kardeş, E. (2007). *Discounted robust stochastic games with applications to homeland security and flow control*. Ph.D. Dissertation, University of Southern California.

Langewiesche, W. (2007). *The atomic bazaar*. New York: Farrar, Straus and Giroux.

Maerli, B. M., Schaper, A., & Barnaby, F. (2003). The characteristics of nuclear terrorist weapons. *American Behavioral Scientist*, *46*(6), 727–744.

Major, J. A. (2002). Advanced techniques for modeling terrorism risk. *Journal of Risk Finance*, *4*(1), 15–24.

Martin, B. (2007). Nuclear power and antiterrorism: Obscuring the policy contradictions. *Prometheus*, *25*(1), 19–29.

Paruchuri, P., Tambe, M., Ordóñez, F., & Kraus, S. (2006a). Increasing security through communication and policy randomization in multiagent systems. In *Proceedings of the AAMAS-2006 conference*, Hakodate, Japan.

Paruchuri, P., Tambe, M., Ordóñez, F., & Kraus, S. (2006b). Security in multiagent systems by policy randomization. In *Proceedings of the AAMAS-2006 conference*, Hakodate, Japan.

Paruchuri, P., Pearce, J., Tambe, M., Ordóñez, F., & Kraus, S. (2007). An efficient heuristic approach for security against multiple adversaries. In *Proceedings of the AAMAS-2007 Conference*, Honolulu, HI.

Paruchuri, P., Pearce, J., Marecki, J., Tambe, M., Ordóñez, F., & Kraus, S. (2008). Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games. In *Proceedings of the AAMAS-2008 conference*, Estoril, Portugal.

Pita, J., Jain, M., Marecki, J., Ordóñez, F., Portway, C., Tambe, M., Western, C., Paruchuri, P., & Kraus, S. (2008). Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles international airport. In *Proceedings of the AAMAS-2008 conference*, Estoril, Portugal.

Powell, R. (2007). Defending against terrorist attacks with limited resources. *The American Political Science Review*, *101*(3), 527–541.

Wein, L. M., Wilkins, A. H., Baveja, M., & Flynn, S. E. (2006). Preventing the importation of illicit nuclear materials in shipping containers. *Risk Analysis*, *26*(5), 1377–1393.

Zhuang, J., & Bier, V. M. (2007). Balancing terrorism and natural disasters—Defensive strategy with endogenous attacker effort. *Operations Research*, *55*(5), 976–991.