Economics of Transportation 16 (2018) 21–28

Contents lists available at ScienceDirect

Economics of Transportation

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

A game theory model for freight service provision security investments for high-value cargo

Anna Nagurney[a,*], Shivani Shukla[b], Ladimer S. Nagurney[c], Sara Saberi[d]

[a] *Department of Operations and Information Management, Isenberg School of Management, University of Massachusetts, Amherst, MA, 01003, USA*
[b] *Department of Business Analytics and Information Systems, School of Management, University of San Francisco, San Francisco, CA, 94117-1080, USA*
[c] *Department of Electrical and Computer Engineering, University of Hartford, West Hartford, CT, 06117, USA*
[d] *Foisie School of Business, Worcester Polytechnic Institute, Worcester, MA, 01609-2280, USA*

ARTICLE INFO

Keywords:
Security
Freight
Networks
High-value cargo
Game theory
Variational inequalities
Security policy

ABSTRACT

In this paper, we develop a game theory model in which freight service providers seek to maximize their expected utility by competing for business from shippers and also investing in security. The focus is on high-value cargo, which has been the target of attacks globally. Shippers reflect their preferences for freight service providers through the prices they are willing to pay which depend on quantities shipped and security levels invested in. The Nash Equilibrium is formulated as a variational inequality problem for which existence is guaranteed. Numerical examples illustrate the framework and give essential freight security investment policy related information.

1. Introduction

Effective freight services, as critical service components of supply chains, are essential to the transportation and delivery of products from points of origin to destinations. Shippers expect their goods to arrive in their entirety, in good condition, and in a timely manner. Nevertheless, according to Heyn (2014), the US Federal Bureau of Investigation reports that, each year, approximately $30 billion worth of cargo is lost, with estimates of cargo theft reaching record highs in 2012. Cargo theft is not limited to the continental United States, however, and, in Europe, cargo theft increased 24 percent in 2012, and rose in Asia as well (Terry (2014)). The greatest risk of cargo theft currently exists in Brazil, Mexico, and South Africa, often via hijacking.

High-value products, in particular, which can range from high tech equipment to precious metals and jewelry and certain fashion and other luxury items, alcohol and high-end food products, as well as pharmaceuticals, are especially attractive targets for theft while in transit. High-value goods have always required extra security, but recently several factors have increased the risk. As the world's appetite for luxury goods grows, sourcing and marketing locations have become more spread out and diverse with longer supply chains adding touch points and, hence, increasing vulnerability (Terry (2014)). Indeed, as global trade expands, companies are faced with greater security challenges, and to illustrate the scope of issues, observe that more than 200 million containers are shipped between the world's seaports annually (Closs and McGarrell (2004)), with the United States receiving approximately 19.6 million containers in 2014, which corresponds to about 53,700 per day (see World Shipping Council (2016)). In addition, crime organizations are increasingly focused on goods in transit. Furthermore, localized disruptions such as severe weather, political unrest, and natural disasters can also increase risk by idling high-value cargo. Holiday seasons, such as the period of Christmas and New Year's, and even the July 4th holiday, pose additional challenges because of increased cargo thefts in the US (cf. Kilcarr (2015)). In 2016, incidents involving theft of full truckload continued as the most prevalent method of theft during the third quarter in the United States, with 78% of all reported thefts, recording an average loss value of over $120,000, according to FreightWatch (see Cole (2016)).

According to Weiss (2016), cargo thefts in Europe, the Middle East, and Africa have almost tripled in the past five years, based on data reported by the Transport Asset Protection Association (TAPA). To illustrate the breadth of high-value goods that have been targets of thefts, according to TAPA, and, as reported in Weiss (2016), in recent months, criminals have absconded with salmon worth 100,000 euros ($112,000) from a trailer in Norway, 80 cases of whiskey from a vehicle near London, and truckloads of nuts worth $10 million in more than 30 incidents. 85% of all major cargo theft involves trucks, according to TAPA, with such thefts costing businesses more than $10 billion

* Corresponding author.
E-mail address: nagurney@isenberg.umass.edu (A. Nagurney).

https://doi.org/10.1016/j.ecotra.2018.09.002
Received 1 July 2017; Received in revised form 14 September 2018; Accepted 26 September 2018

annually worldwide (Brown (2013)). TAPA was initially established to protect shipments of electronic goods but criminals are also diversifying as to the products that they steal and the Internet is making it easier to fence the pilfered items. In addition, some freight thieves are becoming cybercriminals, impersonating companies, and engaging in fictitious pickups and redirected deliveries (cf. Morris (2015)).

Shippers, as noted by Meixell and Norbis (2012) (see also Rinehart et al. (2004)), can reduce security-related negative impacts by selecting security-conscious carriers, which we refer to here as freight service providers (FSPs), who, in turn, must decide on the best mode and route choices from the origin node where the goods are picked up from to the destination points, where the goods are delivered to. Voss et al. (2006) also argue that security practices are an important criterion in carrier selection. Of course, shippers also consider price in making a decision as to the carrier or freight service provider (cf. Meixell and Norbis (2008), Nagurney et al. (2015a,b), and the references therein). Moreover, to keep cargo safe, freight service provider companies may use teams of drivers, GPS tracking technology, and remote vehicle disabling in transit, as examples of possible security measures (Heyn (2014)).

Investing in security is, nevertheless, costly (see, e.g., Russell and Saldanha (2003)). Hence, FSPs must take their security investments into consideration when pricing for their services. Peleg-Gillai et al. (2006), in their investigations of 11 manufacturers from a variety of industries and 3 freight service providers, considered to be innovators in the area of supply chain security, determined that the vast majority of companies were able to realize many benefits from their security investments, with some of them reaching very significant levels. Based on these inputs, the authors concluded that investments in supply chain security can help organizations to improve internal operations, strengthen relationships with their customers, and increase, in general, their profitability.

Shippers, these days, including those dealing with high-value products, have a spectrum of FSPs that they can select from, with examples in the United States including UPS, FedEx, DHL, Ryder, Schneider, Brink's, etc. FSPs, in turn, compete for the shippers' business and security is increasingly an essential requirement to shippers. Thefts of high-value products may result in incurred damages and insurance may be insufficient to cover the losses. Plus, a freight service provider's reputation may be at stake with negative publicity associated with thefts which can affect future business prospects. An overview of cargo theft and supply chain security, from a practitioner standpoint, can be found in the book by Burges (2013). Ekwall (2012) provides an excellent overview of supply chain security issues and possible solutions. The edited volume of Wagner and Bode (2009) contains interesting contributions to security and risk with a focus on logistics service providers.

According to the Federal Bureau of Investigation, cargo theft is a $15 billion to $30 billion a year problem (FleetOwner (2016)). Such thefts are indication of a much larger and a more pressing issue of inconsistencies in perception of cargo theft along a supply chain. There are multiple stakeholders in this complex network that involves multiple modes as well. In addition to coordination and collaboration, these stakeholders also need to communicate their issues, best practices, and security related activities to withstand the decentralized, diffused, and evolving threats they are facing. While transportation security administration and related authorities have been building standards and regulations to improve security, much of the onus lies on the FSPs. Since in our paper we focus on the security measures adopted by freight service providers and the willingness to pay for their services being sensitive to those measures, we focus on how the investments into security can affect their overall security policies.

Generally, FSPs employ experienced investigators and surveillance personnel to monitor shipments closely at all times. They also use technology with bar-code and internet-based tracking systems to follow the shipment as long as it is in their possession. These measures would determine the security levels we discuss in this paper. Investments into these security measures ultimately determine the individual FSPs and, thus, the entire networks vulnerability. The policies and mandates set by the governmental authorities can get complemented by smart security investments at the operational level by stakeholders in the supply chain. In this paper, we discuss the implications of security investments by FSPs.

Gould et al. (2010), in their review of the literature on security and supply chain management to that date, note that topics such as passing on the costs of security to customers as well as understanding security performance, and supply chain benefits, is an area for future research. Meixell and Norbis (2012), in their review of carrier selection and supplier selection, and in motivating their integrated supplier and carrier selection model with a focus on security, observe that not much research has been devoted to including supply chain security measures into either carrier or supplier choice decision models. Their work provides an elegant multi-objective optimization framework based on a single buyer.

We emphasize that several frameworks expanding the breadth of the freight modeling literature, but not focused on security, have been utilized to-date. A summarized literature review of the work until 1985 is provided in Harker (1985). The majority of the literature until then focused on one or two shipper or carrier problems in an intercity freight transportation system with subsequent advances including the contributions of Harker and Friesz (1986a,b), Dafermos and Nagurney (1987), Harker (1988), Miller et al. (1991), Hurley and Petersen (1994), Forkenbrock (1999), Fernandez et al. (2003), Agrawal and Ziliaskopoulos (2006), Xiao and Yang (2007), Xu and Holguin-Veras (2009), and Lin and Huang (2017), with freight network equilibrium utilized by most of these authors. Spatial price equilibrium, in turn, has been employed by Florian and Los (1982), Friesz et al. (1983), and Dafermos and Nagurney (1987), among others. In addition, as noted by Lee et al. (2014), Stackelberg games have been used for evaluating sequential decision-making (see, e.g., Miller et al. (1991), Xiao and Yang (2007)). There has also been work in the coopetition (competition and cooperation) space of freight network equilibrium (Lin et al. (2017)) as well as in the context of supply chain network equilibrium (cf. Nagurney (2006), Saberi et al. (2018), and the references therein).

The model that we develop in this paper fills gaps in the literature in several ways. We develop a game theory model consisting of FSPs who compete with one another as to the quantity of the high-value product that they will transport from origin locations to destinations. The shippers, in turn, reflect their preferences for transport of the high-value cargo through the prices that they are willing to pay, which depend on the quantities carried as well as the investment in security by the FSPs. We posit security investment cost functions, which the FSPs encumber, if they invest in security, and include the probability of an attack on the logistics/transport links, and the associated damages. Each FSP seeks to maximize his expected utility associated with the quantities that he transports as well as his investment in security, which may differ for different links. The governing Nash Equilibrium (1950, 1951) conditions are then shown to satisfy a variational inequality problem for which existence is guaranteed. Conditions for uniqueness are provided and an algorithmic scheme proposed, which yields closed form expressions at each iteration in the quantity shipments as well as the security levels to be invested in. The fact that we demonstrate, for a computable model, sensitivity to capturing security in a freight network of high value cargo, show how shippers reflect their preferences, and how investments by FSPs can affect their businesses in an equilibrium setting (and not optimization), is among our contributions.

Although there is a rich body of literature on game theory models for homeland security (cf. Kardes (2007) for a review), the modeling of security in supply chain contexts, as already noted earlier, is limited, and, even more so, for security associated with freight service provision investments. Bakir (2011) considers a defender and attacker engaged in a game regarding cargo container transportation. Gkonis and Psaraftis (2010), earlier, developed a game theory model with discrete choices