November 2017

Game Theory for Security Investments in Cyber and Supply Chain Networks

Shivani Shukla

GAME THEORY FOR SECURITY INVESTMENTS IN CYBER AND SUPPLY CHAIN NETWORKS

A Dissertation Presented

by

SHIVANI SHUKLA

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

September 2017

Isenberg School of Management

GAME THEORY FOR SECURITY INVESTMENTS IN CYBER AND SUPPLY CHAIN NETWORKS

A Dissertation Presented

by

SHIVANI SHUKLA

Approved as to style and content by:

____

Anna Nagurney, Chair

____

Hari Jagannathan Balasubramanian, Member

____

Eric Gonzales, Member

____

Adams Steven, Member

____

George R.Milne, Program Director
Isenberg School of Management

To Anila Shukla, Gautam Shukla, and Niraja Shukla.

ACKNOWLEDGEMENTS

I will always be thankful to my academic advisor, Professor Anna Nagurney, John F. Smith Memorial Professor, for accepting me as her student. She has contributed to my rewarding graduate school experience by giving me the time, space, and opportunities to grow intellectually and personally. Her guidance and support led me to achieve various milestones through this time. I will always remember my first conference that she helped me attend. She has been instrumental in providing me with exposure and direction on multiple counts. I will always be grateful to her for furnishing a much needed structure to my pursuit of scientific inquiry. Her energy, enthusiasm, appreciation for the smallest attainments, and an undying spirit are nothing short of amazing. I strive to inculcate them in my academic career.

I would like to thank Professors Hari Balasubramanian, Eric Gonzales, and Adams Steven for their time and effort in providing thought-provoking comments and suggestions. Their support has given relief on many occassions. In addition, I am thankful to Professor Iqbal Agha for his consistent interest and guidance through my unique and gratifying teaching journey at the Isenberg School. Thank you to Professor Ahmed Ghoniem for being a support during my coursework. I will always appreciate his clarity. Also, I am grateful to Professors D. Anthony Butterfield and George Milne for helping me through the program. I wish to thank all the professors with whom I have interacted

and received encouragement at the Isenberg School.

It is said that a building is as strong as its foundation. Thank you to Mr. Jagdish Shah for teaching me how to enjoy what I do. I owe my love for mathematics, that developed during my formative years, to him. Professor G. Raghuram at the Indian Institute of Management Ahmedabad taught me the importance of the right attitude toward whatever I pursue, the need to question and not just accept, and bring credibility to my work. Had he not supported me through my Master's and beyond, I would not have considered doctoral studies.

A special group of people have not been mentioned yet because they deserve their own part. My colleagues and mentors at the Virtual Center for Supernetworks have guided me, been a reason for my drive, and helped me personally and professionally. I would like to thank Dr. Dong ”Michelle” Li, Dr. Jose Cruz, Dr. Dmytro Matsypura, Dr. Amir Masoumi, Dr. Min Yu, Dr. Sara Saberi, Deniz Besik, and all the others who have helped directly or indirectly.

Administrative and technology support of Priscilla Mayoussier, Susan Boyer, Audrey Kieras, Sarah Malek, Lynda Vassallo, Dianne Kelly, Rebecca Jerome, Matthew LaClaire, and Daniel Kasal, are greatly appreciated.

I finish by thanking my family and friends. My mother has always been a source of light, energy, and strength for me. I could never have come this far without her. Thank you to my father for introducing me to Operations Research and I will always be grateful for his vision and foresight. Also, thanks to my sister for being a source of support and encouragement. Thanks to all my friends, especially Stavan, for the inception of the idea of coming to the United States for further studies and supporting since.

ABSTRACT

GAME THEORY FOR SECURITY INVESTMENTS IN CYBER AND SUPPLY CHAIN NETWORKS

SEPTEMBER 2017

SHIVANI SHUKLA
B.S., GUJARAT UNIVERSITY
M.S., GUJARAT UNIVERSITY
Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Anna Nagurney

In a constantly and intricately connected world that is going digital, cybersecurity is imperative to not just the success but also the survival of a business. The ubiquitous digital transformation is fueled by a convulsive growth of devices and data that are leading important innovations in the domain of cyber-physical systems. However, this growth has also enabled internal and external threats to skyrocket, depicting the inherent dichotomy. With an

evolving threat landscape, a perpetrator has to be successful once, while the defenders have to continually succeed in fending-off attacks to protect critical infrastructure and digital assets.

The retail and financial sectors are prime targets owing to the large amounts of personal and financial information they process in disperse and distributed environments. One of the biggest retail breaches was that of Target when 30 million credit card numbers and personal information of 70 million customers were stolen and sold on the dark net (Riley and Pagliery (2015)). In the financial sector, JP Morgan Chase lost data of 83 million customers. The accussed laudered the $100 million obtained, used 75 shell companies that employed hundreds of people, and 30 fake passports from 17 countries to keep the money hidden (Pagliery (2015)).

Monetization of this sensitive data validates that the motivation of such criminals is principally financial. According to NTT 2016 Global Threat Intelligence Report, retailers are experiencing nearly three times as many cyberattacks as those by financial service providers that were top targets until 2014. Thus, in this dissertation, the focus is, mainly, on the retail and financial sectors, the top two sufferers in the recent past.

Increased sophistication in cyber threats can be attributed to the fact that criminals are now highly skilled, well-funded, coordinated, and organized. As a result, worldwide security breaches are increasing at just about 40% per annum and attackers stay undetected for an average of 200 days. One of the prominent examples of slow detection is the negligence suit filed by Yahoo users over a 2014 breach that compromised personal data of 500 million users but was discovered recently in 2016 (Vishwanath (2016)). While large organizations are cautious (JPMorgan doubled its cybersecurity spending to $500 million in 2015; Global information security spending will increase by 36% to $101 billion by 2018 (Purnell (2015))), the small and medium level enterprises are not known for ensuring basic precautionary measures (Forrester (2016)), which stems from their belief that attacks on larger organizations are more consequential. Unfortunately, cyber criminals do not discriminate.

Businesses are facing a barrage of attacks, majority of which have a financial or an espionage motive. In a highly interconnected and mutually dependent world, organizations are constantly interacting and transacting with each other. If one organization in this complex network is breached, there could be ramifications for the others since they might also be vulnerable. Often, attackers circumvent sophistical organizational firewalls and go after soft targets (CNN (2016)). Against the hackers, businesses put forth an asymmetric and myopic struggle.

Organizing funds for proactive and targeted responses requires careful security investment decision-making. In view of the above, a network approach to security investments while evaluating vulnerabilities of the individual organizations and the entire network is essential. Cyber threat cannot be eliminated, rather the culminating risks need to be managed. Investments in stronger defense mechanisms, preventive protocols, cyber intelligence, and agile systems that provide required redundancies or backups could aid in effective risk management.

If threats are rampant in the cyber space, physical supply chain networks are also not exempt from thefts, losses, and damages. In 2015, 1500 incidents of cargo theft, heavy commercial vehicle theft, and identity theft of trucking companies in the United States and Canada was reported. Out of these, in about 470 thefts, cargo and assets worth \$98 million were stolen. The average theft loss value per incident was \$187,490 (CargoNet (2015)). Some of the principal choke points that attackers manipulate are poor infrastructure and transportation networks, lax port security, and inadequate telecommunications to support tracking devices. Threats can vary by product type, mode of transportation, freight carriers, region, and even day of the week.

In view of the above, this work attempts to answer the following principal questions: (i) For competing firms in a network, what should their security levels be considering their investment costs or budget constraints to ensure a reduction in the entire network's vulnerability? (ii) If firms in a network cooperate, what are the implications on the network vulnerability? Does cooperation yield more economic/financial benefits? (iii) In a supply chain network for high value cargo with competing freight service providers, what should the shipment sizes and security levels be to ensure reduction in vulnerability?

Through this dissertation, I contribute to the modeling and analysis of security investments in cyber and supply chain networks considering network vulnerability also nonlinear budget constraints. The latter contributes significantly to the literature on variational inequality, game theory, and cybersecurity by being methodologically relevant to the application and solution of such problems. I also explore cooperation in terms of cybersecurity among firms in a network, providing a quantitative basis to information sharing to explore its financial and policy related benefits. This work extends the current literature in the cooperative game theory and cybersecurity domains. In addition, I explore the high value cargo supply chains that are faced with security investment decisions at the freight service providers' level. All the models presented in this dissertation are neither limited to a fixed number of firms or customers, nor to functions of any specific form. Moreover, very few cybersecurity or supply chain security investment models using game theory with competition, network perspective, network vulnerability, nonlinear budget constraints, and cooperation have been solved to-date.

The first part of this dissertation discusses the introduction of and motivation behind this research endeavor, along with a detailed literature review. Next, I discuss the contributions of the work I have undertaken. An overview of relevant methodologies, including variational inequality theory, competitive game theory, cooperative game theory and Nash bargaining theory, and two algorithms used in the chapters to follow is also provided.

Subsequently, I present a supply chain network model in which firms compete on security levels and product flows. The study takes a network approach to cybersecurity investment decision-making to obtain Nash equilibrium and ascertain vulnerabilities of the individual firms and the network on the whole. The model is probabilistic and includes demand side of the network along with its dynamics.

In the next part, a crucial and unique extension to the cybersecurity investment and risk determination model as discussed in the previous part is considered. Nonlinear budget constraints are added to the model that increase its complexity and call for theoretical and methodological contributions.

Thereafter, the cybersecurity investment model is modified to include a cooperative game approach to address the pressing need of collaboration and information sharing among firms in a network through which they can present a more coordinate front against the emerging cyber threat landscape. This inclusion is pivotal to the cybersecurity investment decisions.

Finally, I include my work that advanced modeling of physical security in supply chain networks. My current work in cybersecurity competition and cooperation was leveraged to cater to security investments regarding cargo, infrastructure, and other assets. The model contains features that are innate to physical flows and networks, thereby, marking a distinction from my work in cybersecurity. It deals, primarily, with security investment decisions in the presence of competing freight service providers shipping high value cargo from shipping origins to demand market destination points.

TABLE OF CONTENTS

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

CHAPTER 1

INTRODUCTION AND RESEARCH MOTIVATION

The effects of cyberattacks are being felt across the globe in multiple sectors and industries. The damages include direct financial losses and reputation issues, the loss of business, the inability to provide the expected services, opportunity costs, and the loss of trust.

Governments, military, private organizations, banks and financial institutions, hospitals, and many others generate a multitude of data on a regular basis. Often this information is confidential and is transmitted within and across organizations. Cyberattacks are growing and becoming more sophisticated with time. They are generally orchestrated from groups of hackers that are spatially diverse, thereby, utilizing infrastructure from multiple locations across the world. This makes it hard for officials to trace and assign ownership.

Juniper Research (2015) predicted that rapid digitization of consumer and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015. North America has been among the most targeted; however, the research argues that with digitization in other parts of the world, this proportion might decrease. According to the Center for Strategic and International Studies (2014), the world economy sustained $445 billion in losses from cyberattacks in 2014. The United States suffered a loss of $100 billion, Germany lost $60 billion, China lost $45 billion, and the United Kingdom reported a loss of $11.4 billion due to cybersecurity lapses. The think tank also presented an analysis that indicated that of the $2 trillion to $3 trillion generated by the Internet annually, about 15%-20% is extracted by cybercrime.

Perpetrators include spies from nation-states that seek secrets and intellectual property for strategic advantage; organized criminals that are financially motivated, sometimes even personally; terrorists who would want to create mass panic and an environment of fear and vulnerability by infiltrating power grids, water supply sources, or other critical infrastructure; and hacktivist groups who are trying to make a political or social statement (Deloitte (2014)).

The growing threat landscape of cybercrime extensively targets organizations in energy, retail, financial services, critical manufacturing, communications, and even healthcare. As per the US Department of Homeland Security (2015), the energy sector constituted the highest number of incidents (32%) reported in Fiscal Year 2014. The energy infrastructure faced a jolt when the "UglyGorilla" attack in 2014 sought access to pipeline schematics and natural gas flow regulation systems in the United States and caused a remote shutdown of critical systems (Bloomberg (2014b)). Monetary and regulatory efforts are being made to protect electric grids, oil and gas infrastructure, and intellectual property. The Energy Department announced $34 million in R&D in October 2015 (US Department of Energy (2015)).

In the retail sector, security breaches have been the most damaging and publicized. Loss of reputation, data, and business are evident. In 2014 alone, Target, Home Depot, Michaels Stores, Staples, and eBay were breached. Card data and personal information of millions of customers were stolen and the detection of cyber espionage became the prime focus for the retail sector with regards to cybersecurity (Granville (2015)).

Financial gains from subversion of processes and controls are highly lucrative to attackers infiltrating financial services firms, financial institutions, and banks. It is known that they are targeted incessantly to gain access to data, systems, people, processes, and finances. The large-scale data breach of JP Morgan Chase, Kaspersky Lab's detection of a two-year infiltration of 100 banks across the world costing $1 billion (USA Today (2015)), and the Dridex malware related losses of $100 million worldwide (Dodd (2015)) are some of the widely accepted cautionary tales in this sector.

One of the other major sectors that face disruption due to cyber and physical attacks is Logistics. Cargo thefts are giving rise to thriving black markets that are proving to be detrimental to agents involved and, in turn, the global economy. If GPS tracking tools can help locate a stolen vehicle, and geofencing solutions can send distress alarms if the vehicle is in peril, they can also be compromised to trace the vehicles and hack their systems to enable thefts (FBI (2016), FleetOwner (2016)).

In addition, cyberattacks can also disrupt critical physical civilian services, posing new challenges. For example, according to FastCompany (2016), the first documented cyberattack to result in widespread public blackouts occurred in Ukraine on December 23, 2015, leaving approximately half of the Ivano-Frankivsk region without electric power. This attack, and its associated service disruptions, were due to the BlackEnergyTrojan. Prior to this cyberattack, only physical infrastructure limited to governmental or industrial settings had been compromised. Cyberattacks on the electric grid can result in significant service disruptions and economic losses as well as fatalities.

The majority of cybercrimes constitute denial of service, malicious insiders, and malware threatening permanent physical and virtual damage to assets. The average annualized cost of cybercrime incurred by a benchmark sample of organizations was \$15 million. The range of these annualized costs was \$1.9 million to \$65 million, an 82% increase in the past six years (Ponemon Institute (2015)). A survey conducted by AON Risk Services with Ponemon Institute (2015) concluded that despite the comparability of the average potential loss to information assets (\$617 million) and property, plant and equipment (\$648 million), the percentages of insurance coverage are 51% and 12%, respectively.

Investments are constantly being made to avert impending crises across multiple sectors that have the potential to disrupt economic, social, and political fabrics of a functional economy. However, protection is much costlier than mobilizing an attack. Because of the interlinkages among different firms, organizations, institutions, and even nations, due to persistent data exchanges over the Internet and through advanced technologies, a single firm, organization, nation, or even individual may affect the vulnerability of others to cyberattacks. This instigated the research as presented in Chapter 3.

The technological innovations that are being envisioned could intensify these losses even more as they introduce new entry points for cyberattacks (The Wall Street Journal (2014)). These inclement costs ultimately trickle down to organizations and consumers.

As an example of advanced technologies, the Internet of Things has expanded the possible entry points for cyberattacks (ComputerWeekly.com (2015)). Organizations and governments are constantly attacked. Worries of a successful penetration are beginning to have noticeably negative business implications. Delays in adapting to cutting-edge technologies, implementing successful research findings, or even initiating ground-breaking research are many of the adverse effects of an uncertain business sentiment due to the ever increasing cybercrimes. Survey of McKinsey executives revealed concerns regarding slow down of value creation from cloud computing, mobile computing, and even healthcare technologies. A whopping 70% noted delay of a year or more in adopting models of Software-as-a-Service and Platform-as-a-Service. 40% said that because of such concerns enterprise-mobility capabilities were delayed by a year or more (McKinsey & Company Quarterly (2014)).

In today's networked economy, many businesses are dependent on their globalized supply chains with their IT infrastructure increasingly spread out and, at the same time, vulnerable to cyberattacks. For example, the Target breach of 2013 occurred when the cyberattacker took advantage of the vulnerability in the remote diagnostics of the HVAC system supplier connected to Target's IT system and entered a vulnerable supply chain link (Nagurney, Nagurney, and Shukla (2015)). Hence, there is a growing interest in developing rigorous frameworks for cybersecurity investments. According to PricewaterhouseCoopers (2014), mid-sized and large companies reported a 5% increase in cybersecurity budgets, whereas small companies reduced security costs by more than 20%. As reported in Glazer (2015), JPMorgan was expected to double its cybersecurity spending in 2015 to $500 million from $250 million in 2015. According to Purnell (2015), the research firm Gartner reported in January 2015 that the global information security spending would increase by 7.6% this year to $790 billion and by 36% by 2018 to $101 billion. It is clear that making the best cybersecurity investments, given budget constraints, is a very timely problem and issue, which led to the research in Chapter 4.

In this dissertation, I contribute to the modeling and analysis of security investments in cyber and supply chain networks considering network vulnerability also nonlinear budget constraints. The latter contributes significantly to the literature on variational inequality, game theory, and cybersecurity by being methodologically relevant to the application and solution of such problems. I also explore cooperation in terms of cybersecurity among firms in a network, providing a quantitative basis to information sharing to explore its financial and policy related benefits.

Specifically, on the cybersecurity front, the dissertation attempts to answer the following questions:

- In a competing scenario, what should security levels of firms in a network be considering their investment costs?
- While maintaining emphasis on reducing the entire network's vulnerability, how can the individual firms' vulnerability be reduced keeping the costs in check?
- If there is a nonlinear budget constraint, how will the decisions per the points above change?
- In a cooperation scenario, what should security levels of firms be while balancing network vulnerability and investment costs?
- Does cooperation yield more economic/financial benefits than when firms are competing? I attempt to give quantitative/tractable justifications.

Supplying, manufacturing, and transporting goods safely and securely is gaining more importance with multiple measures being taken in this regard (The Cargo Security Alliance (2012)). In addition to actual external threats, the inherent structure and complexity make supply chains difficult to secure. The stress on speed of delivery can cause reconciliation with security measures difficult. It is challenging to ensure that security procedures are followed throughout. Whether it is a trucker who does not properly verify seal on a container, or a vendor at origin who does not load cargo securely, a rush can lead to break down of processes (Damco (2012)). Besides, since supply chains are mostly long and fragmented, to ensure that security measures and procedures are given the same level of importance and treated with the same degree of urgency by all the entities involved is problematic. This is complicated further if the supply chains are global. For instance, the United States might have limited control over security and mitigation procedures of its international counterparts.

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)). There was an average of 63 cargo thefts per month in the US with the average loss value per incident in 2015 being $190,000 and in 2016 being $206,837. While the absolute number of crimes have been steady, the average loss-value ceiling has been rising (CargoNet (2017)).

As a relevant extension, the concepts and ideation of cybersecurity investments are applied to physical security investment decisions in supply chain networks with freight service providers that transport high-value cargo from various shipping origins to demand market destination nodes through multiple modes of transportation. In the supply chain security space where the attacks are of a physical nature, this dissertation attempts to answer the following question:

- In a competing scenario for freight service providers using multiple modes of transportation, what should be the security levels considering their investment costs and the sensitivity of demand markets toward their security measures given the cargo is high-value?

I now provide the relevant literature review on: cybersecurity and physical security investment decisions in the presence of competition, network perspective to investment decision-making, nonlinear budget constraints of these investments, and the application of game theory in this domain.

My research in the cybersecurity investment and network vulnerability space led to exploring cooperation among entities of a network. In the following section I provide additional motivation and a literature review on cooperation also to indicate the areas of contribution. I then provide an overview of the dissertation with contribution of each of the chapters in this dissertation.

1.1. Literature Review

The application of game theory (including the perspective of competition), development of formulations for incorporating nonlinear budget constraints and quantification of benefits resulting from cooperation are the primary contributions highlighted in this dissertation. This section discusses the literature review conducted for models with multiple firms competing for security considering cybersecurity investments and network vulnerability, nonlinear constraints, and cooperation. This chronological order marks the development of the models and related methodologies.

1.1.1. Cybersecurity Investments Modeled through Game Theory

One of the largest concern facing organizations, businesses, and governments is to devise a way to prevent and recover from cyberattacks whose prominence is imposing the need to prioritize investments with respect to perceived threats. Given the impact of cybercrime on the economy and society, there is great interest in evaluating cybersecurity investments. Each year $15 billion was spent by organizations in the United States to provide security for communications and information systems (see Gartner (2013), Market Research (2013)). Nevertheless, breaches due to cyberattacks continue to make huge negative economic impacts on businesses and society at-large. There is, hence, growing interest in the development of rigorous scientific tools that can help decision-makers assess the impacts of cybersecurity investments.

Anderson and Moore (2006) elaborated on the economics of information security, privacy, network topology and vulnerabilities. Rue, Pfleeger, and Ortiz (2007) provided an overview of models for cybersecurity investments, ranging from input/output models to return on investment frameworks as well as heuristic approaches. The edited volume by Daras and Rassias (2015) contains a collection of papers on cryptography and network security. Panaousis et al. (2014) put forth a method for creation of cybersecurity strategy for an organization. The authors performed a risk analysis of data assets of an organization and analyze the effectiveness of different security controls against various vulnerabilities. Next, they formulated control-games based on these risk assessments in which the organization (defender) attempted to reduce risk of cyberattacks by implementing a control in a way dictated by Nash Equilibrium. As a result, the defender minimized the maximum potential damage inflicted by the attacker. Solution of the control games here was handled by multi-objective, multiple choice knapsack techniques to decide upon optimal budget allocations. The research contributes to the fields of game theory, cybersecurity investments, and vulnerabilities. However, the models are not general, and cannot handle multiple firms. Also, they do not take a network perspective.

In many industries, including retail, investments by one decision-maker may affect the decisions of others and the overall supply chain network security (or vulnerability). Hence, a holistic approach is needed and some are even calling for a new discipline of cyber supply chain risk management (Boyson (2014)). Maughan et al. (2013) provided an execution framework and discussed challenges of transitioning cybersecurity research into practice. Since countries all across are investing significantly in cybersecurity research; for example, the

European Union recently approved 450 million euros to research (The Verge (2016)); this field of research is important and essential.

The domain of security in computer networks has limited but a useful literature employing game theory. Zero-sum, non-zero-sum, dynamic, stochastic, repeated, Stackelberg, static, and coalition games have been applied to computer and communication networks. Manshaei et al. (2013) provided a survey of the literature combining game theory and security. The survey is divided into six main categories: security of the physical and MAC layers, security of self-organizing networks, intrusion detection systems, anonymity, and privacy, the economics of network security, and cryptography. Das (2015) presented a cybersecurity ecosystem consisting of network, cloud, and software providers and economically analyzes the risk of correlation between agents in the ecosystem in case of a breach. Shetty et al. (2009) and Shetty (2010) focused on game theory for the determination of cybersecurity levels through investments. In both those publications, the authors determined the Nash Equilibrium as well as the social optimum associated with security levels. However, it was assumed that the firms face identical cybersecurity investment cost functions, had identical wealth, and also the damages afflicted due to a cyberattack were the same.

1.1.2. Nonlinear Constraints of Cybersecurity Investments Modeled through Game Theory

There is considerable literature on nonlinear constraints in the field of nonlinear programming. My contributions to the literature lie in advancing the state-of-the-art of game theory for cybersecurity investments as well as applications of variational inequalities, with the accompanying theory, for problems with nonlinear constraints. To-date, with the exception of the work of Toyasaki, Daniele, and Wakolbinger (2014), in the realm of network equilibrium models for end-of-life products, there has been limited work on such problems.

1.1.3. Models on Cooperation for Cybersecurity

An increasingly interconnected world may amplify the effects of a disruption. Physical and cyber outages of any kind can lead to material losses as well as loss of data, unplanned downtime, and adverse impacts on the reputations of the affected organizations. Firms interacting with one another may be at varied levels of security maturity. In addition, various departments within an organization could lack pertinent security measures. These are generally caused due to lack of coordination between departments for implementation of robust security measures that are all inclusive. Each firm has an independent assessment of its threat vectors, however, this information could be detrimental when not combined with those with whom they do business. Breaking down of silos, cooperating, and sharing information can have a direct impact on not just individual business' continuity but also a network's continuity. Hence, security governance is an integral part of risk management. Taking a network perspective in evaluating and comparing noncooperative and cooperative behavior in terms of security investments in cyber and supply chain networks can provide invaluable insight into the direct and indirect benefits of information sharing. It is critical to note that information sharing may have its disincentives since cooperation on the cyber front is being struck between companies or firms that are otherwise competitors holding variable market shares.

Methodologically, over the past years, network formulation problems have been tackled mainly from a noncooperative point of view. Anshelevich et al. (2004), Chen and Roughgarden (2006), Albers (2008), Nagurney (2015), and many others have modeled independent, rational, and selfish decision-makers that constitute and build a large network that may or may not be self-sufficient. Nash equilibria that present the users'/firms' behavior produce a realistic viewpoint yet could, in terms of implementation, be more expensive than optimal or centralized solutions. This is mainly due to the lack of cooperation among firms. While there is considerable research conducted in the field of non-isolated and independent users of a network, realistically, in the long run, the decision-makers might discuss strategies. Though in highly competitive markets this would take place between few firms that have instilled trust among them, for an issue like cybersecurity in which all firms have a common goal, to strike cooperation would be strategically imperative.

Even so, since critical, and often confidential, information is to be ex-changed, formulation of a successful coalition will be contingent on whether there are strategic actions beneficial to each firm. Also, incentives could be introduced by external governing authorities to formalize stable cooperation. Some of the works like Elias et al. (2010) and Azad, Altman, and El-Azouzi (2009) included a socially-aware component into firms' utility functions to overcome the disbenefits of noncooperation. However, they are not always effective. It was demonstrated in Elias et al. (2010) that socially aware firms can form stable networks that may be much more expensive than a naturally formed one.

The increased rate of cyberattacks has spurred the behavioral analysis of attackers and defenders. Aggarwal et. al. (2015) took a game theory approach to study actions of attackers and defenders in a 2×4 cybersecurity game that is evaluated computationally through 1000 simulations. A defense exercise model using game theory was developed by Patrascu and Simion (2014) to train cyber response specialists. Nagurney (2015) utilized a network economics approach to model cybercrime emphasizing that both firms and hackers act as economic agents. RAND National Security Division (2014) also argued that an economic approach to tackling cybercrime is warranted.

In addition to investigating interactions among attackers and defenders, there has also been a growing literature on cybersecurity investments. The investment in cybersecurity through software and hardware, education, and effective personnel can help resist the growing frequency and severity of attacks, and assist in the planning of appropriate allocation of resources required to prevent/mitigate the likely damage. Garvey, Moynihan, and Servi (2013) suggested an approach that helps to prioritize among competing investment options for better cyber defense. They identify sets of Pareto efficient cost-benefit investments, and their economic returns, that capture tangible and intangible advantages of countermeasures that strengthen cybersecurity. From a social welfare standpoint, Gordon et. al. (2015) examined changes in the maximum a firm should invest into cybersecurity activities in the face of well-recognized externalities.

Nagurney (2015) emphasized the importance of assessing the vulnerabilities of cyberattacks in a rigorous quantifiable manner and identifying possible synergies associated with information sharing for firms providing critical infrastructure networks on which our economy and society depend. The complexity and interdependence of firms, governments, and individuals in intricately woven networks mean that an attack on one may pave the way for attacks on others. Given that the number and intensity of cyber threats for every industrial and non-industrial sector have increased, firms and governments are progressing toward sharing threat information to arrange coordinated defenses against attacks.

I address the above by taking a cooperative game approach whereby firms coordinate their strategies such that each is expected to receive a utility benefit while reducing network vulnerability in the context of cybersecurity. The Nash Bargaining solution is a highly effective tool to model interactions among firms that give rise to tacit cooperative environments. Firms bargain to achieve a strategic point that is beneficial to all. The goal was to arrive at Nash bargaining solution that is unique to the specified game satisfying Pareto optimality.

To model cooperative behavior in otherwise competing players, Nash bargaining theory was proposed in Nash (1950b). Considerable contributions to the area were made by Harsanyi (1977), who extended the original two-person game into a multi-player game and derived important theoretical deductions, and by Muthoo (1999), who applied the theory to various bargaining situations and demonstrated the usefulness. Various extensions of the theory and application to supply chains were proposed by Nagarajan and Sosic (2008). Boonen (2016) discussed strategic interaction between two firms that trade risk over the counter in a one period model. The focus is on an incomplete set of risk redistributions.

In the context of cybercrime, one of the extensions was employed by Wagner et al. (2012), who used Nash bargaining for resource allocation in cloud computing for collaborative defense. An optimization formulation of a collusive cooperative game with product quantities as variables was developed and solved as a nonlinear programming problem in Harrington et al. (2005). Jiang et al. (2009), later, analyzed cooperative content distribution and traffic engineering in ISP networks. Finally, Bakshi and Kleindorfer (2009) did not discuss cybersecurity, yet demonstrated the use of Nash bargaining and cooperative game theory towards investment for resilience in global supply chains. The paper utilized an axiomatic approach to bargaining.

I also focus on cooperation among the firms in terms of their cybersecurity levels, but from a system-optimization perspective in which the sum of the expected utilities of all the firms is maximized. System-optimization models, but different from the one proposed here, were also developed for cybersecurity investments by Shetty et al. (2009) and Shetty (2010).

1.1.4. Models on Security Associated with Physical Aspects of Supply Chain Networks

Supply chains provide food, medicine, energy, money, and other products that support global businesses and societies. Multiple stakeholders and entities are responsible for and reliant on the smooth functioning of these supply chains, such as public and private sectors/industries, law enforcement, policy-makers, and other foreign or domestic partners. Evidently, there are interconnections between supply chains forming a web of transportation, infrastructure, information technology, and cyber networks. The interconnections promote economic development, but they are also manipulated by internal and external factors to propagate shocks across multiple sectors and even geographies.

Integrated supply chains are quick and cost-effective, yet susceptible to risks that can escalate from minor events to large disruptions. The goal is to develop a system that is resilient to evolving threats and can recover from damages rapidly. The ability to withstand threats or attacks while maintaining lean supply chains is what most entities in a supply chain seek to achieve. It is critical to address systemic vulnerability by identifying and protecting key assets, infrastructure, and support systems, and promoting efficient operational processes and redundancy in assets.

Autry and Bobbitt (2008) conducted an exploratory study investigating firm-level constructs for approaches toward mitigation of supply chain security breaches and risk management. Markmann, Darkow, and von der Gracht (2013) proposed a delphi-based risk identification and assessment framework for supply chain security in a multi-stakeholder environment. Their work contributed to the analysis of multidimensional man-made risks that were particularly uncertain in terms of type, location, and affected supply chain partners. Bichou and Talas (2014) provided an overview of supply chain security initiatives in surface and maritime transportation. A game theory perspective to supply chain security was adopted by Bier et al. (2008) to propose a framework for defending infrastructure against planned and intelligent attacks. The research presented sequential games that put forth principles to optimize subsequent actions and defenses to protect vulnerabilities. A few firms were considered but the work lacks a network perspective.

With modernization and the increased role of technological developments in supply chains, the cyber networks also affect supply chains. Bartol (2014) commented on the element of cyber/information technology in the present and its likely proliferation in the future with regards to supply chains. Voss and Williams (2013) investigated public-private collaborations for supply chain security. The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy was discussed by Zailani et al. (2015). The study conducted an empirical analysis to test propositions of connections between security culture and security operational performance metrics.

As supply chains develop global operations, they have become more complex. This hinders early detection of risks and causes greater disruptions, thereby delaying prompt recovery and affecting resilience ((Sheffi (2007), Handfield and McCormack (2007), Thun and Hoening (2011), Sodhi, Son, and Tang (2012)). As per Waters (2011) and Sodhi, Son, and Tang (2012), risks in a supply chain can manifest in many different ways, virtually affecting any link on a network/chain, right from suppliers to customers.

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 is limited, and, even more so, for security associated with freight service provision investments. Bakir (2011) considered 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 (whether to invest or not) for container shipping transportation, which was inspired by the work of Kunreuther and Heal (2003). For examples of innovative game theory models for counter-terrorism, see the work of Bier (2006) and Wein et al. (2006). In the context of supply chain security and cargo theft, Ekwall (2012) provided a comprehensive view of the issues and Burges (2013) gave a practitioner's viewpoint. The edited volume of Wagner and Bode (2009) contains contributions to security and risk with a focus on logistics service providers.

It is critical to note that there are hardly any models that aid in supply chain security investment decision-making from a carrier/freight service provider perspective considering multiple modes. In the realm of supply chain network competition with multiple manufacturers and freight service providers, the paper, Nagurney et al. (2015), focused on developing static and dynamic models of competition between members of a supply chain network.

1.2. Dissertation Overview

The dissertation consists of seven chapters wherein this chapter deals with the research motivation and the literature review. Chapter 2 provides a review of the methodologies that are utilized in this dissertation, mainly variational inequality theory (Nagurney (1999)) and Nash bargaining theory (Harsanyi (1977)). Below I detail the contributions in Chapters 3 through 6 and provide additional background.

1.2.1. Contributions in Chapter 3

Inspired by Shetty et al. (2009) and Shetty (2010), yet significantly more general, the focal point of chapter 3 is the modeling of firms in a supply chain network in which they compete on security levels and product flows. The goal is to obtain the Nash Equilibrium and ascertain network vulnerability and not just the vulnerability of individual firms. During the processes of decision-making firms, I consider not just their own security levels and product flows but also those of other firms. This also applies to the probability of a successful attack on a firm. The model does not consider identical firms as in Shetty (2010) and the demand side of the network and related dynamics are explicitly considered.

The demand side of the network necessitates the inclusion of realistic consumer preferences. Firms generally do not reveal their true security levels but give an overall understanding or indications to maintain competitive advantage over their rivals. Hence, in the model, the consumers reveal their choices through demand price functions that depend on product demands and the average level of security in the supply chain network.

Firms may be faced with distinct security investment cost functions as their current information technology and cyber infrastructure, constitution of assets, urgency, business scope and size are likely to be different. The model is general enough to handle spatially separated firms, firms that have a significant proportion of their business transactions taking place online, or are brick and mortar. An important extension is that we also consider that firms could possibly be faced with different financial damages in event of a successful cyberattack. This chapter is based on the paper by Nagurney, Nagurney, and Shukla (2015) and it will also be included in the dissertation.

1.2.2. Contributions in Chapter 4

Economic constraints threaten efficient response mechanisms put in place by firms to guard against cyberattacks. Cybersecurity investments were considered as pure/necessary costs that do not add discernible value to the product or business as a whole (Ponemon Institute (2015)). However, with the changing landscape, security is among the top priorities of most firms today to protect their operations, personnel and infrastructure. This is the reason external and internal policy-makers are factoring disruptions into their regulatory framework.

The financial commitment to security needs a boost across industries and firms are responding to that need. Sony Pictures plans to spend $15 million to secure itself from future cyberattacks. The company had been attacked in 2014 that cost it $100 million (IT Security (2015)). Despite a budget of $250 million, JP Morgan Chase was attacked in 2014 since they neglected investing into two-step authentication. They were slated to double that budget in the following years. Target after its attack in 2014 that cost $148 million assigned a budget of $100 million that was used specifically to adopt a technology to embed chips into debit and credit cards for added security (CBS News (2014)).

In spite of assigning large amounts of funds and supporting regular maintenance of the infrastructure, there are still tight budgetary constraints and they are bound to remain. Even though companies are investing more than they used to in cybersecurity, mounting risks caused 65% respondents in a survey to state that budget constraints are their number one obstacles to delivering value (EY (2013)). An increase in budgets could lower risks, but might not be sustainable or provide complete protection. As discussed in the sections above, firms are part of a network that exchanges data, information, and transactions. Vulnerability of a firm they are doing business with could still put them at considerable risk. Strategically using budgets is a valuable response.

In this chapter, the work builds on Shetty (2010) and chapter 3 but with a crucial difference - the firms are now subject to individual budget constraints on their cybersecurity investments. These constraints can be highly nonlinear which posed theoretical and computational challenges. In this work, there is an upper bound on the security level of each firm that is less than one, since one implies perfect security which may not be attainable in reality. Earlier work had an upper bound of one. Moreover, upper bounds on product flows are imposed. This restricts the amount moving from a firm to a demand market.

The principal contribution in this chapter lies in advancing the state-of-the-art of game theory literature for cybersecurity investments as well as of variational inequality theory for problems with nonlinear constraints.

This chapter, based on Nagurney, Daniele, and Shukla (2017), develops a supply chain game theory model of competing retailers for the maximization of revenue and minimization of investment costs to plan for defense from an attack, and financial losses/damages caused by a successful cyberattack. The framework also quantifies vulnerability of a firm and of the network as a whole.

1.2.3. Contributions in Chapter 5

In this chapter, cooperation among firms in terms of security levels is modeled by two approaches: (i) Bargaining - firms collaborate and organically try to arrive at a solution that is economically beneficial to all, (ii) System Optimization - the entire network is considered to be a system that has to be optimized to reduce costs and vulnerability. I compare and contrast the results obtained through both approaches with the competitive Nash Equilibrium solution to ascertain the economically beneficial approach that helps to reduce vulnerability of the entire network.

Subsection 1.1.3 highlights the literature in the domain of cooperation and cybersecurity. Most of the research does not utilize Nash bargaining for modeling investments in this domain. If it is utilized, the models are solved axiomatically only. In the realm of information sharing, there are the works of Gal-Or and Ghose (2004), Gal-Or and Ghose (2005), and Gordon et al. (2015) discussed the economics and related benefits, and at the same time, pitfalls of sharing critical information that can be leveraged to gain business advantages. Comparison of cooperative approaches for reducing network vulnerability while maintaining economic incentives, and providing quantitative and tractable justifications to cooperation is the contribution of this chapter to the current literature. Some of the methodological contributions are: (i) Establishing uniqueness, under appropriate assumptions, of the competitive and cooperative solutions, (ii) The objective function of the Nash bargaining model is highly nonlinear and, thus, solvability is among the major challenges.

1.2.4. Contributions in Chapter 6

The model developed and successfully solved in this chapter fills many gaps in the literature. According to the literature review provided in Subsection 1.1.4, some of the key aspects of models developed in Chapters 3, 4, and 5 are extended to include supply chain security investment decisions to fight against physical attacks and not just cyberattacks. Freight service providers are competing to ship high-value cargo from origin to destination nodes. The focus on high-value cargo was due to the fact that the average loss-value of cargo during theft situations is increasing year-on-year. Since the need for security against attacks on cargo and assets has increased, there is a need for models that help ascertain investments and their expected monetary returns.

The literature review in 1.1.4 shows that currently there are hardly any models in the realm of supply chain security. The approach adopted in this work makes the following contributions: (i) Freight service providers are competing as to the quantity of cargo that they can ship, and the security levels, transporting goods through multiple modes, (ii) Shippers reflect their preferences for transportation of high-value cargo through the prices that they are willing to pay to the freight service providers, (iii) The investment decisions include the investment costs that these service providers will have to bear in order to stay relevant and competitive in the market, and (iv) Probability of a successful attack is endogenously dependent on the security levels.

In Chapter 6 of this dissertation, I discuss the model, the governing equilibrium conditions, formulation, and solution process to arrive at equilibria for both security levels and shipment quantities.

1.2.5. Concluding Comments

The main contributions of the methodologies and results in this dissertation to the existing literature are summarized below.

1. The models constructed in Chapters 3, 4, 5, and 6 are general and can incorporate multiple firms. They take a probabilistic perspective with investment cost functions, inverse demand functions, and constraints that have functional forms that are not limited to being linear or quadratic. Furthermore, the investment cost functions or demand price functions need not be separable and can depend on vectors of security levels and quantities in Chapters 3, 4, and 6, and on the vector of security levels in Chapter 5. Such features more realistically capture the nature of competition and cooperation among firms in terms of security levels and/or product flows.
2. A network approach to the economics of cyber and supply chain security has been employed in all the models. The combination of variational inequalities, game theory, network vulnerability, and economics of secu-

rity makes the models unique and pragmatic. Chapter 3 provides an important extension to Shetty et al. (2009) and Shetty (2010).

3. Chapter 4 is an extension of Chapter 3 in that nonlinear budget constraints on investment costs are captured. There has been no literature in advancing cybersecurity investment decisions with applications of variational inequalities considering game theory and nonlinear constraints.

4. As justified in Subsection 1.1.3, cooperation is essential and novel to cybersecurity investment decisions. I apply the Nash bargaining theory to model cooperation among firms in a network that are otherwise competitors in Chapter 5. This proposition contributes to a novel Nash bargaining solution for an m-firm cooperative network problem which has appealing characteristics in terms of efficient and less vulnerable networks and security (cost) allocations in an acceptable computational timeframe.

5. A comparison between Nash bargaining and System-optimization perspectives has been included. Quantifiable and tractable justifications of economic benefits for each firm due to cooperation are made possible and demonstrated. Overall, the contributions are in terms of models, methodology, and solvability.

6. In this dissertation, qualitative results and proofs for nonlinear constraints and existence and uniqueness of noncooperative and cooperative solutions are provided. Moreover, computational procedures are discussed followed by a detailed discussion on the results.

7. To advance physical security in supply chain networks, I leverage the current work done on cybsercurity competition. In Chapter 6, I include the following: (i) Security investment decision-making for competing freight service providers in a supply chain network that utilizes multiple modes for transportation that could have distinct probabilities of attacks, (ii) The focus is on high-value cargo wherein the shippers show their sensitivity to security through the prices they are willing to pay.

8. In the final chapter, I present conclusions and suggestions for future research.

CHAPTER 2

METHODOLOGIES

In this chapter, fundamental theories and methodologies utilized in this dissertation are presented and discussed. Variational inequality theory is an essential methodology used here to analyze the equilibria of supply chain networks with security investments, network vulnerability, budget constraints, and cooperation. Relationships between variational inequality and game theory are also discussed. Since cooperation for cybersecurity investments is an essential dimension explored through Nash bargaining in Chapter 5, I also present its methodological aspects for background and reference. Additional theorems and proofs associated with finite-dimensional variational inequality theory can be found in Nagurney (1999).

Qualitative properties specific to the investment models in Chapters 3, 4, and 5 are discussed at length in the following chapters. The quantitative results pertain to the existence and uniqueness of solutions obtained by variational inequality theory and Nash bargaining theory.

Finally, algorithms used to solve competitive and cooperative models are presented. I discuss the Euler method employed to solve the variational inequality formulations and briefly present the Interior Point method utilized in solving the Nash bargaining and System-Optimization formulations in Chapter 5.

2.1. Variational Inequality Theory

In this section, I briefly recall the theory of variational inequalities. All definitions and theorems are taken from Nagurney (1999). All vectors are assumed to be column vectors, except where noted.

Definition 2.1 (Finite-Dimensional Variational Inequality Problem)

The finite-dimensional variational inequality problem, VI$(F, \mathcal{K})$*, is to determine a vector* $X^* \in \mathcal{K} \subset \mathcal{R}^n$*, such that*

$$\langle F(X^*), X - X^* \rangle \geq 0, \quad \forall X \in \mathcal{K}, \tag{2.1a}$$

where F *is a given continuous function from* $\mathcal{K}$ *to* R^n*,* $\mathcal{K}$ *is a given closed convex set, and* $\langle \cdot, \cdot \rangle$ *denotes the inner product in n-dimensional Euclidean space.*

In (2.1a), $F(X) \equiv (F_1(X), F_2(X), ..., F_n(X))^T$, and $X \equiv (X_1, X_2, ..., X_n)^T$. $F(X)$ and X are both column vectors. Recall that for two vectors $u, v \in \mathcal{R}^n$, the inner product $\langle u, v \rangle = ||u||||v||cos\theta$, where θ is the angle between the vectors u and v, and (2.1a) is equivalent to

$$\sum_{i=1}^{n} F_i(X)(X_i - X_i^*) \geq 0, \quad \forall X \in \mathcal{K}. \tag{2.1b}$$

The variational inequality problem is a general problem that encompasses a wide spectrum of mathematical problems, including, optimization problems, complementarity problems, and fixed point problems (see Nagurney (1999)). It has been shown that optimization problems, both constrained and unconstrained, can be formulated as variational inequality problems. The relationship between variational inequalities and optimization problems, which is explored in this dissertation, is now briefly reviewed.

Proposition 2.1 (Formulation of a Constrained Optimization Problem as a Variational Inequality)

Let X^* be a solution to the optimization problem:

$$Minimize \quad f(X) \tag{2.2}$$

subject to:

$$X \in \mathcal{K},$$

where f is continuously differentiable and $\mathcal{K}$ is closed and convex. Then X^* is a solution of the variational inequality problem:

$$\langle \nabla f(X^*), X - X^* \rangle \geq 0, \quad \forall X \in \mathcal{K}, \tag{2.3}$$

where $\nabla f(X)$ is the gradient vector of f with respect to X, where $\nabla f(X) \equiv (\frac{\partial f(X)}{\partial X_1}, ..., \frac{\partial f(X)}{\partial X_n})^T$.

Proposition 2.2 (Formulation of an Unconstrained Optimization Problem as a Variational Inequality)

If $F(X)$ is a convex function and X^* is a solution to $\mathrm{VI}(\nabla f, \mathcal{K})$*, then X^* is a solution to the optimization problem (2.2). In the case that the feasible set $\mathcal{K} = R^n$, then the unconstrained optimization problem is also a variational inequality problem.*

The variational inequality problem can be reformulated as an optimization problem under certain symmetry conditions. The definitions of positive-semidefiniteness, positive-definiteness, and strong positive-definiteness are recalled next, followed by a theorem presenting the above relationship.

Definition 2.2 (Positive Semi-Definiteness and Definiteness)

An $n \times n$ matrix $M(X)$, whose elements $m_{ij}(X); i,j = 1,...,n$, are functions defined on the set $S \subset \mathcal{R}^n$, is said to be positive semidefinite on S if

$$v^T M(X) v \geq 0, \quad \forall v \in \mathcal{R}^n, X \in S. \tag{2.4}$$

It is said to be positive definite on S if

$$v^T M(X) v \geq 0, \quad \forall v \neq 0, v \in \mathcal{R}^n, X \in S. \tag{2.5}$$

It is said to be strongly positive definite on S if

$$v^T M(X)v \geq \alpha||v||^2, for\ some\alpha > 0, \quad \forall v \in \mathcal{R}^n, X \in S. \tag{2.6}$$

Theorem 2.1 (Formulation of an Optimization Problem from a Variational Inequality Problem Under Symmetry Assumption)

Assume that $F(X)$ is continuously differentiable on $\mathcal{K}$ and that the Jacobian matrix

$$\nabla F(X) = \begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \cdots & \vdots \\ \frac{\partial F_n}{\partial X_1} & \cdots & \frac{\partial F_n}{\partial X_n}, \end{bmatrix} \tag{2.7}$$

is symmetric and positive semidefinite. Then there is a real-valued convex function $f : \mathcal{K} \mapsto \mathcal{R}^1$ satisfying

$$\nabla f(X) = F(X), \tag{2.8}$$

with X^* the solution of VI$(F, \mathcal{K})$ also being the solution of the mathematical programming problem:

$$Minimize \quad f(X)$$

subject to:

$$X \in \mathcal{K},$$

where $f(X) = \int F(X)^T dx$, and $\int$ is a line integral.

Thus, the variational inequality is a more general problem formulation than the optimization problem formulation, since it can also handle a function $F(X)$ with an asymmetric Jacobian (see Nagurney (1999)). Next, the qualitative properties of variational inequality problems, especially, the conditions for existence and uniqueness of a solution, are recalled.

Theorem 2.2 (Existence of a Solution)

If $\mathcal{K}$ is a compact convex set and $F(X)$ is continuous on $\mathcal{K}$, then the variational inequality problem admits at least one solution X^*.

Theorem 2.3 (Condition for Existence if Feasible Set is Unbounded)

If the feasible set $\mathcal{K}$ is unbounded, then $\mathrm{VI}(F, \mathcal{K})$ admits a solution if and only if there exists an $\mathcal{R} > 0$ and a solution of $\mathrm{VI}(F, \mathcal{S})$, X^*_R, such that $||X^*_R|| < \mathcal{R}$, where $\mathcal{S} = \{X : ||X|| \leq \mathcal{R}\}$.

Theorem 2.4 (Existence Following a Coercivity Condition)

Suppose that $F(X)$ satisfies the coercivity condition

$$\frac{\langle F(X) - F(X_0), X - X_0 \rangle}{||X - X_0||} \to \infty, \tag{2.9}$$

as $||X|| \to \infty$ for $X \in \mathcal{K}$ and for some $X_0 \in \mathcal{K}$. Then $\mathrm{VI}(F, \mathcal{K})$ always has a solution.

According to Theorem 2.4, the existence condition of a solution to a variational inequality problem can be guaranteed by the coercivity condition. Next, certain monotonicity conditions are utilized to discuss the qualitative properties of existence and uniqueness. Some basic definitions of monotonicity are reviewed first.

Definition 2.3 (Monotonicity)

$F(X)$ is monotone $\mathcal{K}$ if

$$\langle F(X^1) - F(X^2), X^1 - X^2 \rangle \geq 0, \quad \forall X^1, X^2 \in \mathcal{K}. \tag{2.10}$$

Definition 2.4 (Strict Monotonicity)

$F(X)$ is strictly monotone on $\mathcal{K}$ if

$$\langle F(X^1) - F(X^2), X^1 - X^2 \rangle \geq 0, \quad \forall X^1, X^2 \in \mathcal{K}, X^1 \neq X^2. \tag{2.11}$$

Definition 2.5 (Strong Monotonicity)

$F(X)$ is strongly monotone on $\mathcal{K}$ if

$$\langle F(X^1) - F(X^2), X^1 - X^2 \rangle \geq \alpha ||X^1 - X^2||^2, \quad \forall X^1, X^2 \in \mathcal{K}, \tag{2.12}$$

where $\alpha > 0$.

Definition 2.6 (Lipschitz Continuity)

$F(X)$ is Lipschitz continuous on $\mathcal{K}$ if there exists an $L > 0$, such that

$$\langle F(X^1) - F(X^2), X^1 - X^2 \rangle \leq L ||X^1 - X^2||^2, \quad \forall X^1, X^2 \in \mathcal{K}. \tag{2.13}$$

L is called the Lipschitz constant.

Theorem 2.5 (Uniqueness Under Strict Monotonicity)

Suppose that $F(X)$ is strictly monotone on $\mathcal{K}$. Then the solution to the VI$(F,\mathcal{K})$ *problem is unique, if one exists.*

Theorem 2.6 (Uniqueness Under Strong Monotonicity)

Suppose that $F(X)$ is strongly monotone on $\mathcal{K}$. Then there exists precisely one solution X^* to VI$(F,\mathcal{K})$.

In summary of Theorems 2.2, 2.5, and 2.6, strongly monotonicity of the function F guarantees both existence and uniqueness, in the case of an unbounded feasible set $\mathcal{K}$. If the feasible set $\mathcal{K}$ is compact, that is, closed and bounded, the continuity of F guarantees the existence of a solution. The strict monotonicity of F is then sufficient to guarantee its uniqueness provided its existence.

2.2. The Relationships between Variational Inequality and Game Theory

In this section, some of the relationships between variational inequality theory and game theory are discussed briefly.

Nash (1950a, 1951) developed noncooperative game theory, involving multiple players, each of whom acts in his/her own interest. In particular, consider a game with m players, each player i having a strategy vector $X_i = \{X_{i1}, ..., X_{in}\}$ selected from a closed, convex set $\mathcal{K}^i \subset R^n$. Each player i seeks to maximize his/her own utility function, $U_i : \mathcal{K} \mapsto R$, where $\mathcal{K} = \mathcal{K}^1 \times \mathcal{K}^2 \times ... \times \mathcal{K}^m \subset R^{mn}$. The utility of player i, U_i, depends not only on his/her own strategy vector, X_i, but also on the strategy vectors of all the other players, $(X_1, ..., X_{i-1}, X_{i+1}, ..., X_m)$. An equilibrium is achieved if no one can increase his/her utility by unilaterally altering the value of its strategy vector. The formal definition of the Nash Equilibrium is recalled as following.

Definition 2.7 (Nash Equilibrium)

A Nash Equilibrium is a strategy vector

$$X^* = (X_1^*, ..., X_m^*) \in \mathcal{K}, \tag{2.14}$$

such that

$$U_i(X_i^*, \hat{X}_i^*) \geq U_i(X_i, \hat{X}_i^*), \quad \forall X_i \in \mathcal{K}^i, \forall i, \tag{2.15}$$

where $\hat{X}_i^* = (X_1^*, ..., X_{i-1}^*, X_{i+1}^*, ..., X_m^*)$.

It has been shown by Hartman and Stampacchia (1966) and Gabay and Moulin (1980) that given continuously differentiable and concave utility functions, $U_i, \forall i$, the Nash Equilibrium problem can be formulated as a variational inequality problem defined on $\mathcal{K}$.

Theorem 2.7 (Variational Inequality Formulation of Nash Equilibrium)

Under the assumption that each utility function U_i is continuously differentiable and concave, X^* is a Nash Equilibrium if and only if $X^* \in \mathcal{K}$ is a solution of the variational inequality

$$\langle F(X^*), X - X^* \rangle \geq 0, \quad X \in \mathcal{K}, \tag{2.16}$$

where $F(X) \equiv (-\nabla_{X_1} U_1(X), ..., -\nabla_{X_m} U_m(X))^T$, *and* $\nabla_{X_i} U_i(X)$ $= (\frac{\partial U_i(X)}{\partial X_{i1}}, ..., \frac{\partial U_i(X)}{\partial X_{im}})$.

The conditions for existence and uniqueness of a Nash Equilibrium are now introduced. As stated in the following theorem, Rosen (1965) presented existence under the assumptions that $\mathcal{K}$ is compact and each U_i is continuously differentiable.

Theorem 2.8 (Existence Under Compactness and Continuous Differentiability)

Suppose that the feasible set $\mathcal{K}$ is compact and each U_i is continuously differentiable. Then existence of a Nash Equilibrium is guaranteed.

Gabay and Moulin (1980), on the other hand, relaxed the assumption of the compactness of $\mathcal{K}$, and proved existence of Nash Equilibrium after imposing a coercivity condition on $F(X)$.

Theorem 2.9 (Existence Under Coercivity)

Suppose that $F(X)$, as given in Theorem 2.7, satisfies the coercivity condition (2.9). Then there always exists a Nash Equilibrium.

Furthermore, Karamardian (1969) demonstrated existence and uniqueness of a Nash Equilibrium under the strong monotonicity assumption.

Theorem 2.10 (Existence and Uniqueness Under Strong Monotonicity)

Assume that $F(X)$, as given in Theorem 2.7, is strongly monotone on $\mathcal{K}$. Then there exists precisely one Nash Equilibrium X^*.

Additionally, based on Theorem 2.5, uniqueness of a Nash Equilibrium can be guaranteed under the assumptions that $F(X)$ is strictly monotone and an equilibrium exists.

Theorem 2.11 (Uniqueness Under Strict Monotonicity)

Suppose that $F(X)$, as given in Theorem 2.7, is strictly monotone on $\mathcal{K}$. Then the Nash Equilibrium, X^*, is unique, if it exists.

2.3. Nash Bargaining Theory

Nash (1950b) and Nash (1953) dealt exclusively with a two-person bargaining problem for modeling cooperation. The payoffs and disagreement points were a reflection of the parties' strategic choices arrived at through an axiomatic approach. However, in Harsanyi (1963), a strategic generalized m-person bargaining problem formulation was proposed. The explicit modeling revealed that a bargaining problem was more complicated in an m-person case from both conceptualization and solution standpoints.

Let $\pi_i(X)$ be the utility of party i and π_i^N be the static Nash Equilibrium utility if the parties compete and do not attempt at cooperation. The classical theory of Nash, in which a two-person problem was considered, that is, $i = 1, 2$, provides the following axioms:

Individual Rationality: None of the parties accept utility lower than that during competition.

$$\pi_i(X^*) \geq \pi_i^N, \quad i = 1, 2, \tag{2.17}$$

where $X^* \in \mathcal{K}$, and $\mathcal{K}$ is closed and convex.

Pareto Optimality: The cooperation will represent a situation that cannot be improved upon by either parties to their advantage.

Symmetry: The symmetry condition rules out any differences in the players' bargaining abilities or powers.

Linear Invariance: This axiom imposes that a bargaining solution is invariant to equivalent utility transformations.

Independence of Irrelevant Alternatives: This implies that only the solution outcome and $\pi_i^N, \forall i$ are relevant and the outcome does not depend on other alternatives in the set. The appropriateness of this axiom depends on the bargaining problem itself.

Nash (1950b) proposed a unique solution based on the above axioms. In his bargaining model, it was assumed that the disagreement points/conflict strategies were fixed which could be true in reality. However, more often than not, the parties would have an influence over the disagreement points, making bargaining more complex.

In this dissertation, I take a mathematical approach similar to Harrington et al. (2005) (m-person bargaining) to obtain the Nash bargaining solution by relying on convex optimization theory for ascertaining uniqueness of solution. To reach the solution, disagreement points are Nash equilibria in a noncooperative (or a competition) situation obtained through variational inequality theory. The Nash bargaining solution is, then, obtained by:

$$Maximize \quad \prod_{i=1}^{m} \pi_i(X) - \pi_i^N, \tag{2.18}$$

subject to:

$$\pi_i(X) \geq \pi_i^N, \quad \forall i, \tag{2.19}$$

$$X \in \mathcal{K}.$$

The constraints make sure that an agreement/cooperation is reached if each of the parties is at a utility level greater than or equal to when they are competing. A solution algorithm for the above is presented in Subsection 2.5.

If the parties are symmetric (equivalent in costs/capacities or, more generally, in bargaining power), the best symmetric element of the feasible set, given the constraints, is selected. The payoff is then divided among the parties. However, if the parties are asymmetric, such as in their utilities and costs, there is no such focal point. The selection would be asymmetric.

In addition to the formal motivation above, a global optimization outlook was taken for the optimization problem (2.18, 2.19). In Chapter 5, the contribution is also to obtain conditions for a unique solution to the problem and to provide relevant mathematical insights. While not considered in the work presented in this dissertation, the implementation of the Nash bargaining theory can exhibit computational difficulties such as a nonconcave objective function (2.18) and nonconvex constraint set (2.19).

It is to be noted that the optimization problem in 2.18 and 2.19 can also be formulated as a variational inequality and solved to obtain a Nash bargaining solution.

2.4. The Euler Method

In this section, I recall the Euler-type method, which is based on the general iterative scheme devised by Dupuis and Nagurney (1993), and its convergence conditions. The Euler method can be utilized for the computation of the variational inequality problem as given in 2.1a.

Specifically, recall that, at an iteration $\tau + 1$ of the Euler method (see also Nagurney and Zhang (1996)), where τ denotes a certain iteration/loop counter, one computes:

$$X^{\tau+1} = P_{\mathcal{K}}(X^{\tau} - \alpha_{\tau} F(X^{\tau})), \tag{2.20}$$

where F is the function in (2.1a), and $P_{\mathcal{K}}$ is the projection on the feasible set $\mathcal{K}$, defined by

$$P_{\mathcal{K}}(X) = arg\ min_{X' \in \mathcal{K}} ||X^{'} - X||. \tag{2.21}$$

Now, I state the Euler method.

Step 0: Initialization

Set $X^0 \in \mathcal{K}$. Let $\tau = 1$ and set the sequence $\{\alpha_{\tau}\}$ so that $\sum_{\tau=1}^{\infty} \alpha_{\tau} = \infty, \alpha_{\tau} > 0$ for all τ, and $\alpha_{\tau} \rightarrow 0$ as $\tau \rightarrow \infty$.

Step 1: Computation

Compute $X^\tau \in \mathcal{K}$ by solving the variational inequality subproblem:

$$\langle X^\tau + \alpha_\tau F(X^{\tau-1}) - X^{\tau-1}, X - X^\tau \rangle \geq 0, \quad \forall X \in \mathcal{K}. \tag{2.22}$$

Step 2: Convergence Verification

If $|X^\tau - X^{\tau-1}| \leq \epsilon$, with $\epsilon > 0$, a pre-specified tolerance, then stop; otherwise, set $\tau = \tau + 1$, and go to Step 1.

As assumption is recalled, followed by the convergence conditions of the Euler method in Theorem 2.17 and Corollary 2.1.

Assumption 2.1

Suppose we fix an initial condition $X_0 \in \mathcal{K}$ *and define the sequence* $\{X_\tau, \tau \in N\}$ *by (2.20). We assume the following conditions:*

1. $\sum_{j=1}^{\infty} a_j = \infty, a_j > 0$ *as* $j \to \infty$.

2. $d(F_\tau(x), \bar{F}(x)) \to 0$ *uniformly on compact subsets of* $\mathcal{K}$ *as* $\tau \to \infty$.

3. *The sequence* $\{X_\tau, \tau \in N\}$ *is bounded.*

Theorem 2.17 (Convergence of the General Iterative Scheme)

Let S denote the set of solutions to the variational inequality problem (2.1a). Assume Assumption 2.1. Suppose $\{X_\tau, \tau \in N\}$ is the scheme generated by (2.20). Then $d(X_\tau, S) \rightarrow 0$ as $\tau \rightarrow \infty$, where $d(X_\tau, S) \rightarrow 0 = \inf_{X \in S} ||X_\tau - X||$.

Corollary 2.1 (Existence of a Solution Under the General Iterative Scheme)

Assume the conditions of Theorem 2.17, and also that S consists of a finite set of points. Then $\lim_{\tau \rightarrow \infty} X_\tau$ exists and equals to a solution to the variational inequality.

Theorem 2.17 indicates that Assumption 2.1 is the elementary condition under which the Euler method (2.20) converges.

In the following chapters, for each model, I derive explicit formulae for the entire strategy vectors in the variational inequalities formulated.

2.5. The Interior Point Method

In this section, I briefly concentrate on the primal-dual Interior Point Method (cf. Boyd and Vandenberghe (2004), Wright (1997)) used to solve the nonlinear programming problem formulations of Nash bargaining and system-optimization in Chapter 5. The algorithm was induced by an Interior Point nonlinear programming solver. For this work, I used SAS/OR 9.3 version of the software released in 2011 and available through the SAS Studio. The software offers the Interior Point and Active-Set algorithms (SAS (2011)). Through the tool, one can allow multi-start (multiple initial points) and can alter termination criterion. However for my purpose, I gave a single initial start and let the algorithm terminate on its own to obtain optimal solutions.

To simplify the notation, consider the following nonlinear programming problem:

$$Minimize \;\; h(X), \tag{2.23}$$

subject to:

$$g_i(X) \geq 0, \quad \forall i \tag{2.24}$$

$$X \in \mathcal{K}.$$

Note that the above problem can also include equality constraints. Initially, slack variables are added to the inequality constraints, giving rise to the problem

$$Minimize \;\; h(X),$$

subject to:

$$g_i(X) - e_i = 0, \quad \forall i \tag{2.25}$$

$$e \geq 0, X \in \mathcal{K},$$

where $e = (e_1, ..., e_m)^T$ represents the vector of slack variables. The nonnegativity constraints are eliminated by incorporating them into the objective function via a logarithmic function. This gives rise to the following equality-constrained nonlinear problem.

$$Minimize \;\; B(X, e) = h(X) - \mu \sum_{i=1}^{m} ln(e_i), \tag{2.26}$$

subject to:

$$g_i(X) - e_i = 0, \quad \forall i,$$

$$e \geq 0, X \in \mathcal{K},$$

where μ is a positive parameter. This is called a barrier problem. The logarithmic function prohibits e from taking zero or negative values. The size of the parameter μ determines a minimum of the barrier problem that provides an approximation to the original nonlinear problem. The smaller the size, the better the approximations. For various values of $\mu, \mu \to 0$, the barrier problem is repeatedly solved to obtain a minimum.

To solve the barrier problem, its Lagrangian function is defined here.

$$\mathcal{L}_B(X, e, \mathcal{Z}) = B(X, e) - \mathcal{Z}^T(g(X) - e),$$

$$\mathcal{L}_B(X, e, \mathcal{Z}) = h(X) - \mu \sum_{i=1}^{m} ln(e_i) - \mathcal{Z}^T(g(X) - e). \tag{2.27}$$

The first order optimality conditions are:

$$\nabla_X \mathcal{L}_B = \nabla_X h(X) - J(X)^T \mathcal{Z} = 0, \tag{2.28}$$

$$\nabla_e \mathcal{L}_B = \mu E^{-1} \mathcal{J} + \mathcal{Z} = 0, \tag{2.29}$$

$$g(X) - e = 0, \tag{2.30}$$

where $J(X)$ represents the Jacobian of the vector function $g(X)$, E represents the diagonal matrix whose elements are the elements of the vector e ($E = diag\{e_1, ..., e_m\}$) and $\mathcal{J}$ is the vector of all ones. The above can be reproduced to the following equivalent nonlinear system:

$$\nabla_X h(X) - J(X)^T \mathcal{Z} = 0,$$

$$\mu \mathcal{J} + E\mathcal{Z} = 0,$$

$$g(X) - e = 0. \tag{2.31}$$

If $\mu = 0$, the conditions above represent optimality conditions of the original optimization problem, after adding slack variables. The goal of the algorithm is to reduce the value of μ to zero so that it converges to the optimum of the original nonlinear problem. The rate at which it approaches zero affects the efficiency of the algorithm.

At an iteration τ, the algorithm approximately solves the preceding system by using Newton's method.

$$\begin{pmatrix} H_{\mathcal{L}}(X^\tau, \mathcal{Z}^\tau) & 0 & -J(X^\tau)^T \\ 0 & \mathcal{Z}^\tau & E^\tau \\ J(X^\tau) & -I & 0 \end{pmatrix} \begin{pmatrix} \Delta X^\tau \\ \Delta e^\tau \\ \Delta \mathcal{Z}^\tau \end{pmatrix} = \begin{pmatrix} \nabla_X h(X^\tau) - J(X^\tau)^T \mathcal{Z} \\ \mu \mathcal{J} + E^\tau \mathcal{Z}^\tau \\ g(X^\tau) - e^\tau \end{pmatrix},$$

where $H_{\mathcal{L}}$ is the Hessian matrix of the Lagrangian function $\mathcal{L} = h(X) - \mathcal{Z}^T g(X)$ of the original nonlinear problem, that is, $H_{\mathcal{L}}(X, \mathcal{Z}) = \nabla^2 h(X) - \sum_{i=1}^{m} \mathcal{Z}_i \nabla^2 g_i(X)$.

The solution $(\Delta X^\tau, \Delta e^\tau, \Delta \mathcal{Z}^\tau)$ of the Newton system provides a direction to move from the current iteration $(X^\tau, e^\tau, \mathcal{Z}^\tau)$ to the next, $(X^{\tau+1}, e^{\tau+1}, \mathcal{Z}^{\tau+1}) = (X^\tau, e^\tau, \mathcal{Z}^\tau) + a(\Delta X^\tau, \Delta e^\tau, \Delta \mathcal{Z}^\tau)$,

where a is the step length along the Newton direction. The step length is determined through a line-search procedure that ensures sufficient decrease of a merit function based on the augmented Lagrangian function of the barrier problem. The role of the merit function and the line-search procedure is to ensure that the objective and the infeasibility reduce sufficiently at every iteration and that the iterations approach an optimum of the original NLP problem.

CHAPTER 3

A SUPPLY CHAIN GAME THEORY FRAMEWORK FOR CYBERSECURITY INVESTMENTS UNDER NETWORK VULNERABILITY

In this chapter, I develop a supply chain game theory model consisting of two tiers: the retailers and the consumers. The retailers select the product transactions and their security levels so as to maximize their expected profits. The probability of a successful attack on a retailer depends not only on that retailer's investment in security but also on the security investments of the other retailers. Hence, the retailers and consumers are connected. In some of the previous work in the cybersecurity investment space (see Nagurney and Nagurney (2015)), it was assumed that the probability of a successful attack on a seller depended only on his own security investments. In retail, which I consider in a broad sense here from consumer goods to even financial services, including retail banks, decision-makers interact and may share common suppliers, IT providers, etc. Hence, it is imperative to capture the network effects associated with security investments and the associated impacts.

In this model, retailers seek to maximize their expected profits with the prices that the consumers are willing to pay for the product being a function not only of the demand but also of the average security in the supply chain which I refer to as the cybersecurity or network security. The retailers compete noncooperatively until a Nash Equilibrium is achieved, whereby no retailer can improve upon his expected profit by making a unilateral decision in changing his product transactions and security level. The approach is inspired, in part, by the work of Shetty et al. (2009), but it is significantly more general since the retailers, that is, the firms, are not identical and I explicitly also capture the demand side of the supply chain network. Moreover, the retailers may be faced with distinct security investment cost functions, given their existing IT infrastructure and business scope and size, and they can also be spatially separated. This framework can handle both online retailers and brick and mortar ones. In addition, the retailers are faced with, possibly, different financial damages in the case of a cyberattack. For simplicity of exposition and clarity, I focus on a single type of attack.

This chapter is based on Nagurney, Nagurney, and Shukla (2015). The supply chain game theory model is developed in Section 3.1. The behavior of the retailers is captured, the Nash Equilibrium defined, and the variational inequality formulation derived. I also provide some qualitative properties of the equilibrium product transaction and security level pattern. In Section 3.2, I outline the algorithm that I then utilize in Section 3.3 to compute solutions to the numerical examples. In two sets of numerical supply chain network examples, I illustrate the impacts of a variety of changes on the equilibrium solution, and on the retailer and supply chain network vulnerability. In Section 3.4, I summarize the results and present the conclusions along with suggestions for future research.

3.1. The Supply Chain Game Theory Model of Cybersecurity Investments Under Network Vulnerability

I consider m retailers that are spatially separated and that sell a product to n consumers. The retailers may be online retailers, engaging with consumers through electronic commerce, and/or brick and mortar retailers. Since my focus here is on cybersecurity, that is, network security, I assume that the transactions in terms of payments for the product occur electronically through credit cards and/or debit cards. Consumers may also conduct searches to obtain information through cyberspace. I emphasize that here we consider retailers in a broad sense, and they may include consumer goods retailers, pharmacies, high technology product outlets, and even financial service firms as well as retail banks. The network topology of the supply chain model, which consists of a tier of retailers and a tier of consumers, is depicted in Figure 3.1.

Since the Internet is needed for the transactions between retailers and consumers to take place, network security is relevant. Each retailer in the model may be susceptible to a cyberattack through the supply chain network since retailers may interact with one another as well as with common suppliers and also share consumers. The retailers may suffer from financial damage as a consequence of a successful cyberattack, losses due to identity theft, opportunity costs, as well as a loss in reputation, etc. Similarly, consumers are sensitive as to how secure their transactions are with the retailers.

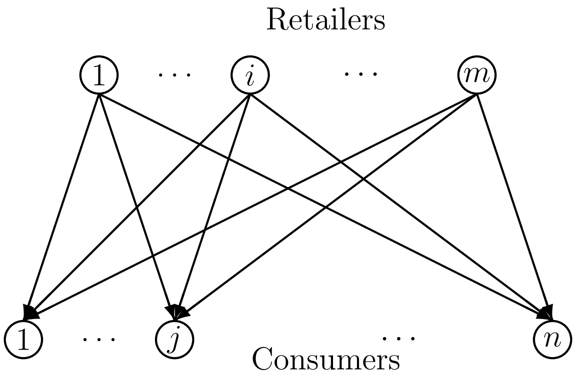

Figure 3.1: The network structure of the supply chain game theory model

I denote a typical retailer by i and a typical consumer by j. Let Q_{ij} denote the nonnegative volume of the product transacted between retailer i and consumer j. Here s_i denotes the network security level, or, simply, the security of retailer i. The strategic variables of retailer i consist of his product transactions $\{Q_{i1}, \ldots, Q_{in}\}$ and his security level s_i. I group the product transactions of all retailers into the vector $Q \in R^{mn}_+$ and the security levels of all retailers into the vector $s \in R^m_+$. All vectors here are assumed to be column vectors, except where noted.

Let $s_i \in [0, 1]$, with a value of 0 meaning no network security and a value of 1 representing perfect security. Therefore,

$$0 \leq s_i \leq 1, \quad i = 1, \ldots, m. \tag{3.1}$$

The network security level of the retail-consumer supply chain is denoted by $\bar{s}$ and is defined as the average network security where

$$\bar{s} = \frac{1}{m}\sum_{i=1}^{m} s_i. \tag{3.2}$$

Let p_i denote the probability of a successful cyberattack on retailer i in the supply chain network. Associated with the successful attack is the incurred financial damage D_i. Distinct retailers may suffer different amounts of financial damage as a consequence of a cyberattack due to their size and their existing infrastructure including cyber infrastructure. As discussed in Shetty (2010) and Shetty et al. (2009), but for an oligopoly model with identical firms and no demand side represented in the network, p_i depends on the chosen security level s_i and on the network security level $\bar{s}$ as in (3.2). Using similar arguments as therein, I also define the probability p_i of a successful cyberattack on retailer i as

$$p_i = (1 - s_i)(1 - \bar{s}), \quad i = 1, \ldots, m, \tag{3.3}$$

where the term $(1-\bar{s})$ represents the probability of a cyberattack in the supply chain network and the term $(1 - s_i)$ represents the probability of success of such an attack on retailer i. The network vulnerability level $\bar{v} = 1 - \bar{s}$ with retailer i's vulnerability level v_i being $1 - s_i$; $i = 1, \ldots, m$.

In terms of cybersecurity investment, each retailer i, in order to acquire security s_i, encumbers an investment cost $h_i(s_i)$ with the function assumed to be continuously differentiable and convex. Note that distinct retailers, because of their size and existing cyber infrastructure (both hardware and software), may be faced with different investment cost functions. I assume that, for a given retailer i, $h_i(0) = 0$ denotes an entirely insecure retailer and $h_i(1) = \infty$ is the investment cost associated with complete security for the retailer (see Shetty (2010) and Shetty et al. (2009)). An example of a suitable $h_i(s_i)$ function is

$$h_i(s_i) = \alpha_i(\frac{1}{\sqrt{(1-s_i)}} - 1) \text{ with } \alpha_i > 0. \tag{3.4}$$

The term α_i allows for different retailers to have distinct investment cost functions based on their size and needs.

The demand for the product by consumer j is denoted by d_j and it must satisfy the following conservation of flow equation:

$$d_j = \sum_{i=1}^{m} Q_{ij}, \quad j = 1, \ldots, n, \tag{3.5}$$

where

$$Q_{ij} \geq 0, \quad i = 1, \ldots, m; j = 1, \ldots, n, \tag{3.6}$$

that is, the demand for each consumer is satisfied by the sum of the product transactions between all the retailers with the consumer. I group the demands for the product for all buyers into the vector $d \in R^n_+$.

The consumers reveal their preferences for the product through their demand price functions, with the demand price function for consumer j, ρ_j, being:

$$\rho_j = \rho_j(d, \bar{s}), \quad j = 1, \ldots, n. \tag{3.7}$$

Observe that the demand price depends, in general, on the quantities transacted between the retailers and the consumers and the network security level. The consumers are only aware of the *average* network security level of the supply chain. This is reasonable since consumers may have information about a retail industry in terms of its cyber investments and security but it is unlikely that individual consumers would have information on individual retailers' security levels. Hence, as in the model of Nagurney and Nagurney (2015), there is information asymmetry (cf. Akerlof (1970)).

In view of (3.2) and (3.5), I define $\hat{\rho}_j(Q, s) \equiv \rho_j(d, \bar{s})$, $\forall j$. These demand price functions are assumed to be continuously differentiable, decreasing with respect to the respective consumer's own demand and increasing with respect to the network security level.

The revenue of retailer i; $i = 1, \ldots, m$, (in the absence of a cyberattack) is:

$$\sum_{j=1}^{n} \hat{\rho}_j(Q, s) Q_{ij}. \tag{3.8}$$

Each retailer i; $i = 1, \ldots, m$, is faced with a cost c_i associated with the processing and the handling of the product and transaction costs $c_{ij}(Q_{ij})$; $j = 1 \ldots, m$, in dealing with the consumers. His total cost, hence, is given by:

$$c_i \sum_{j=1}^{n} Q_{ij} + \sum_{j=1}^{n} c_{ij}(Q_{ij}). \tag{3.9}$$

The transaction costs, in the case of electronic commerce, can include the costs of transporting/shipping the product to the consumers. The transaction costs can also include the cost of using the network services, taxes, etc. I assume that the transaction cost functions are convex and continuously differentiable.

The profit f_i of retailer i; $i = 1, \ldots, m$, (in the absence of a cyberattack and security investment) is the difference between the revenue and his costs, that is,

$$f_i(Q, s) = \sum_{j=1}^{n} \hat{\rho}_j(Q, s)Q_{ij} - c_i \sum_{j=1}^{n} Q_{ij} - \sum_{j=1}^{n} c_{ij}(Q_{ij}). \tag{3.10}$$

If there is a successful cyberattack, a retailer i; $i = 1, \ldots, m$, incurs an expected financial damage given by

$$D_i p_i, \tag{3.11}$$

where D_i takes on a positive value.

Using expressions (3.3), (3.10), and (3.11), the expected utility, $E(U_i)$, of retailer i; $i = 1, \ldots, m$, which corresponds to his expected profit, is:

$$E(U_i) = (1 - p_i)f_i(Q, s) + p_i(f_i(Q, s) - D_i) - h_i(s_i). \tag{3.12}$$

I group the expected utilities of all the retailers into the m-dimensional vector $E(U)$ with components: $\{E(U_1), \ldots, E(U_m)\}$.

Let K^i denote the feasible set corresponding to retailer i, where $K^i \equiv$

$\{(Q_i, s_i) | Q_i \geq 0, \text{ and } 0 \leq s_i \leq 1\}$ and define $K \equiv \prod_{i=1}^{m} K^i$.

The m retailers compete noncooperatively in supplying the product and invest in cybersecurity, each one trying to maximize his own expected profit. I seek to determine a nonnegative product transaction and security level pattern (Q^*, s^*) for which the m retailers will be in a state of equilibrium as defined below. Nash (1950a) and Nash (1951) generalized Cournot's concept (see Cournot (1838)) of an equilibrium for a model of several players, that is, decision-makers, each of which acts in his/her own self-interest, in what has been come to be called a noncooperative game.

Definition 3.1: A Supply Chain Nash Equilibrium in Product Transactions and Security Levels

A product transaction and security level pattern $(Q^*, s^*) \in K$ is said to constitute a supply chain Nash Equilibrium if for each retailer $i; i = 1, \ldots, m$,

$$E(U_i(Q_i^*, s_i^*, \hat{Q}_i^*, \hat{s}_i^*)) \geq E(U_i(Q_i, s_i, \hat{Q}_i^*, \hat{s}_i^*)), \quad \forall (Q_i, s_i) \in K^i, \tag{3.13}$$

where

$$\hat{Q_i^*} \equiv (Q_1^*, \ldots, Q_{i-1}^*, Q_{i+1}^*, \ldots, Q_m^*); \quad \textit{and} \quad \hat{s_i^*} \equiv (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_m^*). \tag{3.14}$$

According to (3.13), an equilibrium is established if no retailer can unilaterally improve upon his expected profits by selecting an alternative vector of product transactions and security levels.

3.1.1. Variational Inequality Formulations

I now present alternative variational inequality formulations of the above supply chain Nash equilibrium in product transactions and security levels.

Theorem 3.1: Variational Inequality Formulation

Assume that, for each retailer i; $i = 1, \dots, m$, the expected profit function $E(U_i(Q,s))$ is concave with respect to the variables $\{Q_{i1}, \dots, Q_{in}\}$, and s_i, and is continuous and continuously differentiable. Then $(Q^*, s^*) \in K$ is a supply chain Nash Equilibrium according to Definition 3.1 if and only if it satisfies the variational inequality

$$-\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{\partial E(U_i(Q^*,s^*))}{\partial Q_{ij}} \times (Q_{ij} - Q^*_{ij}) - \sum_{i=1}^{m} \frac{\partial E(U_i(Q^*,s^*))}{\partial s_i} \times (s_i - s^*_i) \geq 0,$$

$$\forall (Q,s) \in K, \quad (3.15)$$

or, equivalently, $(Q^*, s^*) \in K$ is a supply chain Nash equilibrium product transaction and security level pattern if and only if it satisfies the variational in-

equality

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\left[c_i+\frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}}-\hat{\rho}_j(Q^*,s^*)-\sum_{k=1}^{n}\frac{\partial\hat{\rho}_k(Q^*,s^*)}{\partial Q_{ij}}\times Q_{ik}^*\right]\times(Q_{ij}-Q_{ij}^*)$$

$$+\sum_{i=1}^{m}\left[\frac{\partial h_i(s_i^*)}{\partial s_i}-(1-\sum_{j=1}^{m}\frac{s_j^*}{m}+\frac{1-s_i^*}{m})D_i-\sum_{k=1}^{n}\frac{\partial\hat{\rho}_k(Q^*,s^*)}{\partial s_i}\times Q_{ik}^*\right]\times(s_i-s_i^*)\geq 0,$$

$$\forall(Q,s)\in K. \quad (3.16)$$

Proof: (3.15) follows directly from Gabay and Moulin (1980) and Dafermos and Nagurney (1987).

In order to obtain variational inequality (3.16) from variational inequality (3.15), I note that, at the equilibrium:

$$-\frac{\partial E(U_i)}{\partial Q_{ij}}=c_i+\frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}}-\hat{\rho}_j(Q^*,s^*)-\sum_{k=1}^{n}\frac{\partial\hat{\rho}_k(Q^*,s^*)}{\partial Q_{ij}}\times Q_{ik}^*;\quad\forall i,\forall j,\ (3.17)$$

and

$$-\frac{\partial E(U_i)}{\partial s_i}=\frac{\partial h_i(s_i^*)}{\partial s_i}-(1-\sum_{j=1}^{m}\frac{s_j^*}{m}+\frac{1-s_i^*}{m})D_i-\sum_{k=1}^{n}\frac{\partial\hat{\rho}_k(Q^*,s^*)}{\partial s_i}\times Q_{ik}^*;\quad\forall i.\quad (3.18)$$

Making the respective substitutions using (3.17) and (3.18) in variational inequality (3.15) yields variational inequality (3.16) □

I now put the above Nash Equilibrium problem into standard variational inequality form (cf. (2.1a)), that is: determine $X^* \in \mathcal{K} \subset R^N$, such that

$$\langle F(X^*), X - X^* \rangle \geq 0, \quad \forall X \in \mathcal{K}, \tag{3.19}$$

where F is a given continuous function from $\mathcal{K}$ to R^N and $\mathcal{K}$ is a closed and convex set.

I define the $(mn + m)$-dimensional vector $X \equiv (Q, s)$ and the $(mn + m)$-dimensional vector $F(X) = (F^1(X), F^2(X))$ with the (i, j)-th component, F^1_{ij}, of $F^1(X)$ given by

$$F^1_{ij}(X) \equiv -\frac{\partial E(U_i(Q, s))}{\partial Q_{ij}}, \tag{3.20}$$

the i-th component, F^2_i, of $F^2(X)$ given by

$$F^2_i(X) \equiv -\frac{\partial E(U_i(Q, s))}{\partial s_i}, \tag{3.21}$$

and with the feasible set $\mathcal{K} \equiv K$. Then, clearly, variational inequality (3.15) can be put into standard form (3.19).

In a similar way, one can prove that variational inequality (3.16) can also be put into standard variational inequality form (3.19). □

3.1.2. Qualitative Properties

It is reasonable to expect that the expected utility of any seller i, $E(U_i(Q,s))$, would decrease whenever his product volume has become sufficiently large, that is, when $E(U_i)$ is differentiable, $\frac{\partial E(U_i(Q,s))}{\partial Q_{ij}}$ is negative for sufficiently large Q_{ij} Hence, the following assumption is not unreasonable:

Assumption 3.1

Suppose that in this supply chain game theory model there exists a sufficiently large M, such that for any (i,j),

$$\frac{\partial E(U_i(Q,s))}{\partial Q_{ij}} < 0, \tag{3.22}$$

for all product transaction patterns Q with $Q_{ij} \geq M$.

I now give an existence result.

Proposition 3.1: Existence

Any supply chain Nash Equilibrium problem in product transactions and security levels, as modeled above, that satisfies Assumption 3.1 possesses at least one equilibrium product transaction and security level pattern.

Proof: The proof follows from Proposition 1 in Zhang and Nagurney (1995).

□

I now present the uniqueness result, the proof of which follows from the basic theory of variational inequalities (cf. Nagurney (1999)).

Proposition 3.2: Uniqueness

Suppose that F is strictly monotone at any equilibrium point of the variational inequality problem defined in (3.19). Then it has at most one equilibrium point.

3.2. The Algorithm

I, now, describe the realization of the Euler method, which is fully discussed in Section 2.4, for the computation of the solution to variational inequality (3.16).

As proven in Dupuis and Nagurney (1993), for convergence of the general iterative scheme, which induces the Euler method, the sequence $\{a_\tau\}$ must satisfy: $\sum_{\tau=0}^{\infty} a_\tau = \infty$, $a_\tau > 0$, $a_\tau \to 0$, as $\tau \to \infty$. Specific conditions for convergence of this scheme as well as various applications to the solutions of other network-based game theory models can be found in Nagurney (2006), Nagurney (2015), and the references therein.

Explicit Formulae for the Euler Method Applied to the Supply Chain Game Theory Model

The elegance of this procedure for the computation of solutions to this model is apparent from the following explicit formulae. In particular, I have the following closed form expression for the product transactions $i = 1, \ldots, m; j = 1, \ldots, n$:

$$Q_{ij}^{\tau+1} = \max\{0, Q_{ij}^{\tau} + a_{\tau}(\hat{\rho}_j(Q^{\tau}, s^{\tau}) + \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^{\tau}, s^{\tau})}{\partial Q_{ij}} Q_{ik}^{\tau} - c_i - \frac{\partial c_{ij}(Q_{ij}^{\tau})}{\partial Q_{ij}})\}, \tag{3.23}$$

and the following closed form expression for the security levels $i = 1, \ldots, m$:

$$s_i^{\tau+1} =$$

$$\max\{0, \min\{1, s_i^{\tau} + a_{\tau}(\sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^{\tau}, s^{\tau})}{\partial s_i} Q_{ik}^{\tau} - \frac{\partial h_i(s_i^{\tau})}{\partial s_i} + (1 - \sum_{j=1}^{m} \frac{s_j}{m} + \frac{1 - s_i}{m}) D_i)\}\}. \tag{3.24}$$

I now provide the convergence result. The proof is direct from Theorem 5.8 in Nagurney and Zhang (1996).

Theorem 3.2: Convergence

In the supply chain game theory model developed above let $F(X) = -\nabla E(U(Q, s))$ be strictly monotone at any equilibrium pattern and assume that Assumption 3.1 is satisfied. Also, assume that F is uniformly Lipschitz continuous. Then *there exists a unique equilibrium product transaction and security level pattern* $(Q^*, s^*) \in K$ *and any sequence generated by the Euler method as given by (3.23) and (3.24), with* $\{a_\tau\}$ *satisfies* $\sum_{\tau=0}^{\infty} a_\tau = \infty$, $a_\tau > 0$, $a_\tau \to 0$, *as* $\tau \to \infty$ *converges to* (Q^*, s^*).

In the next Section, I apply the Euler method to compute solutions to numerical game theory problems.

3.3. Numerical Examples

In Nagurney, Nagurney, and Shukla (2015) the Euler method was implemented, as discussed in Section 3.2, using FORTRAN on a Linux system at the University of Massachusetts Amherst. The convergence criterion was $\epsilon = 10^{-4}$. Hence, the Euler method was considered to have converged if, at a given iteration, the absolute value of the difference of each product transaction and each security level differed from its respective value at the preceding iteration by no more than ϵ.

The sequence $\{a_\tau\}$ was: $.1(1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3} \ldots)$. I initialized the Euler method by setting each product transaction $Q_{ij} = 1.00$, $\forall i, j$, and the security level of each retailer $s_i = 0.00$, $\forall i$.

I present two sets of numerical examples. Each set of examples consists of an example with four variants.

Example Set 3.1

The first set of examples consists of two retailers and two consumers as depicted in Figure 3.2. This set of examples begins with the baseline Example 3.1, followed by four variants. The equilibrium solutions are reported in Table 3.1.

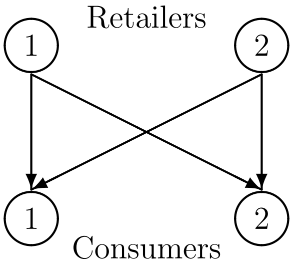

Figure 3.2: Network Topology for Example Set 3.1

The cost function data for Example 3.1 are:

$$c_1 = 5, \quad c_2 = 10,$$

$$c_{11}(Q_{11}) = .5Q_{11}^2 + Q_{11}, \quad c_{12}(Q_{12}) = .25Q_{12}^2 + Q_{12},$$

$$c_{21}(Q_{21}) = .5Q_{21}^2 + 2, \quad c_{22}(Q_{22}) = .25Q_{22}^2 + Q_{22}.$$

The demand price functions are:

$$\rho_1(d, \bar{s}) = -d_1 + .1(\frac{s_1 + s_2}{2}) + 100, \quad \rho_2(d_2, \bar{s}) = -.5d_2 + .2(\frac{s_1 + s_2}{2}) + 200.$$

The damage parameters are: $D_1 = 50$ and $D_2 = 70$ with the investment functions taking the form:

$$h_1(s_1) = \frac{1}{\sqrt{(1-s_1)}} - 1, \quad h_2(s_2) = \frac{1}{\sqrt{(1-s_2)}} - 1.$$

As can be seen from the results in Table 3.1 for Example 3.1, the equilibrium demand for Consumer 2 is over four times greater than that for Consumer 1. The price that Consumer 1 pays is about one half of that of Consumer 2. Both retailers invest in security and achieve equilibrium security levels of .91. Hence, in Example 3.1 the vulnerability of Retailer 1 is .09 and that of Retailer 2 is also .09, with the network vulnerability being .09.

In the first variant of Example 3.1, Variant 3.1.1, I change the demand price function of Consumer 1 to reflect an enhanced willingness to pay more for the product. The new demand price function for Consumer 1 is:

$$\rho_1(d, \bar{s}) = -d_1 + .1(\frac{s_1 + s_2}{2}) + 200.$$

The product transactions to Consumer 1 more than double from their corresponding values in Example 3.1, whereas those to Consumer 2 remain unchanged. The security level of Retailer 2 increases slightly whereas that of Retailer 1 remains unchanged. Both retailers benefit from increased expected profits. The vulnerability of Retailer 2 is decreased slightly to .08.

Variant 3.1.2 is constructed from Variant 3.1.1. Consumer 2 no longer values the product much so his demand price function is

$$\rho_2(d_2, \bar{s}) = -.5d_2 + .2(\frac{s_1 + s_2}{2}) + 20,$$

with the remainder of the data as in Variant 3.1.1. The product transactions decrease by almost an order of magnitude to the second consumer and the retailers experience reduced expected profits by about 2/3 as compared to those in Variant 3.1.1. The vulnerability of Retailer 1 is now .12 and that of Retailer 2: .11 with the network vulnerability being: .115.

Variant 3.1.3 is constructed from Example 3.1 by increasing both security investment cost functions so that:

$$h_1(s_1) = 100(\frac{1}{\sqrt{(1-s_1)}} - 1), \quad h_2(s_2) = 100(\frac{1}{\sqrt{(1-s_2)}} - 1)$$

and having new damages: $D_1 = 500$ and $D_2 = 700$. With the increased costs associated with cybersecurity investments both retailers decrease their security levels to the lowest level of all the examples solved, thus far. The vulnerability of Retailer 1 is now .34 and that of Retailer 2: .28 with the network vulnerability =.31.

Variant 3.1.4 has the same data as Variant 3.1.3, but we now further increase Retailer 2's investment cost function as follows:

$$h_2(s_2) = 1000(\frac{1}{\sqrt{(1-s_2)}} - 1).$$

Retailer 2 now has an equilibrium security level that is one quarter of that in Variant 3.1.3. Not only do his expected profits decline but also those of Retailer 1 do.

The vulnerability of Retailer 1 is now: .27 and that of Retailer 2: .82. The network vulnerability for this example is: .54, the highest value in this set of examples. The cybersecurity investment cost associated with Retailer 2 is so high that he greatly reduces his security level. Moreover, the network security is approximately half of that obtained in Example 3.1.

Table 3.1: Equilibrium Solutions for Examples in Set 3.1

Solution	Ex. 3.1	Var. 3.1.1	Var. 3.1.2	Var. 3.1.3	Var. 3.1.4
Q_{11}^*	24.27	49.27	49.27	24.27	24.26
Q_{12}^*	98.30	98.30	8.30	98.32	98.30
Q_{21}^*	21.27	46.27	46.27	21.27	21.26
Q_{22}^*	93.36	93.36	3.38	93.32	93.30
d_1^*	45.55	95.55	95.55	45.53	45.52
d_2^*	191.66	191.66	11.68	191.64	191.59
s_1^*	.91	.91	.88	.66	.73
s_2^*	.91	.92	.89	.72	.18
$\bar{s}^*$	.91	.915	.885	.69	.46
$\rho_1(d_1^*, \bar{s}^*)$	54.55	104.55	104.54	54.54	54.52
$\rho_2(d_2^*, \bar{s}^*)$	104.35	104.35	14.34	104.32	104.30
$E(U_1)$	8136.45	10894.49	3693.56	8121.93	8103.09
$E(U_2)$	7215.10	9748.17	3219.94	7194.13	6991.11

Example Set 3.2

The second set of numerical examples consists of three retailers and two consumers as shown in Figure 3.3.

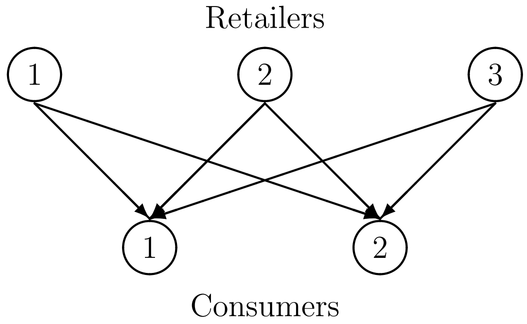

Figure 3.3: Network Topology for Example Set 3.2

In order to enable cross comparisons between the two example sets, Example 3.2 is constructed, which is the baseline example in this set, from Example 3.1 in Set 3.1. Therefore, the data for Example 3.2 is identical to that in Example 3.1 except for the new Retailer 3 data as given below:

$$c_3 = 3, \quad c_{31}(Q_{31}) = Q_{31}^2 + 3Q_{31}, \quad c_{32}(Q_{32}) = Q_{32}^2 + 4Q_{32},$$

$$h_3(s_3) = 3(\frac{1}{\sqrt{(1-s_3)}} - 1), \quad D_3 = 80.$$

The equilibrium solutions for examples in Set 3.2 are reported in Table 3.2. With the addition of Retailer 3, there is now increased competition. As a consequence, the demand prices for the product drop for both consumers and there is an increase in demand. Also, with the increased competition, the expected profits drop for the two original retailers. The demand increases for Consumer 1 and also for Consumer 2, both at upwards of 10%.

The vulnerability of Retailer 1 is .10, that of Retailer 2: .09, and that of

Retailer 3: .19 with a network vulnerability of: .13. The network vulnerability, with the addition of Retailer 3 is now higher, since Retailer 3 does not invest much in security due to the higher investment cost.

Variant 3.2.1 is constructed from Example 3.2 with the data as therein except for the new demand price function for Consumer 1, who now is more sensitive to the network security, where

$$\rho_1(d_1, \bar{s}) = -d_1 + (\frac{s_1 + s_2}{2}) + 100.$$

The expected profit increases for all retailers since Consumer 1 is willing to pay a higher price for the product.

The vulnerability of Retailer 1 is now .08, that of Retailer 2: .08, and that of Retailer 3: .17 with a network vulnerability of: .11. Hence, all the vulnerabilities have decreased, since the retailers have higher equilibrium security levels.

Variant 3.2.2 is constructed from Variant 3.2.1. The only change is that now Consumer 2 is also more sensitive to average security with a new demand price function given by:

$$\rho_2(d_2, \bar{s}) = -.5d_2 + (\frac{s_1 + s_2}{2}) + 200.$$

As shown in Table 3.2, the expected profits are now even higher than for

Variant 2.1. The vulnerability of Retailer 1 is now .05, which is the same for Retailer 2, and with Retailer 3 having the highest vulnerability at: .14. The network vulnerability is, hence, .08. Consumers' willingness to pay for increased network security reduces the retailers' vulnerability and that of the supply chain network.

Variants 3.2.1 and 3.2.2 demonstrate that consumers who care about security can also enhance the expected profits of retailers of a product through their willingness to pay for higher network security.

Variant 3.2.3 has the identical data to that in Variant 3.2.2 except that the demand price functions are now:

$$\rho_1(d_1, \bar{s}) = -2d_2 + (\frac{s_1 + s_2}{2}) + 100, \quad \rho_2(d_2, \bar{s}) = -d_2 + (\frac{s_1 + s_2}{2}) + 100.$$

As can be seen from Table 3.2, the product transactions have all decreased substantially, as compared to the respective values for Variant 3.2.2. Also, the demand prices associated with the two consumers have decreased substantially as have the expected profits for all the retailers.

The vulnerabilities of the retailers are, respectively: .07, 07, and .16 with the network vulnerability equal to .10.

Variant 3.2.4 is identical to Variant 3.2.3 except that now the demand price function sensitivity for the consumers has increased even more so that:

$$\rho_1(d_1, \bar{s}) = -2d_2 + 10(\frac{s_1 + s_2}{2}) + 100, \quad \rho_2(d_2, \bar{s}) = -d_2 + 10(\frac{s_1 + s_2}{2}) + 100.$$

All the equilibrium product transactions now increase. The demand prices have both increased as have the expected profits of all the retailers.

In this example, the vulnerabilities of the retailers are, respectively: .02, .02, and .05, yielding a network vulnerability of .03. This is the least vulnerable supply chain network in this numerical study.

Table 3.2: Equilibrium Solutions for Examples in Set 3.2

Solution	Ex. 3.2	Var. 3.2.1	Var. 3.2.2	Var. 3.2.3	Var. 3.2.4
Q_{11}^*	20.80	20.98	20.98	11.64	12.67
Q_{12}^*	89.45	89.45	89.82	49.62	51.84
Q_{21}^*	17.81	17.98	17.98	9.64	10.67
Q_{22}^*	84.49	84.49	84.83	46.31	48.51
Q_{31}^*	13.87	13.98	13.98	8.73	9.50
Q_{32}^*	35.41	35.41	35.53	24.50	25.59
d_1^*	52.48	52.94	52.95	30.00	32.85
d_2^*	209.35	209.35	210.18	120.43	125.94
s_1^*	.90	.92	.95	.93	.98
s_2^*	.91	.92	.95	.93	.98
s_3^*	.81	.83	.86	.84	.95
$\bar{s}^*$	.87	.89	.917	.90	.97
$\rho_1(d_1^*, \bar{s}^*)$	47.61	47.95	47.96	40.91	44.01
$\rho_2(d_2^*, \bar{s}^*)$	95.50	95.50	95.83	80.47	83.77
$E(U_1)$	6654.73	6665.88	6712.29	3418.66	3761.75
$E(U_2)$	5830.06	5839.65	5882.27	2913.31	3226.90
$E(U_3)$	2264.39	2271.25	2285.93	1428.65	1582.62

3.4. Summary and Conclusions

Cybercrime is affecting companies as well as other organizations and establishments, including governments, and consumers. Recent notable data breaches have included major retailers in the United States, resulting in both financial damage and a loss in reputation. With companies, many of which are increasingly global and dependent on their supply chains, seeking to determine how much they should invest in cybersecurity, a general framework that can quantify the investments in cybersecurity in supply chain networks is needed. The framework should also be able to illuminate the impacts on profits as well as a firm's vulnerability and that of the supply chain network.

In this chapter, I develop a supply chain network game theory model consisting of a tier of retailers and a tier of consumers. The retailers may be subject to a cyberattack and seek to maximize their expected profits by selecting their optimal product transactions and cybersecurity levels. The firms compete noncooperatively until a Nash Equilibrium is achieved, whereby no retailer can improve upon his expected profits. The probability of a successful attack on a retailer, in my framework, depends not only on his security level, but also on that of the other retailers. Consumers reveal their preferences for the product through the demand price functions, which depend on the demand and on the network security level, which is the average security of the supply chain network.

I derive the variational inequality formulation of the governing equilibrium conditions, discuss qualitative properties, and demonstrate that the algorithm that I propose has nice features for computations. Specifically, it yields, at each iteration, closed form expressions for the product transactions between retailers and consumers and closed form expressions for the retailer security levels. The algorithm is then applied to compute solutions to two sets of numerical examples, with a total of ten examples. The examples illustrate the impacts of an increase in competition, changes in the demand price functions, changes in the damages incurred, and changes in the cybersecurity investment cost functions on the equilibrium solutions and on the incurred prices and the expected profits of the retailers. I also provide the vulnerability of each retailer in each example and the network vulnerability.

The approach of applying game theory and variational inequality theory with expected utilities of decision-makers to network security / cybersecurity that this chapter adopts is original in itself. The results in this work pave the way for a range of investigative questions and research avenues in this area. For instance, at present, the model considers retailers and consumers in the supply chain network. However, it can be extended to include additional tiers, namely, suppliers, as well as transport service providers, and so on. The complexity of the supply chain network would then make it even more susceptible to cyberattacks, in which a security lapse in one node can affect many others in succession. Moreover, to account for the fact that the exchange of data takes place through multiple forms, the model could be extended to include multiple modes of transactions.

While the solution equilibrium in the context of competition does moderate investments, the model can also be extended to explicitly include constraints on cybersecurity investments subject to expenditure budgets allocated to cybersecurity. The numerical examples section dealt with multiple retailer and consumer scenarios and their variants to validate the ease of adoption and practicality of the model. A case study and empirical analysis can further corroborate the cogency of the model and assist in the process of arriving at investment decisions related to cybersecurity. This could also provide insights as to how to strike a balance between effectiveness of service and security.

CHAPTER 4

A SUPPLY CHAIN NETWORK GAME THEORY MODEL OF CYBERSECURITY INVESTMENTS WITH NONLINEAR BUDGET CONSTRAINTS

In this chapter, a supply chain network game theory model of cybersecurity investments consisting of a tier of retailers and a tier of demand markets is developed. The retailers can be consumer goods retailers, high tech retailers, or even financial service ones. What is needed is that they are in the same industry and that their individual decisions may impact the decisions of the others in terms of the volume of product handled and the level of cybersecurity investment. This work builds on that of Shetty (2010), Shetty et al. (2009), and Chapter 3 but with a crucial difference – the retailers are now subject to individual budget constraints for their cybersecurity investments. These constraints are nonlinear, posing challenges for both theory (Section 2.2) and computations (Section 2.4). In addition, unlike in Chapter 3, each retailer has a distinct upper bound on security levels of retailers and product transactions between retailers and consumers at the demand markets.

This chapter is organized as follows. In Section 4.1, I present the supply chain network game theory model with competing retailers, who seek to individually maximize their expected utilities, which capture the expected revenue and financial losses, in the case of a cyberattack, along with the costs associated with cybersecurity investments. I also discuss how to measure the vulnerability of a firm to cyberattacks and that of the supply chain network, as a whole. The Nash Equilibrium conditions, theoretical foundations, and variational inequality formulations are provided. In the first variational inequality formulation, the nonlinear budget constraints appear in the feasible set and, in the alternative one, through the use of Lagrange multipliers, the nonlinear constraints are captured in the function that enters the variational inequality with the feasible set consisting of the nonnegative orthant and the bounds on the security levels. In Section 4.2, I present the algorithm, with nice features for computations, that yields, at each iteration, closed form expressions for the product transactions, the security levels, and the Lagrange multipliers associated with the budget constraints of the retailers. In Section 4.3, I present the numerical examples and, in Section 4.1, I summarize and conclude. This chapter is based on Nagurney, Daniele, and Shukla (2017).

4.1. The Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints

The supply chain network game theory model of cybersecurity investments with nonlinear budget constraints consists of m retailers, with a typical retailer denoted by i, and n demand markets, with a typical demand market denoted by j. Retailers may be brick and mortar stores or online retailers. In this framework, I consider retailer in a broad sense in that a retailer may correspond to a financial service firm such as a retail bank, a consumer goods store, etc. I do assume that the retailers transact the same product. Since the concern is with cybersecurity investments, the transactions between the two tiers take place electronically in terms of payments and, hence, there may be a possibility of cyberattacks with the concomitant financial damage, loss of reputation, opportunity costs, and associated disruptions. Specifically, consumers at the demand markets make their purchases by credit or debit cards or via an online payment system. They reflect their preferences as to the cybersecurity of the supply chain network through the demand price functions. The information that they have available is the average supply chain network cybersecurity, which is referred to as the supply chain network security or, simply, the network security. One can expect consumers at the demand markets to have information as to the security in an industry rather than the individual retailer cybersecurity levels. Since here I am concerned with supply chain aspects, the retailers share some connectivity and may be exposed to cyberattacks through their suppliers, and/or possibly, common payment systems, or even computer infrastructure.

The bipartite network structure of the problem is depicted in Figure 4.1 and the notation for the model is presented in Table 4.1. The network topology is similar to that in Chapter 3. However, there are important notational additions in Table 4.1.

I first present the constraints and then construct the objective function of each retailer. I also discuss how we quantify the cybersecurity of the supply chain network along with its vulnerability, and that of the individual retailers. One of the challenging aspects of the model is that the budget constraints are nonlinear and, hence, convexity of the feasible sets of the retailers must be established.

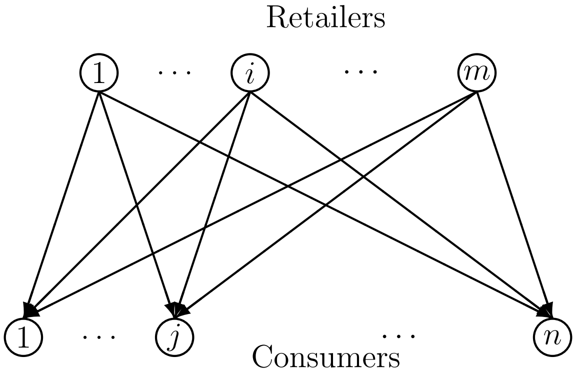

Figure 4.1: The Bipartite Structure of the Supply Chain Network Game Theory Model

Notation	Definition
Q_{ij}	the amount of the product transacted between retailer i and demand market j; $i = 1, ..., m; j = 1, ..., n$. The transactions $\{Q_{ij}\}$ for retailer i are grouped into the vector $Q_i \in R^n_+$ and all the transactions of all retailers into the vector $Q \in R^{mn}_+$.
d_j	the demand for the product at demand market $j; j = 1, ..., n$. The demands are grouped into the vector $d \in R^n_+$.
s_i	the cybersecurity level of retailer $i; i = 1, ..., m$. The security levels of all retailers are grouped into the vector $s \in R^m_+$.
$\bar{s}$	the cybersecurity level in the supply chain network, where $\bar{s} = \frac{1}{m}\sum_{k=1}^{m} s_k$.
p_i	the probability of a successful cyberattack on retailer i.
c_i	the cost associated with handling and processing the product at retailer $i; i = 1, ..., m$.
$c_{ij}(Q_{ij})$	the transaction cost associated with transacting between i and j; $i = 1, ..., m; j = 1, ..., n$.
$\rho_j(d, \bar{s})$	the demand price of the product at demand market $j; j = 1, ..., n$.
B_i	the budget of retailer i for cyberinvestments, which cannot be exceeded;$i = 1, ..., m$.
D_i	the financial damage accrued by retailer i after a successful cyberattack on $i; i = 1, ..., m$.
Q_{ij}	the upper bound on the product transaction between i and j; $i = 1, ..., m; j = 1, ..., n$.
u_{s_i}	the upper bound on the security level of retailer i; $i = 1, ..., m$.

Table 4.1: Notation for the Model

The demand for the product at demand market j must satisfy the following conservation of flow equation:

$$d_j = \sum_{i=1}^{m} Q_{ij}, \quad j = 1, ..., n, \tag{4.1}$$

where

$$0 \leq Q_{ij} \leq \bar{Q}_{ij}, \quad i = 1, ..., m; j = 1, ..., n, \tag{4.2}$$

that is, the demand at each demand market is satisfied by the sum of the product transactions between the retailers with the demand market, and these transactions must be nonnegative and not exceed the imposed upper bounds.

The cybersecurity level or, simply, security, of each retailer i must satisfy the following constraint:

$$0 \leq s_i \leq u_{s_i}, \quad i = 1, ..., m, \tag{4.3}$$

where $u_{s_i} < 1$ for all $i; i = 1, ..., m$. The larger the value of s_i, the higher the security level, with perfect security reflected in a value of 1, but, since perfect security might not be attainable, $u_{s_i} < 1; i = 1, ..., m$. If $s_i = 0$ this means that retailer i has no security.

Associated with acquiring a security level s_i is an investment cost function $h_i; i = 1, ..., m$, with the function assumed to be continuously differentiable and convex. It is assumed that, for a given retailer i, $h_i(0) = 0$ denotes an entirely insecure retailer and $h_i(1) = \infty$ is the investment cost associated with complete security for the retailer. An example of an $h_i(s_i)$ function that satisfies these properties and that is utilized in this model as

$$h_i(s_i) = \alpha_i(\frac{1}{\sqrt{1 - s_i}} - 1), \quad \alpha_i > 0. \tag{4.4}$$

The term α_i enables distinct retailers to have different investment cost functions based on their size and needs. Such functions were introduced by Shetty (2010) and Shetty et al. (2009) and also used in Chapter 3. However, in those models, there are no cybersecurity budget constraints and the cybersecurity investment cost functions only appear in the objective functions of the decision-makers.

In this model, each retailer is faced with a limited budget for cybersecurity investment. Hence, the following nonlinear budget constraints must be satisfied:

$$\alpha_i(\frac{1}{\sqrt{1-s_i}} - 1) \leq B_i; \quad i = 1, ..., m, \tag{4.5}$$

that is, each retailer can't exceed his allocated cybersecurity budget. Clearly, the constraints in (4.5) are nonlinear and pose challenges for the analysis and solution of our model, which, as demonstrated, can be overcome.

As in Shetty et al. (2009) and Shetty (2010), probability p_i of a successful cyberattack on retailer i is defined as

$$p_i = (1 - s_i)(1 - \bar{s}), \quad i = 1, ..., m, \tag{4.6}$$

where the term $(1-\bar{s})$ represents the probability of a cyberattack on the supply chain network and the term $(1 - s_i)$ represents the probability of success of an attack on retailer i. The supply chain network vulnerability level $\bar{v} = 1 - \bar{s}$ with retailer i's vulnerability level v_i being $1 - s_i; i = 1, ..., m$. Such measures are also used in Nagurney, Nagurney, and Shukla (2015).

In view of (4.1), demand price functions are defined as $\hat{\rho}_j(Q, s) \equiv \rho_j(d, \bar{s}), \forall j$. The consumers reflect their preferences for the product through the demand price functions, which depend not only on the vector of demands but also on the supply chain network security. The consumers are expected to be willing to pay more for enhanced network security but the degree may differ from consumer to consumer. Also, there is information asymmetry (cf. Akerlof (1970)) in the model, since retailers are aware of their investments in cybersecurity, but consumers known only the average security as defined by $\bar{s}$.

The profit f_i of retailer $i; i = 1, ..., m$ (in the absence of a cyberattack and security investment) is the difference between the revenue and costs, that is,

$$f_i(Q, s) = \sum_{j=1}^{n} \hat{\rho}_j(Q, s) Q_{ij} - c_i \sum_{j=1}^{n} Q_{ij} - \sum_{j=1}^{n} c_{ij}(Q_{ij}). \tag{4.7}$$

If there is a successful cyberattack on a retailer $i; i = 1, ..., m$, he incurs an expected financial damage given by

$$D_i p_i, \tag{4.8}$$

where D_i takes on a positive value.

Using expressions (4.6), (4.7), and (4.8), the expected utility, $E(U_i)$, of retailer $i; i = 1, ..., m$, which corresponds to the retailer's expected profit, is:

$$E(U_i) = (1 - p_i) f_i(Q, s) + p_i(f_i(Q, s) - D_i) - h_i(s_i)$$

$$= f_i(Q, s) - p_i D_i - h_i(s_i). \tag{4.9}$$

According to (4.9), each retailer encumbers the cost associated with its cybersecurity investment. On grouping the expected utilities of all the retailers into the m-dimensional vector $E(U)$, the following components are obtained: $\{E(U_1), ..., E(U_m)\}$.

Let K^i denote the feasible set corresponding to retailer i, where $K^i \equiv \{(Q_i, s_i) | 0 \leq Q_{ij} \leq \bar{Q}_{ij}, \forall j$, and $0 \leq s_i \leq u_{s_i}$ and (4.5) holds for $i\}$ and define $K \equiv \prod_{i=1}^{m} K^i$.

The m retailers compete noncooperatively in supplying the product and invest in cybersecurity, each one trying to maximize his own expected profit. I seek to determine a nonnegative product transaction and security level pattern $(Q^*, s^*) \in K$ for which the m retailers will be in a state of equilibrium as defined below. Nash (1950a, 1951) generalized Cournot's concept (see Cournot (1838)) of an equilibrium for a model of several players, that is, decision-makers, each of which acts in his/her own self-interest, in what has been come to be called a noncooperative game.

Definition 4.1: A Supply Chain Nash Equilibrium in Product Transactions and Security Levels

A product transaction and security level pattern $(Q^*, s^*) \in K$ *is said to constitute a supply chain Nash Equilibrium if for each retailer* $i; i = 1, \ldots, m$*,*

$$E(U_i(Q_i^*, s_i^*, \hat{Q}_i^*, \hat{s}_i^*)) \geq E(U_i(Q_i, s_i, \hat{Q}_i^*, \hat{s}_i^*)), \quad \forall (Q_i, s_i) \in K^i, \tag{4.10}$$

where

$$\hat{Q_i^*} \equiv (Q_1^*, \ldots, Q_{i-1}^*, Q_{i+1}^*, \ldots, Q_m^*); \hat{s_i^*} \equiv (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_m^*). \tag{4.11}$$

According to (4.10), a supply chain network equilibrium is established if no retailer can unilaterally improve upon his expected profits by selecting an alternative vector of product transactions and security levels. I now present alternative variational inequality formulations of the above supply chain Nash Equilibrium in product transactions and security levels. It is first established that the feasible set K is convex in the following lemma. In this model, unlike in many network equilibrium problems from congested urban transportation networks to supply chains and financial networks (cf. Nagurney (1999, 2006), Daniele (2006)), the feasible set contains nonlinear constraints.

Lemma 4.1

Let h_i be a convex function for all retailers $i; i = 1, ..., m$. The feasible set K is then convex.

Proof: Convexity of the constraint set is studied below.

$$\bar{K} = \{s_i \in R : h_i(s_i) \leq B_i\}. \tag{4.12}$$

Let $s_i^1, s_i^2 \in \bar{K}$ and $\lambda \in [0, 1]$, namely:

$$h_i(s_i^1) \leq B_i \quad \text{and} \quad h_i(s_i^2) \leq B_i. \tag{4.13}$$

Since $h_i(s_i)$ is a convex function,

$$h_i(\lambda s_i^1 + (1 - \lambda)s_i^2) \leq \lambda \underbrace{h_i(s_i^1)}_{\leq B_i} + (1 - \lambda) \underbrace{h_i(s_i^2)}_{\leq B_i} \leq B_i, \tag{4.14}$$

namely,

$$h_i(\lambda s_i^1 + (1 - \lambda)s_i^2) \leq B_i, \tag{4.15}$$

that is,

$$\lambda s_i^1 + (1 - \lambda)s_i^2 \in \bar{K}. \tag{4.16}$$

Hence, the set defined by (4.12) is convex.

Also, we know that each K_i consists of the above budget constraint, the box-type constraint (4.3) on s_i, and the nonnegativity constraints on retailer i's transactions as in (4.12). The intersection of these sets is also convex. Finally, since K is the Cartesian product of convex sets, $K_i; i = 1, ..., m$, it is also convex, so the conclusion follows. □

Note that each investment cost function $h_i(s_i); i = 1, ..., m$, as in (4.4), and defined on $[0, u_{s_i}]$ is convex since its second derivative is positive. Indeed,

$$h_i^{'}(s_i) = \frac{\alpha_i}{2}(1 - s_i)^{-\frac{3}{2}} \quad \text{and} \quad h_i^{''}(s_i) = \frac{3\alpha_i}{4}(1 - s_i)^{-\frac{5}{2}} > 0. \tag{4.17}$$

Theorem 4.1: Variational Inequality Formulation

Assume that, for each retailer $i; i = 1, ..., m$, the expected profit function $E(U_i(Q, s))$ is concave with respect to the variables $\{Q_{i1}, ..., Q_{in}\}$, and s_i, and is continuously differentiable. Then $(Q^*, s^*) \in K$ is a supply chain Nash Equilibrium according to Definition 4.1 if and only if, $\forall (Q, s) \in K$, it satisfies the variational inequality

$$-\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} \times (Q_{ij} - Q_{ij}^*) - \sum_{i=1}^{m} \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0, \tag{4.18}$$

or, equivalently, $(Q^*, s^*) \in K$ is a supply chain Nash Equilibrium product transaction and security level pattern if and only if it satisfies the variational inequality

$$\sum_{i=1}^{m}\sum_{j=1}^{n} \Big[c_i + \frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n} \frac{\hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} Q_{ik}^*\Big] \times (Q_{ij} - Q_{ij}^*)$$

$$+\sum_{i=1}^{m} \Big[\frac{\partial h_i(s_i^*)}{\partial s_i} - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} Q_{ik}^*$$

$$-(1-\sum_{k=1}^{m}\frac{s_k^*}{m}+\frac{1-s_i^*}{m})D_i\Big]\times(s_i-s_i^*)\geq 0,\quad \forall(Q,s)\in K. \tag{4.19}$$

Proof: As per Lemma 4.1, the feasible set for each retailer i, $K_i; i=1,...,m$, is convex as is the Cartesian product of these sets, K. Under the imposed assumptions on the expected utility functions of the retailers, according to Proposition 2.2 in Gabay and Moulin (1980), which established the equivalence between the solution to a Nash Equilibrium problem and the solution to the corresponding variational inequality problem, we know that each retailer $i; i=1,...,m$, maximizes his expected utility according to Definition 4.1 if and only if, $\forall s_i\in[0,u_{s_i}]$,

$$-\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{\partial E(U_i(Q^*,s^*))}{\partial Q_{ij}}\times(Q_{ij}-Q_{ij}^*)-\sum_{i=1}^{m}\frac{\partial E(U_i(Q^*,s^*))}{\partial s_i}\times(s_i-s_i^*)\geq 0, \tag{4.20}$$

which is precisely variational inequality (4.18).

In order to obtain variational inequality (4.19) from the variational inequality (4.18), note that, at the equilibrium:

$$-\frac{\partial E(U_i)}{\partial Q_{ij}}=c_i+\frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}}-\hat{\rho}_j(Q^*,s^*)-\sum_{k=1}^{n}\frac{\hat{\rho}_k(Q^*,s^*)}{\partial Q_{ij}}Q_{ik}^*;\quad \forall i,j; \tag{4.21}$$

and

$$-\frac{\partial E(U_i)}{\partial s_i}=\frac{\partial h_i(s_i^*)}{\partial s_i}-\sum_{k=1}^{n}\frac{\partial\hat{\rho}_k(Q^*,s^*)}{\partial s_i}Q_{ik}^*-(1-\sum_{k=1}^{m}\frac{s_k^*}{m}+\frac{1-s_i^*}{m})D_i),\forall i. \tag{4.22}$$

Substituting the above expressions into variational inequality (4.20), variational inequality (4.18) is obtained. □

The variational inequality (4.18) can be put into the standard variational inequality form as depicted in (2.1a). I define the $(mn+m)$-dimensional column vector $X \equiv (Q,s)$ and the $(mn+m)$-dimensional column vector $F(X) \equiv (F^1(X), F^2(X))$ with the (i,j)-th component, F^1_{ij}, of $F^1(X)$ given by

$$F^1_{ij} \equiv -\frac{\partial E(U_i(Q,s))}{\partial Q_{ij}}, \tag{4.23}$$

the i-th component, F^2_i, of $F^2(X)$ given by

$$F^2_{ij} \equiv -\frac{\partial E(U_i(Q,s))}{\partial s_i}, \tag{4.24}$$

and with the feasible set $\mathcal{K} \equiv K$. Then, clearly, variational inequality (4.18) can be put into standard form (2.1a). In a similar way, one can prove that (4.19) can also be put into the standard form (2.1a).

Additional background on the variational inequality problem can be found in Nagurney (1999).

Remark

If the retailers are not subject to budget constraints, $u_{s_i} = 1$, for $i = 1, ..., m$, and there are no upper bounds on the product transactions, then the above model collapses to the model in Chapter 3 with the associated variational inequalities having the same structure as those in (4.18) and (4.19) but with a substantially simpler feasible set which consists of the nonnegative orthant for the product transactions and the security levels, with the latter also bounded from above by one. Such a model, nevertheless, can be used to identify the (Q^*, s^*) under "ideal" unlimited conditions as to budgets and product transactions. Now, some qualitative properties are provided, in terms of existence and uniqueness of a solution to variational inequality (4.18).

Theorem 4.2: Existence

A solution (Q^*, s^*) *to variational inequality (4.18) (equivalently, (4.19)) is guaranteed to exist.*

Proof: The result follows from the classical theory of variational inequalities (see Kinderlehrer and Stampacchia (1980), and Section 2.1) since the feasible set K is compact, and the function that enters the variational inequality ((2.1a) with (4.23) and (4.24)) is continuous. □

Moreover, I have the following result.

Theorem 4.3: Uniqueness

The solition (Q^*, s^*) *to variational inequality (4.18) is unique if the function* $F(X)$ *as in (2.1a) with components defined by (4.23) and (4.24), and* $X \equiv$

(Q, s) is strictly monotone, that is:

$$\langle (F(X^1) - F(X^2)), X^1 - X^2 \rangle > 0, \quad \forall X^1, X^2 \in \mathcal{K}, \quad X^1 \neq X^2. \qquad (4.25)$$

Proof: See Kinderlehrer and Stampacchia (1980) and Section 2.1.

The function $F(X)$ is strictly monotone over $\mathcal{K}$ if its Jacobian $\nabla F(X)$ is positive definite over $\mathcal{K}$.

Since the feasible set K has nonlinear constraints and this may pose challenges for numerical computations, now an alternative variational inequality to (4.19) which incorporates Lagrange multipliers is derived. Specifically, the Lagrange multiplier $\lambda_i \geq 0; i = 1, ..., m$ are associated with the budget constraint (4.5), respectively, for each retailer $i = 1, ..., m$. The Lagrange multipliers are grouped into the vector $\lambda \in R^{mn}_+$. The new variational inequality is defined over the feasible set $\mathcal{K}^2 \equiv \prod_{i=1}^m \mathcal{K}^1_i \times R^{mn}_+$, where $\mathcal{K}^1_i \equiv \{(Q_i, s_i) | Q_i \geq 0; 0 \leq s_i \leq u_{s_i}\}$.

The following section shows that this novel variational inequality will be amenable to solution via an iterative scheme that is straightforward to implement.

Theorem 4.4: Alternative Variational Inequality Formulation

A vector $(Q^*, s^*, \lambda^*) \in \mathcal{K}^2$ *is a solution to variational inequality (4.19) if and only if it is a solution to the variational inequality:*

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\Big[c_i + \frac{\partial c_{ij}(Q^*_{ij})}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n}\frac{\hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}}Q^*_{ik}\Big] \times (Q_{ij} - Q^*_{ij})$$

$$+\sum_{i=1}^{m}\Big[\frac{\partial h_i(s^*_i)}{\partial s_i} - \sum_{k=1}^{n}\frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i}Q^*_{ik} - (1 - \sum_{k=1}^{m}\frac{s^*_k}{m} + \frac{1 - s^*_i}{m})D_i$$

$$+\frac{\lambda^*_i}{2}\alpha_i(1 - s^*_i)^{-\frac{3}{2}}\Big] \times (s_i - s^*_i) + \sum_{i=1}^{m}\Big[B_i - \alpha_i(\frac{1}{\sqrt{1 - s^*_i}} - 1)\Big] \times (\lambda_i - \lambda^*_i) \geq 0,$$

$$\forall (Q, s, \lambda) \in \mathcal{K}^2. \qquad (4.26)$$

Proof: Each retailer $i; i = 1, ..., m$, according to Definition 4.1, seeks to determine his strategy vector (Q_i, s_i) so as to

$$\text{Maximize}_{(Q_i, s_i)} E(U_i) = (1 - p_i)f_i(Q, s) + p_i(f_i(Q, s) - D_i) - h_i(s_i) \qquad (4.27)$$

subject to:

$$\alpha_i(\frac{1}{\sqrt{(1 - s_i)}} - 1) - B_i \leq 0,$$

$$0 \leq Q_{ij} \leq \bar{Q}_{ij}, \quad j = 1, ..., n,$$

$$0 \leq s_i \leq u_{s_i},$$

where $f_i(Q, s)$ is given by (4.7), $h_i(s_i)$ is given by (4.4), and $p_i = (1 - s_i)(1 - \bar{s})$.

Simplifying the terms in the objective function (4.27) and converting the maximization problem into a minimization problem, the above optimization problem with the newly defined feasible set $\mathcal{K}_i^1$ becomes:

$$\text{Minimization} \quad -f_i(Q,s) + D_i(1-s_i)(1-\bar{s}) + h_i(s_i) \tag{4.28}$$

subject to:

$$\alpha_i(\frac{1}{\sqrt{(1-s_i)}} - 1) - B_i \leq 0,$$

$$(Q_i, s_i) \in \mathcal{K}_i^1.$$

Now, let $X_i \equiv (Q_i, s_i), \hat{X}_i \equiv (X_1, ..., X_{i-1}, X_{i+1}, ..., X_m)$, and $\hat{f}_i(X_i, \hat{X}_i) \equiv -f_i(Q,s) + D_i(1-s_i)(1-\bar{s}) + h_i(s_i)$. One can rewrite retailer i's optimization problem, where $\hat{X}_i^*$ denotes the other retailers' optimal solutions, as:

$$\text{Minimize} \quad \hat{f}_i(X_i, \hat{X}_i^*) \tag{4.29}$$

subject to:

$$g_i(X_i) \leq 0, \tag{4.30}$$

$$X_i \in \mathcal{K}_i^1. \tag{4.31}$$

Note that $g_i(X_i) = \alpha_i(\frac{1}{\sqrt{(1-s_i)}}) - B_i$.

Now the Lagrangian is formed $\mathcal{L}(X_i, \hat{X}_i^*, \lambda_i) = \hat{f}_i(X_i, \hat{X}_i^*) + \lambda_i g_i(X_i)$.

Also, the following assumption is made:

Assumption: (Slater Condition). There exists a Slater vector $\tilde{X}_i \in \mathcal{K}_i^1$ for each $i = 1, ..., m$, such that $g_i(\tilde{X}_i) < 0$.

This is easy to verify.

Then, according to Koshal, Nedic, and Shanbhag (2011), pages 1049-1051, since $\hat{f}_i$ is convex in X_i and is continuously differentiable and g_i is also convex and continuously differentiable, and $\mathcal{K}_i^1$ is nonempty, closed and convex, $(X_i^*, \lambda_i^*) \in \mathcal{K}_i^1 \times R_+$ is a solution to the above optimization problem (4.29), subject to (4.30) and (4.31), if and only if it is a solution to the variational inequality:

$$\nabla_{X_i}\mathcal{L}(X_i^*, \hat{X}_i^*, \lambda_i^*) \times (X_i - X_i^*) + (-g_i(X_i^*)) \times (\lambda_i - \lambda_i^*) \geq 0, \quad \forall (X_i, \lambda_i) \in \mathcal{K}_i^1 \times R_+, \tag{4.32}$$

with $\nabla_{X_i}\mathcal{L}$ representing the gradient with respect to X_i of the Lagrangian $\mathcal{L}$.

Expanding (4.32) by using the definitions of these functions and vectors and making the appropriate substitutions, it is obtained that $X_i^* \in \mathcal{K}_i^1$ is a solution to (4.32) if and only if $(Q_i^*, s_i^*, \lambda_i^*) \in \mathcal{K}_i^1$ is a solution to the variational inequality:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \Big[c_i + \frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n} \frac{\hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} Q_{ik}^* \Big] \times (Q_{ij} - Q_{ij}^*)$$

$$+ \sum_{i=1}^{m} \Big[\frac{\partial h_i(s_i^*)}{\partial s_i} - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} Q_{ik}^* - (1 - \sum_{k=1}^{m} \frac{s_k^*}{m} + \frac{1 - s_i^*}{m}) D_i + \frac{\lambda_i^*}{2} \alpha_i (1 - s_i^*)^{-\frac{3}{2}} \Big] \times (s_i - s_i^*)$$

$$+\sum_{i=1}^{m}\Big[B_i-\alpha_i(\frac{1}{\sqrt{1-s_i^*}}-1)\Big]\times(\lambda_i-\lambda_i^*)\geq 0,\quad \forall(Q_i,s_i,\lambda_i)\in\mathcal{K}_i^1. \quad (4.33)$$

But inequality (4.33) holds for each $i; i=1,...,m$, since I am dealing with a Nash Equilibrium problem, so summation of (4.33) over all $i; i=1,...,m$, the variational inequality (4.26) is obtained.□

Now, variational inequality (4.26) into standard form (2.1a). Let $X\equiv(Q,s,\lambda)$ and let $F(X)\equiv(\hat{F}^1(X),\hat{F}^2(X),\hat{F}^3(X))$ be the $(mn{+}2m)$-dimensional vector consisting of components: $\hat{F}^1_{ij}; i=1,...,m; j=1,...,n, \hat{F}^2_i; i=1,...,m$, and $\hat{F}^3_i(X); i=1,...,m$, where:

$$\hat{F}^1_{ij}(X)\equiv\Big[c_i+\frac{\partial c_{ij}(Q_{ij})}{\partial Q_{ij}}-\hat{\rho}_j(Q,s)-\sum_{k=1}^{n}\frac{\hat{\rho}_k(Q,s)}{\partial Q_{ij}}Q_{ik}\Big],\forall i,\forall j,$$

$$\hat{F}^2_i(X)\equiv\Big[\frac{\partial h_i(s_i)}{\partial s_i}-\sum_{k=1}^{n}\frac{\partial\hat{\rho}_k(Q,s)}{\partial s_i}Q_{ik}-(1-\sum_{k=1}^{m}\frac{s_k}{m}+\frac{1-s_i}{m})D_i+\frac{\lambda_i}{2}\alpha_i(1-s_i)^{-\frac{3}{2}}\Big],\forall i,$$

$$\hat{F}^3_i(X)\equiv\Big[B_i-\alpha_i(\frac{1}{\sqrt{1-s_i}}-1)\Big],\forall i.$$

Also, let $\mathcal{K}\equiv\mathcal{K}^2$. Then, clearly, variational inequality (4.26) can be put into standard form (2.1a).

4.2. The Computational Procedure

I, now, describe the realization of the Euler method (cf. Chapter 2), which is fully discussed in Section 2.4, for the computation of the solution to variational inequality (4.26).

As proven in Dupuis and Nagurney (1993), for convergence of the general iterative scheme, which induces the Euler method, the sequence $\{a_\tau\}$ must satisfy: $\sum_{\tau=0}^{\infty} a_\tau = \infty$, $a_\tau > 0$, $a_\tau \to 0$, as $\tau \to \infty$. Specific conditions for convergence of this scheme as well as various applications to the solutions of other network-based game theory models can be found in Nagurney and Zhang (1996) and Nagurney (2006).

Explicit Formulae for the Euler Method Applied to the Game Theory Model

The elegance of this algorithm for the variational inequality (4.26) for the computation of solutions to this model is apparent from the following explicit formulae. In particular, I have the following closed form expression for the product transactions $i = 1, ..., m; j = 1, ..., n$:

$$Q_{ij}^{\tau+1} = \max\{0,$$

$$\min\{\bar{Q}_{ij}, \bar{Q}_{ij} + a_\tau(\hat{\rho}_j(Q^\tau, s^\tau) + \sum_{k=1}^{n} \frac{\hat{\rho}_k(Q^\tau, s^\tau)}{\partial Q_{ij}} Q_{ik}^\tau - c_i - \frac{\partial c_{ij}(Q_{ij}^\tau)}{\partial Q_{ij}})\}\}, \quad (4.34)$$

the following closed form expressions for the security levels, and for the Lagrange multipliers, respectively, for $i = 1, ..., m$:

$$s_i^{\tau+1} = \max\{0, \min\{u_{s_i}, s_i^\tau + a_\tau$$

$$(\sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^\tau, s^\tau)}{\partial s_i} Q_{ik}^\tau - \frac{\partial h_i(s_i^\tau)}{\partial s_i} + (1 - \sum_{k=1}^{m} \frac{s_k^\tau}{m} + \frac{1 - s_i^\tau}{m}) D_i - \frac{\lambda_i^\tau}{2} \alpha_i (1 - s_i^\tau)^{-\frac{3}{2}})\}\}, \tag{4.35}$$

$$\lambda_i^{\tau+1} = \max\{0, \lambda_i^\tau + a_\tau(-B_i + \alpha_i(\frac{1}{\sqrt{(1 - s_i^\tau)}}))\}. \tag{4.36}$$

4.3. Numerical Examples

In Nagurney, Daniele, and Shukla (2017) the Euler method was implemented, as discussed in Section 4.2, using FORTRAN on a Linux system at the University of Massachusetts Amherst. The convergence criterion was $\epsilon = 10^{-4}$. Hence, the Euler method was considered to have converged if, at a given iteration, the absolute value of the difference of each product transaction and each security level differed from its respective value at the preceding iteration by no more than ϵ.

The sequence $\{a_\tau\}$ was: $.1(1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3} \ldots)$. The Euler method was initialized by setting each product transaction $Q_{ij} = 1.00$, $\forall i, j$, the security level of each retailer $s_i = 0.00$, $\forall i$, and the Lagrange multiplier for each retailer's budget constraint $\lambda_i = 0.00; \forall i$. The capacities $\bar{Q}_{ij}$ were set to 100 for all i, j.

The examples were constructed to reflect recent data in specific industrial reports as discussed below.

The examples had transaction cost functions of the following form:

$$c_{ij}(Q_{ij}) = a_{ij}Q_{ij}^2 + b_{ij}Q_{ij}, \quad i = 1, ..., m; j = 1, ..., n,$$

and demand price functions of the following form:

$$\hat{\rho}_j(Q, s) = -m_j(\sum_{i=1}^{m} Q_{ij}) + r_j(\sum_{i=1}^{m} \frac{s_i}{m}) + q_j, \quad j = 1, ..., n,$$

with a_{ij}, b_{ij}, m_j, r_j, and q_j all greater than zero, for all i and j.

Note that the transaction cost functions are strictly convex and the demand price functions are decreasing in the quantity demanded at a demand market but increasing in the average security level at the demand market. I expect that the consumers are willing to pay a higher price for a higher level of average security. The transaction cost functions include the transportation costs and having such functions being increasing functions of the product volume has been used in many network equilibrium problems (see Nagurney (1999, 2006) and the references therein).

It is straightforward to verify that, with the above functions, the assumptions of Theorem 4.1. Indeed, for all i and j:

$$\frac{\partial^2 E(U_i)}{\partial Q_{ij}^2} = -2m_{ij} - 2a_{ij} < 0$$

and

$$\frac{\partial^2 E(U_i)}{\partial s_i^2} = -\frac{3\alpha_i}{4}(1 - s_i)^{-\frac{5}{3}} - 2\frac{D_i}{m} < 0, \quad \forall s_i \in [0, u_{s_i}].$$

Hence, the expected utility of each retailer i, $E(U_i); i = 1, ..., m$, is concave with respect to its strategic variables: $Q_{i1}, Q_{i2}, ..., Q_{in}$ and s_i. In fact, these functions are strictly concave. Clearly, the expected utilities are also twice continuously differentiable.

4.3.1. Examples 4.1 and 4.2 with Sensitivity Analysis

Examples 4.1 and 4.2, with the accompanying sensitivity analysis, consist of two retailers and two demand markets as depicted in Figure 4.2.

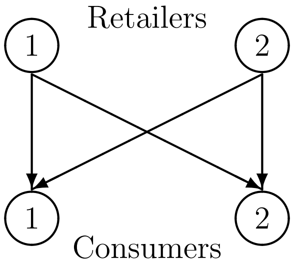

Figure 4.2: Network Topology for Examples 4.1 and 4.2 and Sensitivity Analysis

Example 4.1 and Sensitivity Analysis

The cost function data for Example 4.1 are:

$$c_1 = 5, \quad c_2 = 10,$$

$$c_{11}(Q_{11}) = .5Q_{11}^2 + Q_{11}, \quad c_{12}(Q_{12}) = .25Q_{12}^2 + Q_{12},$$

$$c_{21}(Q_{21}) = .5Q_{21}^2 + 2, \quad c_{22}(Q_{22}) = .25Q_{22}^2 + Q_{22}.$$

The demand price functions are:

$$\rho_1(d,\bar{s}) = -d_1 + .1(\frac{s_1+s_2}{2}) + 100, \quad \rho_2(d_2,\bar{s}) = -.5d_2 + .2(\frac{s_1+s_2}{2}) + 200.$$

The damage parameters are: $D_1 = 50$ and $D_2 = 70$ with the investment functions taking the form:

$$h_1(s_1) = \frac{1}{\sqrt{(1-s_1)}} - 1, \quad h_2(s_2) = \frac{1}{\sqrt{(1-s_2)}} - 1.$$

The damage parameters are in millions of \$US, the expected profits (and revenues) and the costs are also in millions of \$US. The prices are in thousands of dollars and the product transactions are in thousands. The budgets for the two retailers are identical with $B_1 = B_2 = 2.5$ (in millions of \$US). These data are representative for financial damages, due to a cyberattack, as reported by Yakowicz (2014), and for cybersecurity budgets of medium-sized to large firms, as reported by PricewaterhouseCoopers (2014) in their survey.

The computed equilibrium solution for this example is given in Table 4.2.

Retailer 1 has .21 (in millions) in unspent cybersecurity funds whereas Retailer 2 has .10 (in millions) in unspent funds. Hence, the associated Lagrange multipliers $\lambda_1^* = \lambda_2^* = 0.00$. Both retailers have a firm vulnerability of .09 and the network vulnerability is, hence, also .09. In the sensitivity analysis, the budget of Retailer 2 is fixed at 2.5 (in millions of \$US dollars), and the

Table 4.2: Equilibrium Solution for Example 4.1

Solution	Example 4.1
Q_{11}^*	24.27
Q_{12}^*	98.34
Q_{21}^*	21.27
Q_{22}^*	93.34
d_1^*	45.55
d_2^*	191.68
s_1^*	.91
s_2^*	.91
$\bar{s}^*$	.91
λ_1^*	0.00
λ_2^*	0.00
$\rho_1(d_1^*, \bar{s}^*)$	54.55
$\rho_2(d_2^*, \bar{s}^*)$	104.35
$E(U_1)$	8137.38
$E(U_2)$	7213.49

budget of Retailer 1 is varied from $B_1 = 1$ to $B_1 = 2.5$ in increments of .5. The values for the equilibrium security levels of the retailers, along with the network vulnerability, are reported in Figure 4.3. Figure 4.3 shows that, as the budget of Retailer 1 increases, its equilibrium security level increases, and the network vulnerability decreases. Hence, even Retailer 2 benefits from an increase in budget of Retailer 1.

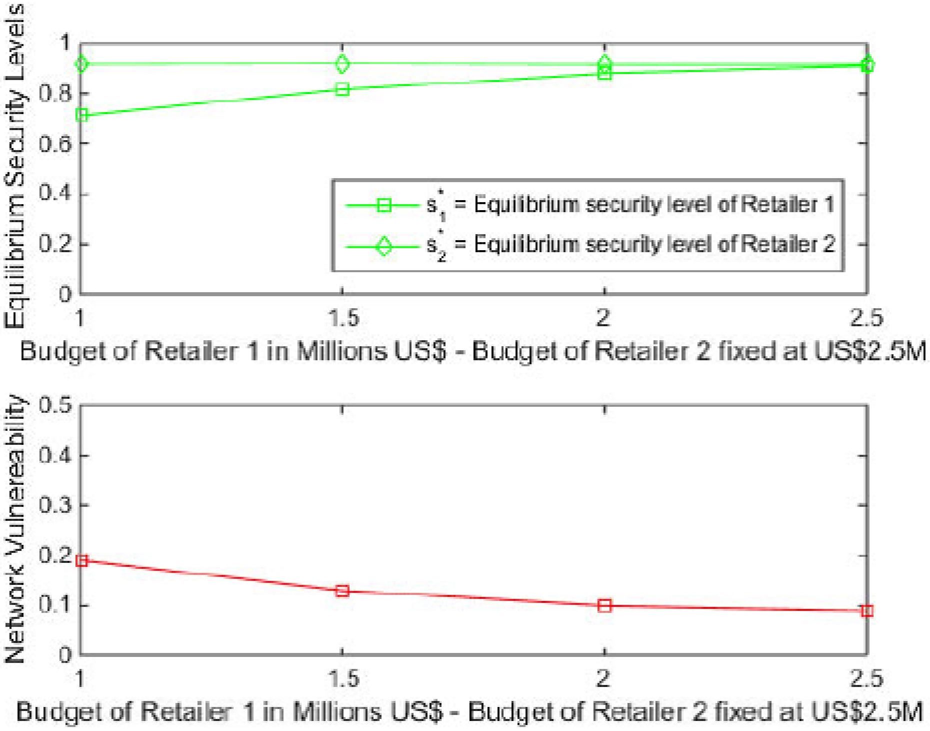

Figure 4.3: Sensitivity Analysis for Example 4.1 for Budget Size Variations of Retailer 1 with Retailer 2's Budget Fixed

Example 4.2 and Sensitivity Analysis

Example 4.2 was constructed from Example 4.1 and had the same data except that the investment cost function for Retailer 1 is now changed to:

$$h_1(s_1) = 10\frac{1}{\sqrt{(1-s_1)}} - 1$$

Such a change in an investment cost function could occur, for example, in the case of acquisition of additional computers that need to be protected with additional associated costs. The equilibrium solution is reported in Table 4.3.

Table 4.3: Equilibrium Solution for Example 4.2

Solution	Example 4.2
Q_{11}^*	24.27
Q_{12}^*	98.31
Q_{21}^*	21.27
Q_{22}^*	93.31
d_1^*	45.53
d_2^*	191.62
s_1^*	.36
s_2^*	.91
$\bar{s}^*$	.63
λ_1^*	3.68
λ_2^*	1.06
$\rho_1(d_1^*, \bar{s}^*)$	54.55
$\rho_2(d_2^*, \bar{s}^*)$	104.32
$E(U_1)$	8122.77
$E(U_2)$	7207.47

With higher security investment cost for Retailer 1, in Example 4.2, he invests less in security then he had in Example 4.1. The average security drops from $\bar{s}^* = .91$ in Example 4.1 to $\bar{s}^* = .63$ in Example 4.2 so that the network vulnerability $1 - \bar{s}^* = .09$ in Example 1 whereas $\bar{v} = .37$ in Example 4.2, an increase of over a factor of 4. Also, the equilibrium Lagrange multipliers are now no longer equal at 0.00 since the budgets of both retailers are now fully spent. The equilibrium product flows remain the same or decrease slightly. Both firms suffer a drop in expected profits.

A sensitivity analysis was conducted for this example. The results are reported in Figure 4.4. The network vulnerability is consistently higher for each datapoint in Figure 4.4 as compared to the respective datapoint in Figure 4.3. These results demonstrate how increased cybersecurity investment costs can dramatically affect the vulnerability of the supply chain network as to cyberattacks. Also, they reveal that the budget size of one retailer can have system-wide effects not only in terms of network vulnerability but also in terms of expected profits.

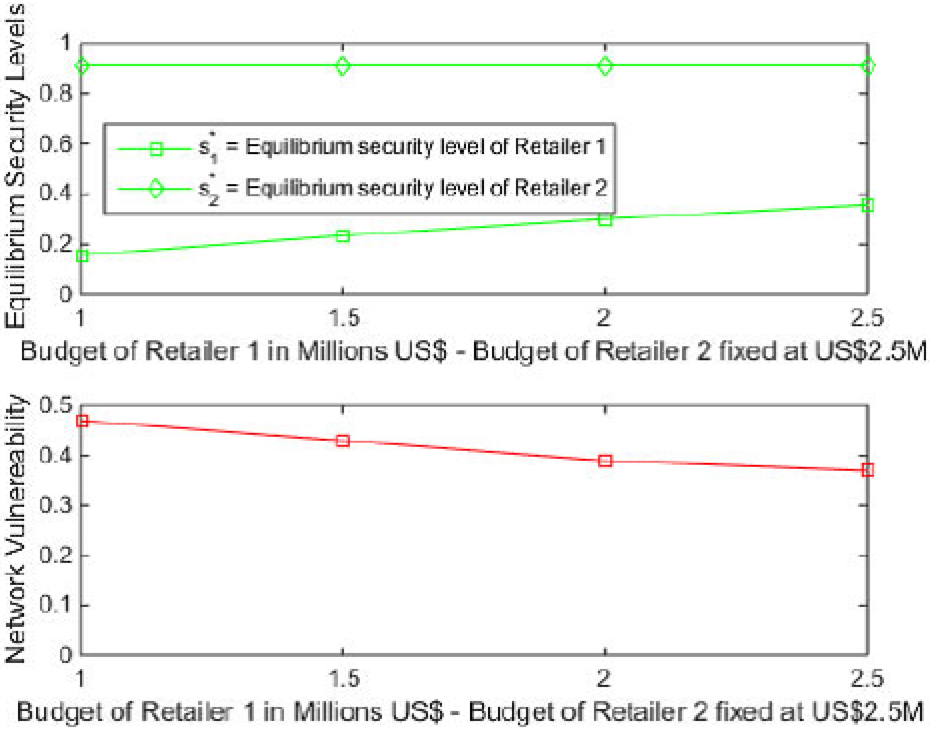

Figure 4.4: Sensitivity Analysis for Example 4.2 for Budget Size Variations of Retailer 1 with Retailer 2's Budget Fixed

4.3.2. Examples 4.3 and 4.4 with Sensitivity Analysis

Examples 4.3 and 4.4 consist of 3 retailers and 2 demand markets as depicted in Figure 4.5.

Example 4.3 and Sensitivity Analysis

Example 4.3 is constructed from Example 4.1 except for the new Retailer 3 data as given below:

$$c_3 = 3, \quad c_{31}(Q_{31}) = Q_{31}^2 + 3Q_{31}, \quad c_{32}(Q_{32}) = Q_{32}^2 + 4Q_{32},$$

$$h_3(s_3) = 3(\frac{1}{\sqrt{(1-s_3)}} - 1), \quad D_3 = 80.$$

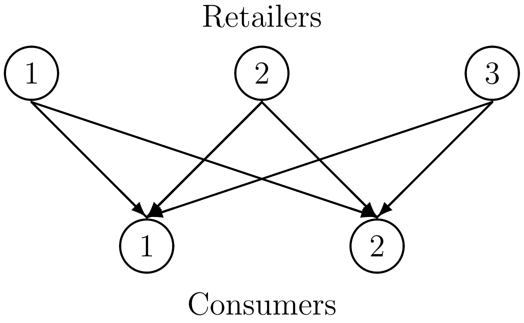

Figure 4.5: Network Topology for Examples 4.3 and 4.4 with Sensitivity Analysis

The budget for Retailer 3 is 3.0 (in millions of $US).

The equilibrium solutions for Example 4.3 are reported in Table 4.4.

With the addition of Retailer 3, there is now increased competition. As a consequence, the demand prices for the product drop at both demand markets and there is an increase in demand. Also, with the increased competition, the expected profits drop for the two original retailers. The demand increases for Demand Market 1 and also for Demand Market 2, both at upwards of 10%.

The vulnerability of Retailer 1 is .10, that of Retailer 2: .09, and that of Retailer 3: .26 with a network vulnerability of: .15. The network vulnerability, with the addition of Retailer 3 is now higher, since Retailer 3 does not invest

Table 4.4: Equilibrium Solutions for Example 4.3

Solution	Example 4.3
Q_{11}^*	20.80
Q_{12}^*	89.48
Q_{21}^*	17.80
Q_{22}^*	84.48
Q_{31}^*	13.87
Q_{32}^*	35.40
d_1^*	52.48
d_2^*	209.36
s_1^*	.90
s_2^*	.91
s_3^*	.74
$\bar{s}^*$	.85
λ_1^*	0.00
λ_2^*	0.00
λ_3^*	0.00
$\rho_1(d_1^*, \bar{s}^*)$	47.61
$\rho_2(d_2^*, \bar{s}^*)$	95.49
$E(U_1)$	6655.13
$E(U_2)$	5828.82
$E(U_3)$	2262.26

much in security due to the higher investment cost.

Interestingly, all retailers do not exhaust their cybersecurity budgets. This may be due, in part, to information asymmetry in that the consumers at the demand markets only know the average security in the network and, hence, a retailer may invest less in cybersecurity. Hence, Retailer 3 is, in a sense, a “free rider”.

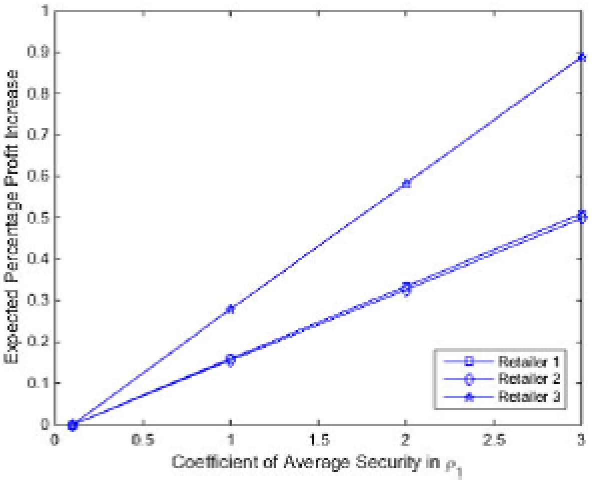

Figure 4.6: Sensitivity Analysis for Example 4.3 for Changes in ρ_1 Average Security Level Coefficient

The above show results of sensitivity analysis. The coefficient in the demand price function at Demand Market 1 is .1. I proceed to increase this coefficient to 1.0, 2.0, and 3.0, and report the percent increase in expected profits of the retailers in Figure 6. All retailers benefit financially from consumers' higher valuation placed on average network security. These examples demonstrate that consumer awareness to supply chain network security, even in an average sense, can benefit retailers in terms of expected profits.

Example 4.4 and Sensitivity Analysis

Example 4.4 is constructed from Example 4.3 as follows. The data are identical except that all the damages: $D_1 = D_2 = D_3 = 0.00$. The computed equilibrium solution is given in Table 4.5.

Table 4.5: Equilibrium Solutions for Example 4.4

Solution	Example 4.4
Q^*_{11}	20.80
Q^*_{12}	89.43
Q^*_{21}	17.80
Q^*_{22}	84.47
Q^*_{31}	13.87
Q^*_{32}	35.40
d^*_1	52.47
d^*_2	209.30
s^*_1	.82
s^*_2	.81
s^*_3	.34
$\bar{s}^*$	.66
λ^*_1	0.00
λ^*_2	0.00
λ^*_3	0.00
$\rho_1(d^*_1, \bar{s}^*)$	47.60
$\rho_2(d^*_2, \bar{s}^*)$	95.48
$E(U_1)$	6652.45
$E(U_2)$	5828.10
$E(U_3)$	2264.24

Increased competition from Retailer 3 continues to increase the demand and decrease the prices when compared to Examples 4.1 and 4.2. However, with a sharp decrease in the damage parameters, that is, from $D_1 = 50, D_2 = 70, D_3 = 80$ to $D_1 = D_2 = D_3 = 0.00$, we observe a fall in the security levels for all the retailers. The average network security is down to 0.66 from 0.85 in the previous example. The vulnerability of Retailer 1 is 0.18, that of Retailer 2 is 0.19, and that of Retailer 3 is 0.66. Retailer 3, having a high investment cost, seems is the most vulnerable due to low investments in cybersecurity.

Interestingly, all retailers do not exhaust their cybersecurity budgets. This may be due, in part, to information asymmetry in that the consumers at the demand markets only know the average security in the network and, hence, a retailer may invest less in cybersecurity.

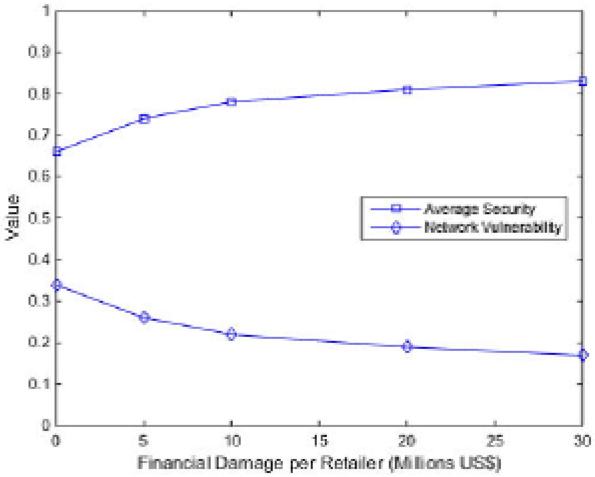

Figure 4.7: Sensitivity Analysis for Example 4.4 for Changes in Financial Damages with $D_1 = D_2 = D_3$

In Figure 4.7, I display the results of the sensitivity analysis. The damages are increased for the retailers from $D_1 = D_2 = D_3 = 0.00$ to $D_1 = D_2 = D_3 = 5.00$ and then to $D_1 = D_2 = D_3 = 10.00$, followed by increments of 10.00 through 30.00. As the damages increase, the average security levels go up and the network vulnerability goes down. Retailers become more sensitive to building security as the damages accrued due to a successful cyberattack increase.

4.4. Summary and Conclusions

Increasing cybercrime incidents, and associated impacts, emphasize the importance of investment into counteracting these events for companies and other organizations, including financial institutions, retailers, and governments. Several of the recent notable data breaches and thefts have been reported by retailers in the United States, wherein financial damage, theft of critical information, and reputation loss took place. Complexities in the supply chains with numerous spatially dispersed entry points have led to loopholes that attackers have exploited. Retailers, being in the forefront, have become highly susceptible to breaches and ensuing losses. As a result, they seek to determine the optimal level of investments to be made given strict budget constraints for cybersecurity. This chapter builds a general framework for quantifying these investments in the backdrop of competing retailers trying to maximize their expected profits subject to budget constraints. The game theory framework also identifies the vulnerability of the individual retailers and that of the supply chain network on the whole.

A bipartite supply chain network game theory model consisting of retailers and demand markets is developed. The retailers may be subject to a cyberattack and seek to maximize their expected profits by selecting their optimal product transactions and cybersecurity levels. The retailers compete noncooperatively until a Nash Equilibrium is achieved, whereby no retailer can improve upon his expected profit. The probability of a successful attack on a retailer, in our framework, depends not only on his security level, but also on that of the other retailers. Consumers at the demand markets reveal their preferences for the product through the demand price functions, which depend on the demand and on the network security level, which is the average security of the supply chain network. Nonlinear investment cost functions levied on each retailer who is bounded by a budget level are included. These nonlinear budget constraints are incorporated into a variational inequality formulation through two alternative variational inequality formulations.

The governing equilibrium conditions and convexity of the feasible set have been derived for the variational inequalities, and the solvability is demonstrated with an appropriate algorithm with features supporting computations. Specifically, the algorithm yielded closed form expressions for the product transactions between retailers and demand markets, the security levels of retailers, as well as the Lagrange multipliers associated with the budget constraints at each iteration. Various data instances are evaluated through the algorithm, with relevant managerial insights and sensitivity analysis. The latter is conducted on the budgets, the coefficients of the demand price functions, and the damage parameters for pertinent analysis. The examples illustrate the impacts of an increase in competition, changes in the demand price functions, changes in the damages incurred, and changes in the cybersecurity investment cost functions, and budgets on the equilibrium solutions and on the incurred prices and the expected profits of the retailers. Vulnerability of each retailer in each example and the network vulnerability are also provided.

CHAPTER 5

MULTIFIRM MODELS OF CYBERSECURITY INVESTMENTS: COMPETITION VS. COOPERATION

In this chapter, I present three new models of cybersecurity investments. The proposed models are not restricted to the number of firms, their locations, or the sectors that they belong to. I begin with a Nash Equilibrium model of noncooperation and competition, which is formulated, analyzed, and solved using variational inequality theory. The solution to this Nash Equilibrium model then serves as the disagreement point over which the bargaining takes place in the second model, which is one of cooperation. For this model, I utilize Nash bargaining theory, a type of cooperative game theory, to argue for the sharing of information on firms' security levels, where here security refers to cybersecurity. I assume that firms bargain with each other to decide upon the security levels that they would be willing to implement vis-a-vis their investment cost functions, wealth, and damages in the case of a cyberattack. The constraints guarantee that the expected utility of each firm is no lower than that obtained under the Nash Equilibrium solution.

The third model in this chapter also focuses on cooperation among the firms in terms of their cybersecurity levels, but from a system-optimization perspective in which the sum of the expected utilities of all the firms is maximized. System-optimization models, but different from the one proposed here, were also developed for cybersecurity investments by Shetty et al. (2009) and Shetty (2010).

In addition to the model developments and the associated theory, here I also apply and compare the obtained solutions in terms of firm and network vulnerability. Moreover, I demonstrate the benefits of bargaining through case studies in the retail and financial services sectors.

This chapter is organized as follows. In Section 5.1, I present the three distinct models, along with their qualitative properties. I also outline the algorithm for the determination of solutions to the noncooperative cybersecurity investment model governed by the Nash Equilibrium, along with convergence results. In Section 5.2, I highlight the software utilized to compute solutions to the two cooperative cybersecurity investment models since these are highly nonlinear programming problems. I then provide solutions to the three distinct cybersecurity investment models for a spectrum of case studies in the retail and financial services sectors. I also provide sensitivity analysis results. Summary and conclusions are presented in Section 5.3. This section is based on the paper Nagurney and Shukla (2017).

5.1. The Multifirm Cybersecurity Investment Models

In this Section, I present three distinct multifirm cybersecurity investment models reflecting three distinct behavioral concepts. In the first model, the firms compete noncooperatively on their cybersecurity levels, each one trying to maximize its expected utility, with the governing concept being the Nash Equilibrium (NE). In the second model, the firms cooperate under the Nash bargaining (NB) concept (detailed discussion in Subsection 2.3). The objective function therein, which is maximized, is the product over all the firms of each firm's expected utility minus its expected utility evaluated at the Nash Equilibrium solution. The Nash Equilibrium solution is here the disagreement point. The constraints guarantee that the firms' respective expected utilities are never less than those under the Nash Equilibrium solution. In the third model, the solution concept is that of system-optimization (S-O), where the sum of the expected utilities of all the firms with respect to their cybersecurity investments is maximized. In each of the three models, the firms are also faced with bounds on the cybersecurity levels.

I first outline the common features of the models and in subsequent subsections I detail their specifics. The models are one period models, as in Kunreuther and Heal (2003), and, hence, the probability of an attack is defined over the period under study.

I assume that there are m firms in the "network." These firms can be financial service firms, energy firms, manufacturing firms, or even retailers. The network aspect lies in their connectivity in cyberspace through the Internet and in their frequent such interactions because of a common industry. I assume that each firm i; $i = 1, \dots, m$, in the network is interested in determining how much it should invest in cybsecurity with the cybersecurity level or, simply, security level of firm i denoted by s_i; $i = 1 \dots, m$.

The cybersecurity level s_i of each firm i must satisfy the following constraint:

$$0 \leq s_i \leq u_{s_i}, \quad i = 1, \dots, m, \tag{5.1}$$

where u_{s_i}<1, and is also greater than zero, is the upper bound on the security level for firm i. Note that a value of a cybersecurity level of 1 would imply perfect security, which is not achievable. When $s_i = 0$ the firm has no security. I group the security levels of all firms into the m-dimensional vector s.

In order to attain security level s_i, firm i encumbers an investment cost $h_i(s_i)$ with the function assumed to be continuously differentiable and convex. As noted in Shetty et al. (2009), the intuition is that user security costs increase with security, and that improving security level imposes an increasing marginal cost on the user. Distinct firms, because of their size and existing cyber infrastructure (both hardware and software), will be faced with different investment cost functions. I assume that, for a given firm i, $h_i(0) = 0$ denotes an entirely insecure firm and $h_i(1) = \infty$ is the investment cost associated with complete security for the firm, as in Shetty et al. (2009) and Shetty (2010).

An example of a suitable $h_i(s_i)$ function that I use in this chapter is

$$h_i(s_i) = \alpha_i(\frac{1}{\sqrt{(1-s_i)}} - 1) \tag{5.2}$$

with $\alpha_i > 0$. Such a function was utilized in Nagurney and Nagurney (2015), in Nagurney, Nagurney, and Shukla (2015), and in Nagurney, Daniele, and Shukla (2017). In the latter reference strict convexity of the cyberinvestment cost function (5.2) was established. According to the cybersecurity investment cost function in (5.2), and, as noted in Shetty et al. (2009), it becomes increasingly costly to improve the security level at a higher level of security.

The network security level, $\bar{s}$, is the average security, given by:

$$\bar{s} = \frac{1}{m}\sum_{j=1}^{m} s_j. \tag{5.3}$$

The vulnerability of firm i, $v_i = (1-s_i)$ and the network vulnerability, $\bar{v} = (1-\bar{s})$. Similar measures, but in a supply chain cybersecurity investment context, were used by Nagurney, Nagurney, and Shukla (2015). Therein, however, only competition and not cooperation was considered and the strategic variables included product quantities in addition to security levels.

In this chapter, I study how the network security and the network vulnerability vary under the three different behavioral concepts.

Following Shetty (2010), the probability p_i of a successful attack on firm i;

$i = 1, \dots, m$ is

$$p_i = (1 - s_i)(1 - \bar{s}), \quad i = 1, \dots, m, \tag{5.4}$$

where $(1 - \bar{s})$ is the probability of an attack on the network and $(1 - s_i)$ is the probability of success of such an attack on firm i.

Each firm i; $i = 1, \dots, m$ has a utility associated with its wealth W_i, denoted by $f_i(W_i)$, which is increasing, and is continuous and concave. The form of the $f_i(W_i)$ that I use in this chapter is $\sqrt{W_i}$ (see Shetty et al. (2009)). Such a function is increasing, continuous, and concave, reflecting that a firm's wealth has a positive but decreasing marginal benefit. Also, a firm i is faced with damage D_i if there is a successful cyberattack on it.

Hence, the expected utility $E(U_i)$ of firm i; $i = 1, \dots, m$, is given by the expression:

$$E(U_i) = (1 - p_i)f_i(W_i) + p_i(f_i(W_i - D_i)) - h_i(s_i). \tag{5.5}$$

Note that, according to (5.3), each firm i encumbers an investment cost associated with cybersecurity, which, of course, is equal to zero if the security level s_i is zero. I group the expected utilities of all firms into the m-dimensional vector $E(U)$. In view of (5.2), I may write $E(U_i) = E(U_i(s)), \forall i$.

In this framework, the firms differ in these aspects, which provides realism. For example, the firms can have different wealth, value their wealth distinctly, have different damage due to a cyberattack, given their existing cyber infrastructure, and also have distinct associated cyberinvestment cost functions. Moreover, different firms may have distinct upper bounds on their achievable security levels. Furthermore, I do not assume that an individual firm has a negligible effect on the network security level (5.3) and takes that value as given.

5.1.1. The Nash Equilibrium Model of Cybersecurity Investments

In the first model, I assume that the m firms compete noncooperatively, each one trying to maximize its expected utility. I seek to determine a security level pattern $s^* \in K^1$, where $K^1 = \prod_{i=1}^{m} K_i^1$ and $K_i^1 \equiv \{s_i | 0 \leq s_i \leq u_{s_i}\}$, such that the firms will be in a state of equilibrium with respect to their cybersecurity levels as defined below. Note that K^1 is convex since it is a Cartesian product of the firms' feasible sets with each such set being convex since it corresponds to box-type constraints.

I now present the Nash (1950a, 1951) equilibrium definition that captures the decision-makers' competitive behavior in this model.

Definition 5.1: Nash Equilibrium in Cybersecurity Levels

A security level pattern $s^* \in K^1$ is said to constitute a cybersecurity level Nash

Equilibrium if for each firm $i; i = 1, \dots, m$:

$$E(U_i(s_i^*, \hat{s}_i^*)) \geq E(U_i(s_i, \hat{s}_i^*)), \quad \forall s_i \in K_i^1, \tag{5.6}$$

where

$$\hat{s_i^*} \equiv (s_1^*, \dots, s_{i-1}^*, s_{i+1}^*, \dots, s_m^*). \tag{5.7}$$

According to (5.6), a cybersecurity Nash Equilibrium is established if no firm can unilaterally improve upon its expected profits by selecting an alternative security level.

I now present the variational inequality formulation of the Nash equilibrium in security levels.

Theorem 5.1: Variational Inequality Formulation of Nash Equilibrium in Cybersecurity Levels

If for each firm i; $i = 1, \dots, m$, the expected profit function $E(U_i(s))$ is continuously differentiable, and concave, and the feasible set K^1 is convex, I know that $s^* \in K^1$ is a Nash Equilibrium in cybersecurity levels according to Definition 5.1 if and only if it satisfies the variational inequality

$$-\sum_{i=1}^{m} \frac{\partial E(U_i(s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0, \quad \forall s \in K^1, \tag{5.8}$$

or, equivalently, $s^* \in K^1$ is a Nash equilibrium security level pattern if and only if it satisfies the variational inequality

$$\sum_{i=1}^{m} \left[\frac{\partial h_i(s_i^*)}{\partial s_i} + [f_i(W_i) - f_i(W_i - D_i)] \left[\frac{1}{m} \sum_{j=1}^{m} s_j^* - 1 - \frac{1}{m} + \frac{s_i^*}{m} \right] \right]$$

$$\times (s_i - s_i^*) \geq 0, \quad \forall s \in K^1. \tag{5.9}$$

Proof: Since the feasible set is convex for each firm, and minus the expected utility, -$E(U_i(s))$, is convex, from the classical theory of variational inequalities (see also Gabay and Moulin (1980)), it is known that each firm i; $i = 1, \ldots, m$, maximizes its expected utility if and only if

$$-\frac{\partial E(U_i(s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0, \quad \forall s_i \in K_i^1. \tag{5.10}$$

Summing the inequality (5.10) over all firms yields the variational inequality (5.8)

Variational inequality (5.9), in turn, is equivalent to variational inequality (5.8) with notice of (5.5) so that the expansion of

$$-\frac{\partial E(U_i(s^*))}{\partial s_i} = \Big[\frac{\partial h_i(s_i^*)}{\partial s_i} + f_i(W_i) \Big[\frac{1}{m} \sum_{j=1}^{m} s_j^* - 1 - \frac{1}{m} + \frac{s_i^*}{m} \Big]$$

$$+ f_i(W_i - D_i) \Big[1 - \frac{1}{m} \sum_{j=1}^{m} s_j^* + \frac{1}{m} - \frac{s_i^*}{m} \Big] \Big]$$

$$= \left[\frac{\partial h_i(s_i^*)}{\partial s_i} + [f_i(W_i) - f_i(W_i - D_i)] \left[\frac{1}{m} \sum_{j=1}^{m} s_j^* - 1 - \frac{1}{m} + \frac{s_i^*}{m} \right] \right], \qquad (5.11)$$

for each firm i. The conclusion follows. □

Variational inequality (5.9) can be put into standard variational inequality form (2.1a). I define the m-dimensional vectors $X \equiv s$ and $F(X)$ with the i-th component, F_i, of $F(X)$ given by

$$F_i(X) \equiv -\frac{\partial E(U_i(s))}{\partial s_i}$$

$$= \frac{\partial h_i(s_i)}{\partial s_i} + [f_i(W_i) - f_i(W_i - D_i)] \left[\frac{1}{m} \sum_{j=1}^{m} s_j - 1 - \frac{1}{m} + \frac{s_i}{m} \right], \qquad (5.12)$$

and with the feasible set $\mathcal{K} \equiv K^1$ and $N = m$. Clearly, (5.8) and (5.9) can be put into standard form (2.1a).

A solution to variational inequality (5.9), converted to (2.1a) using (5.12), for the Nash Equilibrium cybersecurity investment model is guaranteed to exist since the function $F(X)$ is continuous and the feasible set $\mathcal{K} = K^1$ is compact (see Kinderlehrer and Stampacchia (1980) and Nagurney (1999)). The existence and uniqueness results also follows from Subsection 2.2.

Theorem 5.2: Uniqueness of the Nash Equilibrium

If $F(X)$ is strictly monotone, that is:

$$\langle (F(X^1) - F(X^2)), X^1 - X^2 \rangle > 0, \quad \forall X^1, X^2 \in \mathcal{K}, X^1 \neq X^2, \tag{5.13}$$

then X^*, the solution to variational inequality (2.1a), is unique.

I now provide an interpretation of the strict monotonicity property directly for the Nash Equilibrium model. Specifically, I know that if the Jacobian of $F(X)$, which is denoted by J, is positive definite, then $F(X)$ is strictly monotone.

Construct:

$$\frac{\partial F_i}{\partial s_i} = \frac{3\alpha_i}{4(1-s_i)^{2.5}} + \frac{2}{m}[f_i(W_i) - f_i(W_i - D_i)], \tag{5.14a}$$

and

$$\frac{\partial F_i}{\partial s_j} = \frac{1}{m}[f_i(W_i) - f_i(W_i - D_i)], \quad \text{for } j \neq i. \tag{5.14b}$$

It then follows that

$$J = \begin{bmatrix} \frac{3\alpha_1}{4(1-s_1)^{2.5}} + \frac{2}{m}[f_1(W_1) - f_1(W_1 - D_1)] & \cdots & \frac{1}{m}[f_1(W_1) - f_1(W_1 - D_1)] \\ \vdots & & \vdots \\ \frac{1}{m}[f_m(W_m) - f_m(W_m - D_m)] & \cdots & \frac{3\alpha_m}{4(1-s_m)^{2.5}} + \frac{2}{m}[f_m(W_m) - f_m(W_m - D_m)] \end{bmatrix},$$

It is known that (see, e.g., Nagurney (1999)), if $(J + J^T)/2$, where J need not be symmetric, is strictly diagonally dominant, then it is positive definite and $F(X)$ is then strictly monotone. From the structure of $(J+J^T)/2$ it can be inferred that it is strictly diagonally dominant if, $\forall i$:

$$\frac{3\alpha_i}{4(1-s_i)^{2.5}} > \frac{m-5}{2m}[f_i(W_i)-f_i(W_i-D_i)]+\frac{1}{2m}\sum_{j=1;j\neq i}^{m}[f_j(W_j)-f_j(W_j-D_j)]. \tag{5.15}$$

One can deduce that (5.15) will be satisfied, for example, for $m=3$, if $2[f_i(W_i)-f_i(W_i-D_i)] \geq \sum_{j=1}^{m}[f_j(W_j)-f_j(W_j-D_j)], j \neq i$. Analogous conditions can be determined for $m=2$, and so on. Specifically, for $m=2$ if the following conditions are satisfied then strict diagonal dominance of $(J+J^T)/2$ also holds:

$$3(f_1(W_1)-f_1(W_1-D_1)) \geq f_2(W_2)-f_2(W_2-D_2) \geq \frac{f_1(W_1)-f_1(W_1-D_1)}{3}, \tag{5.16}$$

This result is useful since one then has a unique disagreement point.

Of course, positive-definiteness of J can still hold even when the strict diagonal dominance condition does not.

There are numerous algorithms that can be applied to compute the solution to (5.9). In this chapter, I utilize the Euler method, detailed in Subsection 2.4 for the numerical study in Section 5.2.

If, however, $F(X)$ is not strictly monotone, but only monotone, and Lipschitz continuous, the modified projection method of Korpelevich (1977) can be used. It is essential to note that, in the absence of strict monotonicity, there may be multiple Nash equilibria. If so, firms will prefer the equilibria that are Pareto optimal. For multiple such equilibria, there are Nash Equilibrium solutions. Boonen (2016) studies regulators that aim to optimize welfare of firms while enforcing an attractive Pareto optimal solution by restricting the joint feasible space. Conditions for convergence of the Euler method for a variety of network-based problems can be found in Nagurney and Zhang (1996) and Nagurney (2006).

In view of the simple structure of the underlying feasible set, the Euler method yields at each iteration closed form expressions for the security levels: i; $i = 1, \ldots, m$, given by:

$$s_i^{\tau+1} = \max\{0, \min\{u_{s_i},$$

$$s_i^{\tau} + a_\tau\Big(-\frac{\partial h_i(s_i^\tau)}{\partial s_i^\tau} - (f_i(W_i) - f_i(W_i - D_i))\left[\frac{1}{m}\sum_{j=1}^{m} s_j^\tau - 1 - \frac{1}{m} + \frac{s_i^\tau}{m}\right]\}\}. \quad (5.17)$$

5.1.2. The Nash Bargaining Model of Cybersecurity Investments

The bargaining model proposed by Nash (1950b, 1953) is based on axioms and focused on two players, that is, decision-makers. The framework easily generalizes to m decision-makers, as noted in Leshem and Zehavi (2008). Here the decision-makers are firms. An excellent overview can be found in Binmore, Rubinstein, and Wolinsky (1989) and in the book by Muthoo (1999). In the Nash bargaining model, I use expected utilities, rather than utilities, since I am dealing with uncertainties as represented by the probabilities of cyberattacks.

Let $E(U_j^{NE})$ denote the expected utility of firm j evaluated at the Nash Equilibrium security level solution, as discussed in Section 5.1.1. $E(U_j^{NE})$ is the disagreement point of firm j, according to the bargaining framework.

The objective function underlying the Nash bargaining model of cybersecurity investments is:

$$Z^1 = \prod_{j=1}^{m}(E(U_j(s)) - E(U_j^{NE})). \tag{5.18}$$

The optimization problem to be solved is then:

$$\text{Maximize} \prod_{j=1}^{m}(E(U_j(s)) - E(U_j^{NE})) \tag{5.19}$$

subject to:

$$E(U_j(s)) \geq E(U_j^{NE}), \quad j = 1, \ldots, m, \tag{5.20}$$

$$s \in K^1. \tag{5.21}$$

I define the feasible set K^2 consisting of constraints (5.20) and (5.21). Under the previous assumptions, the set is convex.

A solution to the Nash bargaining model is guaranteed to exist since the feasible set K^2 is compact and the objective function is continuous. I now provide conditions under which the solution is unique.

Theorem 5.3: Uniqueness of the Nash Bargaining Solution

The solution to the above cooperative Nash bargaining model is unique if the objective function, Z^1, is strictly quasi-concave.

Proof: This result follows from classical nonlinear programming theory. □

I now discuss conditions for which Z^1 will be strictly quasi-concave.

I can transform Z^1 as in (5.18) through the following logarithmic transformation:

$$ln(Z^1) = ln(\prod_{j=1}^{m}(E(U_j(s)) - E(U_j^{NE}))) = \sum_{j=1}^{m} ln(E(U_j(s)) - E(U_j^{NE})). \quad (5.22)$$

The objective function Z^1 is strictly quasi-concave if $ln(Z^1)$ is strictly concave.

5.1.3. The System-Optimization Model of Cybersecurity Investments

Under system-optimization, the objective function becomes:

$$Z^2 = \sum_{j=1}^{m} E(U_j(s)) \tag{5.23}$$

and the feasible set remains as for the Nash Equilibrium problem, that is, $s \in K^1$.

Hence, the system-optimization cybersecurity investment problem is to:

$$\text{Maximize} \sum_{j=1}^{m} E(U_j(s)) \tag{5.24}$$

subject to:

$$s \in K^1. \tag{5.25}$$

I know that the feasible set K^1 is convex and compact and that the objective function (5.23) is continuous. Hence, the solution to the above system-optimization problem is guaranteed to exist. In addition, I have the following uniqueness result under an assumption.

Theorem 5.4: Uniqueness of the System-Optimized Solution

The solution to the system-optimization problem above is unique if the objective *function, Z^2, is strictly concave.*

Proof: The result follows from classical nonlinear programming theory. □

I now provide conditions under which the strict concavity of Z^2 will hold.

Construct:

$$\frac{\partial Z^2}{\partial s_j} = -\frac{\alpha_j}{2(1-s_j)^{1.5}} - [f_j(W_j) - f_j(W_j - D_j)][\frac{1}{m}\sum_{l=1}^{m} s_l + \frac{s_j - 1}{m} - 1]$$

$$- \sum_{k=1;j\neq k}^{m} \frac{s_k - 1}{m}[f_k(W_k) - f_k(W_k - D_k)]. \qquad (5.26)$$

Also,

$$\frac{\partial^2 Z^2}{\partial s_j^2} = -\frac{3\alpha_j}{4(1-s_j)^{2.5}} - \frac{2}{m}[f_j(W_j) - f_j(W_j - D_j)], \qquad (5.27)$$

and

$$\frac{\partial^2 Z^2}{\partial s_k \partial s_j} = \frac{\partial^2 Z^2}{\partial s_j \partial s_k}$$

$$= -\frac{1}{m}[f_j(W_j) - f_j(W_j - D_j)] - \frac{1}{m}[f_k(W_k) - f_k(W_k - D_k)], \quad \text{for } k \neq j. \quad (5.28)$$

Z^2 is strictly concave if its Hessian matrix, H, is negative definite or $-H$

is positive definite (for all feasible s), where

$$H = \begin{bmatrix} \frac{\partial^2 Z^2}{\partial s_1^2} & \cdots & \frac{\partial^2 Z^2}{\partial s_1 \partial s_m} \\ \vdots & & \vdots \\ \frac{\partial^2 Z^2}{\partial s_m \partial s_1} & \cdots & \frac{\partial^2 Z^2}{\partial s_m^2} \end{bmatrix},$$

with the individual components for H as in (5.27) and (5.28) above. This matrix is symmetric. Moreover, I know that $-H$ is positive definite if it is strictly diagonally dominant, with the satisfaction of the condition below:

$$\frac{3\alpha_j}{4(1-s_j)^{2.5}} > \frac{m-3}{m}[f_j(W_j) - f_j(W_j - D_j)]$$

$$+\frac{1}{m}\sum_{k=1;k\neq j}^{m}[f_k(W_k) - f_k(W_k - D_k)], \quad j = 1, \ldots, m. \tag{5.29}$$

One can deduce, for example, that (5.29) will always be satisfied for $m = 2$ when $[f_i(W_i) - f_i(W_i - D_i)] = [f_j(W_j) - f_j(W_j - D_j)], \forall j \neq i$. This is useful since, if this relationship is true, strict diagonal dominance will always exist for two firms. However, if this relationship is not true and (5.29) holds, the matrix will still be positive definite. For $m = 3$, condition (5.29) is also useful.

5.2. Numerical Examples

In this Section, I present numerical examples/cases illustrating the cybersecurity investment models developed in Section 5.1. Solutions of the Nash

Equilibrium model are computed by applying the Euler method as outlined in Subsection 5.1.1, with the Euler method implemented in Matlab on a Lenovo G410 laptop with an Intel Core i5 processor and 8GB RAM. The convergence tolerance is set to 10^{-5}, so that the algorithm was deemed to have converged when the absolute value of the difference between each successively computed security level was less than or equal to 10^{-5}. The sequence $\{a_\mathcal{T}\}$ is set to: $.1\{1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, ...\}$. I initialized the Euler method by setting the security levels at their lower bounds. The upper bounds on the security levels $u_{s_i} = 0.99, \forall i$.

The solutions to the Nash Bargaining and System-Optimization models were computed by applying the Interior Point Method in the SAS NLP Solver. The algorithm was called upon while using SAS Studio, a web browser-based programming environment. The maximum optimality error, in each case example below, was 5×10^{-7} for the S-O solutions. The optimality error is defined as the maximum violation of the constraints in the models. The optimality errors in the solution of the NB model in the cases below are reported with the solutions. For both NB and S-O, the solver was initialized at the lower bounds of the security levels.

Below I present cases illustrating two different industries: retail and financial services. The industry aspect affects the firm size, wealth, and the damage parameters. Wealth, damages, and investment costs are given in US dollars in millions. The α_i values in the cybersecurity investment functions across all examples are the number of employees in millions based on the most recently available public data.

Case I: Retailers

In Case I, I consider two retailers. Firm 1 represents the second largest discount retailer in the United States, Target Corporation. The firm, in January 2014, announced that the security of 70 million of its users was breached and their information compromised. Credit card information of 40 million users was used by hackers to generate an estimated \$53.7 million in the black market as per Tobias (2014). Firm 2 represents Home Depot, a popular retailer in the home improvement and construction domain. Products available under these categories are also sold through Target which makes them compete for a common consumer base. The company was struggling with high turnover and old software which led to a compromise of 56 million users (Tobias (2014)). Firm 1 suffered \$148 million in damages, according to the Consumer Bankers Association and the Credit Union National Association (Tobias (2014)). Home Depot incurred \$62 million in legal fees and staff overtime to deal with their cyber attack in 2014. Additionally, it paid \$90 million to banks for re-issuing debit and credit cards to users who were compromised (Tobias (2014)).

I use the annual revenue data for the firms to estimate their wealth. Hence, in US\$ in millions, $W_1 = 72600$; $W_2 = 78800$. The potential damages these firms stand to sustain in the case of similar cyberattacks as above in the future amount to (in US\$ in millions): $D_1 = 148.0$; $D_2 = 152$.

As in Shetty et al. (2009), I assume that the wealth functions are of the following form:

$$f_1(W_1) = \sqrt{W_1}; \quad f_2(W_2) = \sqrt{W_2}.$$

The cybersecurity investment cost functions are:

$$h_1(s_1) = 0.25(\frac{1}{\sqrt{1-s_1}} - 1); \quad h_2(s_2) = 0.30(\frac{1}{\sqrt{1-s_2}} - 1).$$

The parameters $\alpha_1 = .25$ and $\alpha_2 = .30$ are the number of employees of the respective firms in millions, thereby, representing their size.

Results for the Nash Equilibrium model, the Nash Bargaining model, and the System-Optimization model for cybersecurity investments are summarized in Table 5.1. Recall that the values of the expected utilities are in million of dollars.

Solution	**NE**	**NB**	**S-O**
s_1^*	0.384	0.443	0.460
s_2^*	0.317	0.409	0.388
v_1	0.616	0.557	0.540
v_2	0.683	0.591	0.612
$\bar{s}^*$	0.350	0.426	0.424
$\bar{v}$	0.650	0.574	0.576
$E(U_1)$	269.265	269.271	269.268
$E(U_2)$	280.530	280.531	280.534

Table 5.1: Results for NE, NB, and S-O for Target and Home Depot

I now discuss uniqueness of the NE solution in Table 5.1. Referring to the strict diagonal dominance condition (5.15), I observe that the diagonal elements of the Jacobian J above (5.15) will assume their lowest values at $s_i = 0$; $i = 1, 2$, in this example. Hence, if the strict diagonal dominance condition holds at these values of the security levels, it will hold over all values in the feasible set. I now let $b_i = \frac{3\alpha_i}{4(1-s_i)^{2.5}}$, and $c_i = \frac{m-5}{2m}[f_i(W_i) - f_i(W_i - D_i)] + \frac{1}{2m}\sum_{j=1;j\neq i}^{m}[f_j(W_j) - f_j(W_j - D_j)]$ for $i = 1, 2$. Hence, b_1 at $s_1 = 0$, is equal to .188, and $c_1 = -.138$. Similarly, b_2 at $s_2 = 0$, is equal to .225 and $c_2 = -.134$. Clearly, $b_1 > c_1$ and $b_2 > c_2$ and, therefore, the above NE security level pattern is unique.

I also evaluated the Hessian of $ln(Z^1)$ (cf. (5.22)), which is a symmetric matrix, for the NB problem and computed the eigenvalues and the lowest eigenvalue of minus the Hessian evaluated at the computed NB solution was: 321.315 and, therefore, the NB solution is locally unique.

I now turn to examining whether the solution to the S-O problem in Table 5.1 is unique. In particular, I refer to (5.29). I retain the definition of b_i as above for $i = 1, 2$, and define now d_i: $g_i = \frac{m-3}{m}[f_i(W_i) - f_i(W_i - D_i)] + \frac{1}{m}\sum_{j=1;j\neq i}^{m}[f_j(W_j) - f_j(W_j - D_j)]$, $i = 1, 2$. I know, from the above computation, that $b_1 = .188$, and $g_1 = -.002$. Also, I know that $b_2 = .225$, from the above, with $g_2 = .002$. Clearly, $b_1 > g_1$ and $b_2 > g_2$ and, therefore, condition (5.29) is satisfied so the S-O solution for the security levels is unique for this example.

As reported in Table 5.1, the Nash Equilibrium security level for Firm 1 is

0.384 and that for Firm 2 is .317, indicating that neither firm may be well-prepared to ward off against cyber threats. The network security is .35 and the network vulnerability is .65. Firm 2 achieves a higher expected utility than Firm 1 under the Nash Equilibrium solution.

The solution to the Nash Bargaining model, in which the firms collaborate on security levels, shows an increase in the security levels for each firm. The security level of Firm 1 increases from 0.384 to 0.443 and that of Firm 2 increases from 0.317 to 0.409. These increases also result in slightly higher expected utilities for both firms as compared to the values at their NE solution; thus, creating a win-win situation for the retailers and their consumers (who benefit from higher security levels). The network vulnerability decreases from .650 to .574, a marked decline. The optimality error for the NB solution was 3.17×10^{-7}.

I observe an increase of 6000 in expected utility of Target and 1000 for Home Depot if the firms employ NB as compared to NE. Comparison of S-O and NB shows an increase of 3000 for Home Depot but a decrease of 3000 for Target. Results for the S-O model reveal that, while the security level of Firm 1 increases, that of Firm 2 decreases, as compared to the NB solution. The network vulnerability increases. Also, the expected utility for Firm 1 is lower under the S-O solution concept than under the NB one, whereas that for Firm 2 is slightly higher under the S-O solution concept.

Target Corporation is part of the Retail Cyber Intelligence Sharing Center through which the firm shares cyber threat information with other retailers that are part of the Retail Industry Leaders Association and also with public stakeholders such as the U.S. Department of Homeland Security, and the F.B.I (RILA (2014)). Even Home Depot has expressed openness towards the sharing threat information.

Note that the results for the Nash Bargaining model are close to those for the System-Optimization model. The S-O model, however, operates on the premise that the firms are controlled by a single entity, thereby, making it an unlikely scenario in practice.

In order to further examine the magnitude of the possible changes in network vulnerability and expected utilities, I now report the results for sensitivity analysis for varying damage parameters but with the wealth parameters the same as in Table 5.1, and $\alpha_1 = 100.00, \alpha_2 = 120.00$. This would represent a big increase in the number of employees of the two firms and more damaging attacks. The expected utilities for both firms are reported in Table 5.2 under the three solution concepts. In Table 5.3, I report the computed security levels and the network vulnerability values.

Condition (5.15) holds for all the NE solutions in the sensitivity analysis as does condition (5.29) for the S-O solutions, where, as for the baseline example, the evaluation is done at the security levels equal to zero, since this would be the most restrictive.

Parameters		NE		NB		S-O	
D_1	D_2	$E(U_1)$	$E(U_2)$	$E(U_1)$	$E(U_2)$	$E(U_1)$	$E(U_2)$
24800	25200	222.472	235.991	223.541	237.087	223.410	237.220
34800	35200	210.460	223.098	211.619	224.278	211.517	224.381
44800	45200	200.039	212.090	201.276	213.340	201.212	213.405

Table 5.2: Expected Utilities for NE, NB, and S-O for Target and Home Depot for Varying D_i Parameters with $\alpha_1 = 100$ and $\alpha_2 = 200$

Parameters		NE			NB			S-O		
D_1	D_2	s_1^*	s_2^*	$\bar{v}$	s_1^*	s_2^*	$\bar{v}$	s_1^*	s_2^*	$\bar{v}$
24800	25200	.169	.066	.88285	.262	.164	.78711	.265	.161	.78719
34800	35200	.289	.197	.75705	.369	.281	.67496	.371	.279	.67502
44800	45200	.374	.288	.66915	.444	.363	.59661	.445	.362	.59665

Table 5.3: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for Target and Home Depot for Varying D_i Parameters with $\alpha_1 = 100$ and $\alpha_2 = 200$

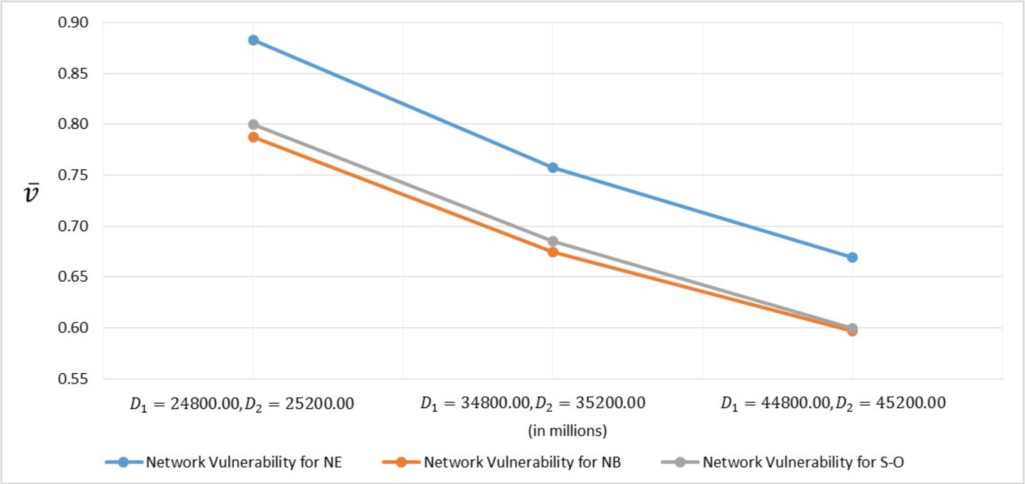

Figure 5.1: Representation of Table 5.3 Showing Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O with Varying D_i Parameters with $\alpha_1 = 100$ and $\alpha_2 = 200$

Minus the Hessian of $ln(Z^1)$, a symmetric matrix, evaluated at the NB solutions of all the sensitivity analysis examples discussed above had positive eigenvalues, implying that they were positive definite. Hence, the NB solutions in Tables 5.2 and 5.3 are locally unique.

For both Target and Home Depot, an increase of over a million is observed on employing NB as compared to NE when $D_1 = 44800, D_2 = 45200$. Also, as illustrated in Table 5.3 and Figure 5.1, the network vulnerability is at 0.60 for NB and 0.67 for NE when $D_1 = 44800, D_2 = 45200$, which indicates that it there is a significant decline in the vulnerability of the overall network if firms cooperate. The optimality error for the NB solutions was 5×10^{-7}.

As the number of employees have increased, the investment cost functions for both firms increased and, hence, the security levels dropped as compared to Table 5.1. However, the varying increase in damages, as shown in Tables 5.2 and 5.3, is leading to an increase in the security levels. The network vulnerability is consistently the lowest for the NB solution concept, demonstrating the benefit of bargaining for cooperation in cybersecurity.

For Home Depot, an increase of 1.25 million in expected utility is observed on employing NB as compared to NE and for Target, an increase of 1.24 million is observed when $D_1 = 44800, D_2 = 45200$, which is the highest of the three scenarios evaluated through the sensitivity analysis. Clearly, the reported increase is much higher than in Table 5.1 and Table 5.2. Comparison of S-O and NB shows an increase of 64,432 for Target but a decrease of 64,081 for Home Depot when $D_1 = 44800, D_2 = 45200$.

Case II: Financial Service Firms

In Case II I consider three banking and financial service firms. Firm 1 represents the largest bank in the United States, JPMorgan Chase (JPMC). Cyber intrusion faced by the bank was one of the largest ever and one of the most talked about in 2014. More than 76 million households and seven million small businesses were compromised. The bank's forensics investigations revealed that hackers had obtained a list of applications and programs run by JPMC and found alternate entry points to penetrate the systems (Silver-Greenberg, Goldstein, and Perlroth (2014)).

Firm 2 represents the third largest bank in the United States, Citibank, part of Citigroup. The bank has reported violation through cyber means in multiple instances in the past few years. However, to focus on one such event, I discuss the reported breach in 2011 in which 34,000 of the company's customers were affected. Financial losses were compensated by the company and 217,657 credit cards were replaced to ensure safety (Neowin (2011)).

Firm 3 is represented by HSBC Holdings Plc's Turkish Unit. Inclusion of the company gives an international angle to the analysis, especially since vulnerability of Turkey's HSBC can be manipulated to penetrate HSBC in the UK, United States, Canada, and so on. The unit was attacked right after JPMC in 2014 and 2.7 million customers' bank data was lost (Bloomberg (2014a)).

In US$ in millions, $W_1 = 51500$; $W_2 = 33300$; $W_3 = 31100$. Since HSBC Holdings Plc in its entirety would battle against an attack on any of its units, the wealth of HSBC Holdings is considered instead of just the Turkish unit. The potential damages these firms could stand to sustain in the future, in the case of similar cyberattacks to those described above, amount to (in US$ in millions): $D_1 = 250.00$; $D_2 = 172.80$; $D_3 = 580.50$. Damage for Firm 1 is estimated based on its spending after cybersecurity in 2014 since the firm claims to not have registered complaints of actual damage from customers. For Firm 2, it was assessed that loss per customer was \$794 US (Neowin (2011)). A survey from the Ponemon Institute (2013) states that per record cost for a cyberattack on financial firms was \$215 US in 2012. Damage for Firm 3 is estimated based on this data and the fact that 2.7 million customers were compromised.

The wealth functions are:

$$f_1(W_1) = \sqrt{W_1}; \quad f_2(W_2) = \sqrt{W_2}; \quad f_2(W_3) = \sqrt{W_3}.$$

The cybersecurity investment cost functions take the form:

$$h_1(s_1) = 0.27(\frac{1}{\sqrt{1-s_1}} - 1); \quad h_2(s_2) = 0.24(\frac{1}{\sqrt{1-s_2}} - 1);$$

$$h_1(s_3) = 0.27(\frac{1}{\sqrt{1-s_3}} - 1).$$

The α_i; $i = 1, 2, 3$ (see (2)) values in the investment cost functions represent the total number of employees of the organizations in millions. As of 2014, the number of employees in JPMC was approximately 265000, the number in Citigroup was 243000, and that in HSBC Holdings Plc: 263273. Since these illustrate the size of the organizations and the number of employees that will need to be protected (and trained) in order to ward off cyber ttacks on the organizations and, thus, consumers, they are included in the investment costs functions.

The results for the Nash Equilibrium model, the Nash Bargaining model, and the System-Optimization model for cybersecurity investments are summarized in Table 5.4.

Solution	**NE**	**NB**	**S-O**
s_1^*	0.467	0.542	0.581
s_2^*	0.454	0.535	0.598
s_3^*	0.719	0.762	0.718
v_1	0.533	0.458	0.419
v_2	0.547	0.465	0.402
v_3	0.281	0.238	0.282
$\bar{s}^*$	0.546	0.613	0.632
$\bar{v}$	0.454	0.387	0.368
$E(U_1)$	226.703	226.709	226.704
$E(U_2)$	182.281	182.286	182.274
$E(U_3)$	175.902	175.916	175.942

Table 5.4: Results of NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit

I first verify whether or not the Nash Equilibrium solution s^* in Table 5.4 is unique. I use the definitions of the b_i and c_i as given in Case I (and evaluated at security levels equal to zero) and compute them for this example with three firms for $i = 1, 2, 3$. Specifically, I have that: $b_1 = .202$, $c_1 = .171$, $b_2 = .180$, $c_2 = .209$, and $b_3 = .520$, with $c_3 = -.380$. Clearly, for this example: $b_1 > c_1$ and $b_3 > c_3$. However, $b_2 < c_2$ so I cannot guarantee that condition (5.15) is satisfied, unlike for the baseline example for Case I. Recall that the strict diagonal dominance condition guarantees that a matrix is positive definite but a matrix may be positive definite even if the strict monotonicity condition does not hold. Indeed, if all the eigenvalues of a symmetric matrix are positive, then positive definiteness of the matrix is guaranteed. I evaluate the eigenvalues for $\frac{1}{2}(J + J^T)$ and find that the smallest eigenvalue is positive and equal to .699. Hence, uniqueness of the NE cybersecurity level investment solution in Table 5.4 is guaranteed.

I also know that the NB solution in Table 5.4 is locally unique since I evaluated the Hessian of (5.22) and the smallest eigenvalue of minus that Hessian is: 501.665.

When I evaluate condition (5.29), which corresponds to the strict diagonal dominance condition holding for the corresponding Hessian matrix $-H$ I find that for this example, the condition does not hold. Nevertheless, the smallest eigenvalue of this matrix is positive and equal to .044. Consequently, I know that the S-O solution reported in Table 5.4 is unique.

In terms of the NE solution, Firm 3 has the highest security level and Firm 2 the lowest. Firm 1 enjoys the highest expected utility and Firm 3 the lowest.

Similar to the results for Case I, I observe lower security levels for the firms with more wealth. For JPMC, I observe an increase of 6000 in expected utility, 1000 for Citibank and 14,000 for HSBC when NB is employed as opposed to NE. Comparison of S-O and NB shows an increase of 26,000 for HSBC but a decrease of 5000 for JPMC and 12,000 for Citibank. The expected utility of Citibank through the S-O solution concept is 7000 below that under the NE concept.

In the results for the NB model, I observe that the security levels of all three firms are higher than their respective security levels for the Nash Equilibrium model. Consequently, the network vulnerability is decreased to 0.387 from 0.454. The optimality error for the NB solution is 9.86×10^{-6}.

Quantum Dawn 2 and 3 are cybersecurity incident response drills conducted for enhancing resolution and coordination processes in the financial services sector. These exercises are meant to avoid ripple effects of a cyberattack on one firm to others. To counteract such coordinated attacks, the financial service firms and banks realize the importance of sharing information and protect through a coordinated response (SIFMA (2015)). The results on the Nash bargaining corroborate this understanding, support negotiations, and numerically reveal the increase in security levels and the concomitant decrease in network vulnerability.

As noted earlier, since the goal of the System-Optimization model is to maximize the sum of the expected utilities and not necessarily to enhance the security level of the network, the individual security levels adjust so that the total expected utility is higher than those obtained through the other models. However, individually, Firm 1 and Firm 2 have lower expected utilities than they had through Nash Bargaining solution concept. Also, Firm 2 has an expected utility lower than that under the Nash Equilibrium.

In order to further examine the magnitude of changes in network vulnerability and expected utilities, I now report results of sensitivity analysis if the wealth parameters are the same as in Table 5.4, but with damage parameters increased to $D_1 = 25000.00, D_2 = 17200.80, D_3 = 28000.50$, and the alpha parameters varying in an elevated range. Such increases represent more damaging attacks on the firms. The expected utilities are reported in Table 5.5 and the computed security levels and network vulnerability values are reported in Table 5.6.

Parameters			**NE**			**NB**		
α_1	α_2	α_3	$E(U_1)$	$E(U_2)$	$E(U_3)$	$E(U_1)$	$E(U_2)$	$E(U_3)$
75	65	75	183.136	144.520	105.422	184.644	145.827	107.881
100	90	100	177.133	139.292	92.330	179.045	140.963	95.448
150	125	150	170.457	133.215	72.735	173.065	135.456	76.988

Parameters			**S-O**		
α_1	α_2	α_3	$E(U_1)$	$E(U_2)$	$E(U_3)$
75	65	75	184.040	144.016	111.114
100	90	100	178.276	138.697	99.500
150	125	150	172.027	132.289	82.638

Table 5.5: Expected Utilities for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit for Varying α_i Parameters with $D_1 = 25000.00, D_2 = 17200.80$ and $D_3 = 28000.50$

Parameters			NE				NB			
α_1	α_2	α_3	s_1^*	s_2^*	s_3^*	$\bar{v}$	s_1^*	s_2^*	s_3^*	$\bar{v}$
75	65	75	.258	.258	.484	.66673	.366	.366	.564	.56793
100	90	100	.169	.151	.423	.75226	.291	.275	.512	.64082
150	125	150	.018	.040	.318	.87477	.161	.180	.423	.74504

Parameters			S-O			
α_1	α_2	α_3	s_1^*	s_2^*	s_3^*	$\bar{v}$
75	65	75	.392	.423	.513	.55717
100	90	100	.319	.339	.456	.62874
150	125	150	.195	.257	.356	.73086

Table 5.6: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit for Varying α_i Parameters with $D_1 = 25000.00, D_2 = 17200.80$ and $D_3 = 28000.50$

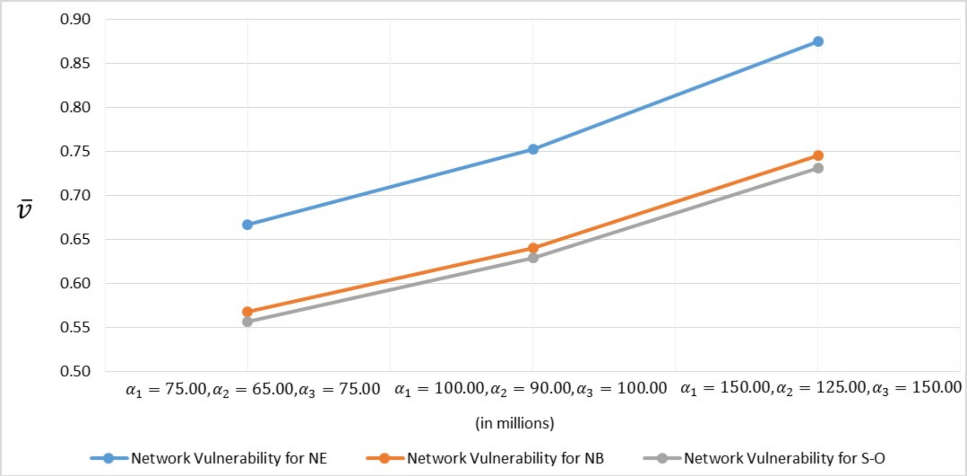

Figure 5.2: Representation of Table 5.6 Showing Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O with Varying α_i Parameters with $D_1 = 25000.00, D_2 = 17200.80$ and $D_3 = 28000.50$

As illustrated in Figure 5.2, the network vulnerability is the lowest in the case of the S-O solutions. However, for Citibank, I observe that the expected utilities for every set of alpha parameters are lower than their corresponding NE values. These results are similar to those in Table 5.4. For the third scenario, the expected utility of Citibank is 133.215 million for NE, 135.456 million for NB, and 132.289 million for S-O. A firm such as Citibank would not prefer an S-O approach if it possibly could attain a utility 927,000 below the value when it competes. But as per constraint (5.20), NB leads to better expected utilities for all three firms and a network vulnerability significantly lower than NE. The optimality error for the NB solutions was 9.40×10^{-7}.

Conditions (5.15) and (5.29) were evaluated for all the sensitivity analysis examples above at the solutions and for security levels equal to zero, which is the most restrictive. The conditions are met, and, thus, the solutions are unique.

Minus the Hessian of $ln(Z^1)$, a symmetric matrix, evaluated at the NB solutions of all the sensitivity analysis examples discussed above had positive eigenvalues, implying that they were positive definite. Hence, the NB solutions in Tables 5.5 and 5.6 are locally unique.

For JPMC, an increase of 2.61 million in expected utility is observed on employing NB as compared to NE; for Citibank, an increase of 2.24 million and for HSBC, an increase of 4.25 million is observed when $\alpha_1 = 150, \alpha_2 = 125, \alpha_3 = 150$, which constitute the highest of the three scenarios evaluated above. Comparison of S-O and NB shows an increase of 5.65 million for HSBC but a decrease of 1.04 million for JPMC and 3.17 million for Citibank when

$\alpha_1 = 150, \alpha_2 = 125, \alpha_3 = 150.$

Since the wealth and damage parameters influence the network vulnerability and expected utilities, I take into consideration another situation wherein the parameters are the same for all three firms. They are fixed as follows: $W_1 = 51500, W_2 = 51500, W_3 = 51500; D_1 = 25000, D_2 = 25000, D_3 = 25000$. The expected utilities are reported in Table 5.7 and the computed security levels and network vulnerability values are reported in Table 5.8.

Parameters			**NE**			**NB**		
α_1	α_2	α_3	$E(U_1)$	$E(U_2)$	$E(U_3)$	$E(U_1)$	$E(U_2)$	$E(U_3)$
50	50	50	189.012	189.012	189.012	190.253	190.253	190.253
50	75	50	187.406	184.183	187.406	188.741	185.647	188.741
50	100	25	188.116	184.881	196.217	189.316	186.288	197.243

Parameters			**S-O**		
α_1	α_2	α_3	$E(U_1)$	$E(U_2)$	$E(U_3)$
50	50	50	190.253	190.253	190.253
50	75	50	188.529	186.091	188.529
50	100	25	189.032	187.397	196.560

Table 5.7: Expected Utilities for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit for Varying α_i Parameters with $D_1 = 25000, D_2 = 25000$ and $D_3 = 25000$

Parameters			**NE**				**NB**			
α_1	α_2	α_3	s_1^*	s_2^*	s_3^*	$\bar{v}$	s_1^*	s_2^*	s_3^*	$\bar{v}$
50	50	50	.389	.389	.389	.61140	.480	.480	.480	.51987
50	75	50	.404	.249	.404	.64780	.494	.358	.494	.55129
50	100	25	.397	.110	.598	.63157	.488	.230	.661	.54062

Parameters			**S-O**			
α_1	α_2	α_3	s_1^*	s_2^*	s_3^*	$\bar{v}$
50	50	50	.480	.480	.480	.51987
50	75	50	.500	.345	.500	.55150
50	100	25	.494	.198	.682	.54215

Table 5.8: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit for Varying α_i Parameters with $D_1 = 25000, D_2 = 25000$ and $D_3 = 25000$

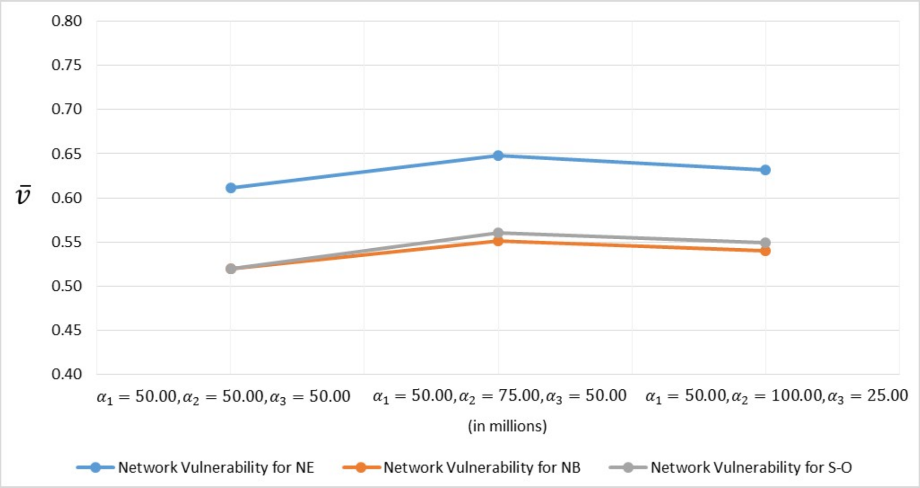

Figure 5.3: Representation of Table 5.8 Showing Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O and Varying α_i Parameters with $D_1 = 25000, D_2 = 25000$ and $D_3 = 25000$

In the first scenario, in which $\alpha_1 = \alpha_2 = \alpha_3$, the expected utilities and network vulnerability for the NB and the S-O solutions are the same. Hence, if all the firms have equal wealth, damages, and size, either NB or S-O approach can be adopted. Yet, the potential to obtain a lower network vulnerability through NB gets highlighted as the size of the firms (or the $\alpha_i; i = 1, 2, 3$) changes. The optimality error for the NB solutions was 3.53×10^{-7}. Through bargaining, the firm of larger size attains a higher security level as compared to during system-optimization.

Based on Cases I and II, which describe results for different industrial sectors along with their sensitivity analysis, it can be stated that the Nash Bargaining model is the most practical and beneficial for firms, the network, and consumers alike in terms of security levels. Moreover, the expected utilities of the firms under NB are always greater than or equal to the respective ones under the NE solution, demonstrating that the firms' individual expected profits do not suffer under cooperation as per Nash Bargaining.

5.3. Summary and Conclusions

In this chapter, I explored cybersecurity investments in the case of multiple firms in the same industrial sector and presented three new models. In the first model, the governing concept was that of Nash Equilibrium with the firms competing in terms of their cybersecurity levels. In the second model, the governing concept was that of Nash Bargaining, in which the disagreement point was the Nash Equilibrium. In this model, the constraints included not only the bounds on the security levels but also that the expected utility for each firm could not be lower than that achieved under the Nash Equilibrium solution. The objective function for the model was the product over all the firms of each firm's expected utility minus its expected utility evaluated at the Nash Equilibrium. The third model was also one of cooperation, and the concept was that of System-Optimization in which the sum of the expected utilities of all firms was maximized.

The Nash Equilibrium was formulated as a variational inequality problem and an algorithm proposed for its solution since an associated optimization reformulation does not exist. Qualitative properties of existence and uniqueness were examined and obtained for all models.

I then investigated the models through three case studies focusing on different industrial sectors in which cyberattacks have been prominent recently; in particular, the retail sector, the financial services sector, and the energy sector. I computed solutions to all three cybersecurity investment models for each case and determined the security levels of the firms, their individual vulnerability as well as the vulnerability of their networks, and their expected utilities. Since the wealth, damage, and alpha parameters significantly affect the security levels, network vulnerability, and expected utilities, I conducted sensitivity analysis for all three cases.

In Case I, I first computed the results based on estimated data for two major retailers, Target and Home Depot. The network vulnerability for NB was found to be the lowest out of the three solution concepts. To explore competition vs. cooperation, I conducted sensitivity analysis over the damage parameters with increasing alpha values associated with the cybersecurity investment cost functions. An increase as high as 1.24 million in expected utility was observed for Target and 1.25 million for Home Depot if NB was employed instead of

NE.

For Case II, I computed the results based on estimated data for three financial service firms: JPMC, Citibank, and HSBC. The network vulnerability was the lowest in the case of S-O. However, expected utility of one of the firms fell below its corresponding NE value which made system-optimization a less appropriate solution concept even with lower network vulnerability. The magnitude of changes in expected utilities was reported through sensitivity analysis on the alpha parameters. Increases as high as 2.61 million for JPMC, 2.24 million for Citibank, and 4.25 million for HSBC in expected utility were observed if NB was adopted in place of NE. I also reported analysis over alpha parameters for the three firms for equal wealth and damage parameters. The results showed that if the wealth, damage, and alpha parameters of all firms were the same, either NB or the S-O approach could be taken. The benefits of bargaining, resulting in lower network vulnerability, also was highlighted as the sizes of the firms change.

The results show that the Nash Bargaining concept yields enhanced network security in all industrial sector cases as compared to the Nash Equilibrium solution. Since firms bargain, the constraints guarantee that a not lower expected utility for each firm is ensured. This concept, with increasing emphasis on the sharing of cyber information, is the most pragmatic one since firms can be expected to negotiate among one another rather than be controlled by a central controller via system-optimization, where a firm may win and another lose as compared to the Nash Bargaining solution. Moreover, there is increasing pressure from the government and policy-makers to have firms exchange information in the cyber space as a possible defensive mechanism. The results support cooperation among firms, which may otherwise be competitors, in terms of cybersecurity investments.

CHAPTER 6

A GAME THEORY MODEL FOR FREIGHT SERVICE PROVISION SECURITY INVESTMENTS FOR HIGH-VALUE CARGO

Supply chain security is a major concern for logistics managers with control over inbound and outbound cargo shipments to and from both domestic and international markets. Meixell and Norbis (2011) propose a model that lets logistics decisions concerning security made in concert with decisions related to supply chain processes like supplier and carrier selection. They develop a mechanism for quantifying and measuring supply chain security within a multi-objective structure of carrier and supplier selection. Rinehart, Myers, and Eckert (2004) propose that shippers can minimize security-related impact by selecting security-conscious carriers, shipping via secure transportation modes. Voss et al. (2006) argue that security practices are an important criterion in carrier selection. Building on this work and that discussed in Subsection 1.1.4, I propose the following network-oriented, probabilistic approach that contributes to the current literature.

The model that is developed in this chapter fills a gap in the literature in several ways. A game theory model is developed consisting of Freight Service Providers (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. 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 are proposed. 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.

To advance physical security of cargo, infrastructure, and other assets, I have leveraged the work undertaken on cybersecurity competition, and dynamics of interaction of multiple entities and modes in physical supply chains as in Nagurney et al. (2015). The focus is on security investment decision-making for freight service providers, sensitivity and preferences of demand markets to these security characteristics and their selection. The goal is for each of these entities to maximize their expected utilities in presence of security threats.

This chapter is organized as follows. In Section 6.1, the game theory model for freight security investments for high-value cargo is constructed and qualitative results provided. In Section 6.2, an algorithm is proposed and then applied to compute solutions to numerical examples that illustrate the practicality of the framework. In Section 6.3, the results are summarized and suggestions are presented for future research. This chapter is based on Nagurney, Shukla, Nagurney, and Saberi (2017).

6.1. The Game Theory Model for Freight Service Provision Security Investments

In this section, a game theory model is developed, governing Nash Equilibrium conditions are defined, and the variational inequality formulation is presented, for which existence results are then provided, along with conditions for uniqueness of the equilibrium quantity flow and security investment pattern.

Consider m FSPs, with a typical provider denoted by i; n shipper "origin" nodes from which the high-value products are to be picked up from for delivery (and corresponding to distinct shippers), with a typical such node denoted by j, and o destination nodes for delivery of the high-value products, with a typical such node denoted by k. The network structure of the problem is depicted in Figure 6.1.

Let q_{ijk} denote the quantity of the high-value product that FSP i; $i = 1, \ldots, m$, transports from j to k, where $j = 1, \ldots, n$, and $k = 1, \ldots, o$. The vector q_i is then the no-dimensional vector consisting of all the high-value

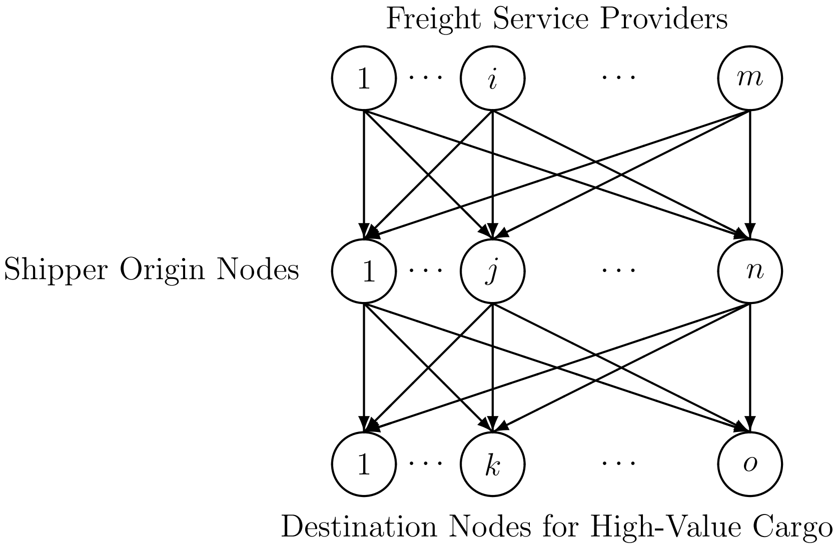
Freight Service Providers
1
i
m
Shipper Origin Nodes
1
j
n
1
k
o
Destination Nodes for High-Value Cargo

Figure 6.1: The Network Structure of the Freight Security Investment Game Theory Model

cargo shipments of FSP i. Associated with each FSP i and cargo shipment from shipper node j to destination node k are the following bounds:

$$0 \leq q_{ijk} \leq \bar{q}_{ijk}, \quad \forall j, \forall k, \tag{6.1}$$

where $\bar{q}_{ijk}$ denotes the upper bound of the high-value cargo shipment between j and k that freight service provider i can carry. We group the cargo shipments of all the freight service providers into the vector $q \in R_+^{mno}$.

Also, let s_{ijk} denote the security level that FSP i; $i = 1, \ldots, m$, invests in from j to k, with s_i denoting the no-dimensional vector consisting of all the security levels of FSP i. The security level for each FSP i must lie in the range:

$$0 \leq s_{ijk} \leq \bar{s}_{ijk}, \quad \forall j, \forall k, \tag{6.2}$$

where $\bar{s}_{ijk}$ denotes the upper bound on the security level between j and k of FSP i and this upper bound is less than 1, since here 1 represents perfect security, which, in practice, is not realizable. I further group the security levels of all the freight service providers into the vector $s \in R_{+}^{mno}$.

Associated with acquiring a security level s_{ijk} is an investment cost function h_{ijk}; $i = 1, \ldots, m$; $j = 1, \ldots, n$; $k = 1, \ldots, o$, with the function assumed to be continuously differentiable and convex. It is assumed that, for a given FSP i, $h_{ijk}(0) = 0$ denotes an entirely insecure route/mode choice between j and k and $h_{ijk}(1) = \infty$ is the investment cost associated with complete security. An example of an $h_{ijk}(s_{ijk})$ function that satisfies these properties and that is utilized in this model as

$$h_{ijk}(s_{ijk}) = \alpha_{ijk}(\frac{1}{\sqrt{(1 - s_{ijk})}} - 1) \text{ with } \alpha_{ijk} > 0, \quad \forall i, \forall j, \forall k. \tag{6.3}$$

The term α_{ijk} allows distinct freight service providers to have different investment cost functions based on their needs and expert knowledge associated with transport between different origin and destination nodes. Related security investment cost functions have been used in the context of cybersecurity, but those in (6.3) are more general since that apply at the link level through α_{ijk} and s_{ijk} (Refer to Chapters 3 and 4).

The probability of successful theft of the high-value cargo from i going from

j to k, p_{ijk}, is given by

$$p_{ijk} = (1 - s_{ijk}), \quad \forall i, \forall j, \forall k. \tag{6.4}$$

According to (6.4), if there is no investment in security by i along transport link (j, k) and, hence, $s_{ijk} = 0$, then the probability of an attack against i, transporting the high-value cargo from j to k, p_{ijk}, is precisely equal to 1.

Each FSP i; $i = 1, \ldots, m$, charges a price ρ_{ijk} to shipper j for transporting a unit of the high-value product from j to k, where it is assumed that, in general,

$$\rho_{ijk} = \rho_{ijk}(q, s), \quad \forall j, \forall k. \tag{6.5}$$

The price ρ_{ijk} reflects how much shipper j is willing to pay i for having the high-value product be transported from j to k. Note that the price depends not only on the quantities transported but also on the security levels associated with the links joining the mid-tier nodes to the bottom-tier nodes in the network in Figure 6.1. It is assumed that the prices are continuously differentiable and are decreasing in the corresponding quantity but increasing in the corresponding security level.

In addition, each FSP i; $i = 1, \ldots, m$, is faced with a total cost associated with transporting the high-value cargo items from j to k given by $\hat{c}_{ijk}$, where

$$\hat{c}_{ijk} = \hat{c}_{ijk}(q), \quad \forall j, \forall k. \tag{6.6}$$

According to (6.6), the total cost associated with transporting the high-value cargo may depend, in general, on the vector of quantities transported. These total cost functions are continuously differentiable and convex. Hence, the freight service providers are affected by the quantities transported by the other freight service providers through the total costs incurred as well as through the prices associated with transporting the high-value cargo.

The damage in case of an attack on i traveling between j and k is denoted by D_{ijk} and the value is positive for all i, j, k. In the case of a successful attack on FSP i traveling from j to k, the expected damage is given by: $p_{ijk}D_{ijk}$ so that his total expected damages correspond to:

$$\sum_{j=1}^{n}\sum_{k=1}^{o} p_{ijk}D_{ijk}. \tag{6.7}$$

Each FSP i; $i = 1, \dots, m$, seeks to maximize his expected profit, $E(U_i)$, given by:

$$E(U_i) = \sum_{j=1}^{n}\sum_{k=1}^{o}(1 - p_{ijk})(\rho_{ijk}(q, s)q_{ijk} - \hat{c}_{ijk}(q))$$

$$+\sum_{j=1}^{n}\sum_{k=1}^{o} p_{ijk}(\rho_{ijk}(q, s)q_{ijk} - \hat{c}_{ijk}(q) - D_{ijk}) - \sum_{j=1}^{n}\sum_{k=1}^{o} h_{ijk}(s_{ijk}). \tag{6.8}$$

The first term in (6.8) after the equal sign represents the expected profit of FSP i in the absence of an attack on links joining a shipper origin node and destination node. The second term in (6.8) following the equal sign represents the expected profit in the case of a successful attack on each link and the last term represents the expenditures associated with security investments of FSP i on each of the transport links (j,k) in the network in Figure 6.1. Different route/mode combinations may be more or less susceptible to attacks, and, hence, having security investments associated with links is very reasonable since destination nodes can correspond to more or less safe transit.

Hence, each FSP i; $i = 1, \ldots, m$, seeks to maximize his expected profit $E(U_i)$ given by (6.8), subject to the constraints: (6.1) and (6.2). Observe that the decisions of each freight service provider in terms of the quantities he agrees to transport and the level of security he invests in for the various links affects not only his expected utility but also those of the other freight service providers that he is in competition with.

Let K^i denote the feasible set corresponding to FSP i, where $K^i \equiv \{(q_i, s_i) | 0 \leq q_{ijk} \leq \bar{q}_{ijk}, \forall j,k \text{ and } 0 \leq s_{ijk} \leq \bar{s}_{ijk}, \forall j,k\}$. The feasible set corresponding to all the freight service providers: $K \equiv \prod_{i=1}^m K^i$.

The m FSPs compete noncooperatively in delivering the high-value cargo and invest in security, with each one trying to maximize his own expected profit. I seek to determine a nonnegative high-value cargo shipment and security level pattern (q^*, s^*) for which the m freight service providers will be in a state of equilibrium as defined below.

Definition 6.1: A Nash Equilibrium in High-Value Product Shipments and Security Levels

A high-value product shipment and security level pattern $(q^*, s^*) \in K$ *is said to constitute a Nash Equilibrium if for each freight service provider* $i; i = 1, \ldots, m$,

$$E(U_i(q_i^*, s_i^*, \hat{q_i^*}, \hat{s}_i^*)) \geq E(U_i(q_i, s_i, \hat{q_i^*}, \hat{s}_i^*)), \quad \forall (q_i, s_i) \in K^i, \tag{6.9}$$

where

$$\hat{q_i^*} \equiv (q_1^*, \ldots, q_{i-1}^*, q_{i+1}^*, \ldots, q_m^*); \quad \textit{and} \quad \hat{s_i^*} \equiv (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_m^*). \tag{6.10}$$

According to (6.9), an equilibrium is established if no freight service provider can unilaterally improve upon his expected profits by selecting an alternative vector of high-value product shipments and security levels.

I now present alternative variational inequality formulations of the above Nash Equilibrium in high value product shipments and security levels.

Theorem 6.1: Variational Inequality Formulations

Assume that, for each freight service provider i; i $= 1, \ldots, m$, *the expected profit function* $E(U_i(q, s))$ *is concave with respect to the variables* $\{q_{i11}, \ldots, q_{ino}\}$

and $\{s_{i11}, \ldots, s_{ino}\}$, *and is continuously differentiable. Then* $(q^*, s^*) \in K$ *is a Nash Equilibrium according to Definition 6.1 if and only if it satisfies the variational inequality*

$$-\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{o} \frac{\partial E(U_i(q^*, s^*))}{\partial q_{ijk}} \times (q_{ijk} - q^*_{ijk}) -$$

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{o} \frac{\partial E(U_i(q^*, s^*))}{\partial s_{ijk}} \times (s_{ijk} - s^*_{ijk}) \geq 0,$$

$$\forall (q, s) \in K, \qquad (6.11)$$

or, equivalently, $(q^*, s^*) \in K$ *is a Nash Equilibrium high-value product shipment and security level pattern if and only if it satisfies the variational inequality*

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{o} \left[\sum_{h=1}^{n}\sum_{l=1}^{o} \frac{\partial \hat{c}_{ihl}(q^*)}{\partial q_{ijk}} - \rho_{ijk}(q^*, s^*) - \sum_{h=1}^{n}\sum_{l=1}^{o} \frac{\partial \rho_{ihl}(q^*, s^*)}{\partial q_{ijk}} q^*_{ihl}\right] \times (q_{ijk} - q^*_{ijk})$$

$$+\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{o} \left[-D_{ijk} + \frac{\partial h_{ijk}(s^*_{ijk})}{\partial s_{ijk}} - \sum_{h=1}^{n}\sum_{l=1}^{o} \frac{\partial \rho_{ihl}(q^*, s^*)}{\partial s_{ijk}} q^*_{ihl}\right]$$

$$\times (s_{ijk} - s^*_{ijk}) \geq 0, \; \forall (q, s) \in K. \qquad (6.12)$$

Proof: (6.11) follows directly from Gabay and Moulin (1980) and Dafermos and Nagurney (1987).

In order to obtain variational inequality (6.12) from variational inequality

(6.11), recall (6.4) and note that, at the equilibrium, for $i = 1, \dots, m; j = 1, \dots, n; k = 1, \dots, o$:

$$-\frac{\partial E(U_i)}{\partial q_{ijk}} = \left[\sum_{h=1}^{n} \sum_{l=1}^{o} \frac{\partial \hat{c}_{ihl}(q^*)}{\partial q_{ijk}} - \rho_{ijk}(q^*, s^*) - \sum_{h=1}^{n} \sum_{l=1}^{o} \frac{\partial \rho_{ihl}(q^*, s^*)}{\partial q_{ijk}} q^*_{ihl} \right]; \tag{6.13}$$

and

$$-\frac{\partial E(U_i)}{\partial s_{ijk}} = \left[-D_{ijk} + \frac{\partial h_{ijk}(s^*_{ijk})}{\partial s_{ijk}} - \sum_{h=1}^{n} \sum_{l=1}^{o} \frac{\partial \rho_{ihl}(q^*, s^*)}{\partial s_{ijk}} q^*_{ihl} \right]. \tag{6.14}$$

Substitution of (6.13) and (6.14) into (6.11) yields (6.12)□

The above variational inequality formulation (6.12) of the Nash Equilibrium problem can be put into standard variational inequality form as depicted in (2.1a). I define the $(2mno)$-dimensional vector $X \equiv (q, s)$ and the $(2mno)$-dimensional vector $F(X) = (F^1(X), F^2(X))$ with the (i, j, k)-th component, F^1_{ijk}, of $F^1(X)$ given by

$$F^1_{ijk}(X) \equiv -\frac{\partial E(U_i(q, s))}{\partial q_{ijk}}, \tag{6.15}$$

the (i, j, k)-th component, F^2_{ijk}, of $F^2(X)$ given by

$$F^2_{ijk}(X) \equiv -\frac{\partial E(U_i(q, s))}{\partial s_{ijk}}, \tag{6.16}$$

and with the feasible set $\mathcal{K} \equiv K$ and $N = 2mno$. Then, clearly, variational inequality (6.12) can be put into standard form (2.1a).

Existence of a solution to variational inequality (6.11) and to its equivalence (6.12) is guaranteed to exist from the standard theory of variational inequalities as per Theorem 2.2 (cf. Kinderlehrer and Stampacchia (1980)) since the feasible set underlying them is compact.

Moreover, if the function that enters the variational inequality, as in its standard form (2.1a) is strictly monotone, as per Definition (2.4) and equation (2.11), then the solution X^* to (2.1a) is unique and, hence, the solution (q^*, s^*) to both (6.11) and (6.12) is also unique.

6.2. The Algorithm and Numerical Examples

For the solution of numerical examples of the model, I utilize the Euler method, which is induced by the general iterative scheme of Dupuis and Nagurney (1993). The method is described in Section 2.4 of Chapter 2.

As established in Dupuis and Nagurney (1993), for convergence of the general iterative scheme, which induces the Euler method, the sequence $\{a_\tau\}$ must satisfy: $\sum_{\tau=0}^{\infty} a_\tau = \infty$, $a_\tau > 0$, $a_\tau \to 0$, as $\tau \to \infty$. Specific conditions for convergence of this scheme as well as various applications to the solutions of other network-based game theory models can be found in Nagurney (2006) and the references therein.

Explicit Formulae for the Euler Method Applied to the Freight Service Provision Game Theory Model with Security Investments

The elegance of this procedure for the computation of solutions to this model is illustrated by the following explicit formulae. Specifically, there is the following closed form expression for the high-value cargo shipments $i = 1, \ldots, m; j = 1, \ldots, n;\ k = 1, \ldots, o$:

$$q_{ijk}^{\tau+1} = \max\{0, \min\{\bar{q}_{ijk}, Q_{ij}^{\tau} + a_\tau(\rho_{ijk}(q^\tau, s^\tau) + \sum_{h=1}^{n}\sum_{l=1}^{o}\frac{\partial \rho_{ihl}(q^\tau, s^\tau)}{\partial q_{ijk}} q_{ihl}^{\tau}$$

$$-\sum_{h=1}^{n}\sum_{l=1}^{o}\frac{\partial \hat{c}_{ihl}(q^\tau)}{\partial q_{ijk}})\}\}, \tag{6.17}$$

and the following closed form expression for the security levels $i = 1, \ldots, m; j = 1, \ldots, n;\ k = 1, \ldots, o$:

$$s_{ijk}^{\tau+1} = \max\{0, \min\{\bar{s}_{ijk}, s_{ijk}^{\tau} + a_\tau(\sum_{h=1}^{n}\sum_{l=1}^{o}\frac{\partial \rho_{ihl}(q^\tau, s^\tau)}{\partial s_{ijk}} q_{ihl}^{\tau} - \frac{\partial h_{ijk}(s_{ijk}^{\tau})}{\partial s_{ijk}} + D_{ijk})\}\}. \tag{6.18}$$

The convergence result is now provided. The proof is direct from Theorem 5.8 in Nagurney and Zhang (1996).

Theorem 6.2: Convergence

In the freight service provision game theory model developed above let $F(X) = -\nabla E(U(Q, s))$ *be strictly monotone at any equilibrium pattern. Also, assume that* F *is uniformly Lipschitz continuous. Then there exists a unique* *equilibrium high-value cargo shipment and security level pattern* $(q^*, s^*) \in K$ *and any sequence generated by the Euler method as given by (2.20), with* $\{a_\tau\}$ *satisfies* $\sum_{\tau=0}^{\infty} a_\tau = \infty$, $a_\tau > 0$, $a_\tau \to 0$, *as* $\tau \to \infty$ *converges to* (q^*, s^*).

The Euler method is now applied to compute the high-value product shipments and security level investments in a series of numerical examples. The algorithm was implemented in FORTRAN and used a LINUX system at the University of Massachusetts Amherst for the computations. The convergence criterion was that the absolute value of the difference of the cargo shipment and security level iterates at two successive iterations was less than or equal to 10^{-5}. All the variables (shipments and security levels) were initialized to 0.00. The sequence $\{a_\tau\} = \{1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \ldots\}$.

Example 6.1: One Freight Service Provider, One Shipper, and One Destination Node

The first example consists of a single FSP (FSP 1), a single shipper, and a single destination, as in the network in Figure 6.2. The high-value cargo consists of precious metals, in units of pounds.

The data are as follows. The total cost function is:

$$\hat{c}_{111} = q_{111}^2 + 5q_{111},$$

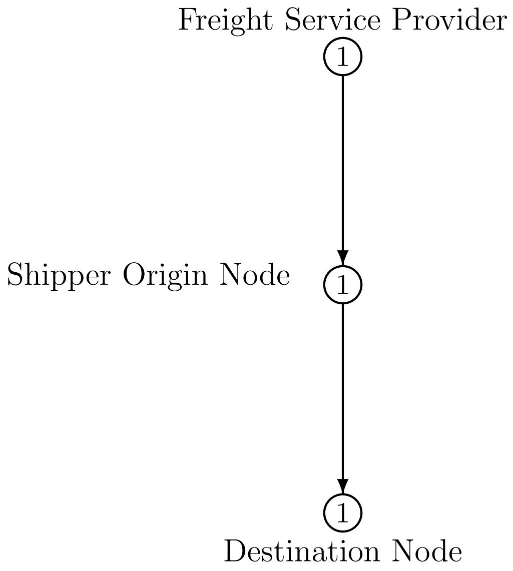

Figure 6.2: One Freight Service Provider, One Shipper, and One Destination

the demand price function is:

$$\rho_{111} = -2q_{111} + 10s_{111} + 100,$$

the upper bound on the security level is:

$$\bar{s}_{111} = .99,$$

the upper bound on the cargo shipment is:

$$\bar{q}_{111} = 100.$$

The damages, in order to reflect the high value of the cargo are:

$$\$50,000,$$

so that, at a unit price of 500 and a maximum capacity of 100 for the shipment, we obtain \$50,000.

The security investment cost function is as in (6.3), with $\alpha_{111} = 10$. This reflects that the freight service provider does not have much security to begin with and, hence, the α_{111} is rather large.

The Euler method yields the equilibrium solution: $q^*_{111} = 17.48$ and $s^*_{111} = .99$. The demand price for shipping one unit, ρ_{111}, evaluated at the equilibrium pattern, is 74.93. The expected utility of freight service provider 1, $E(U_1)$, is 327. FSP 1 invests in the maximum security level possible and still garners a positive expected utility.

Example 6.2: Two Freight Service Providers, One Shipper, and One Destination Node

Example 6.2 introduces a competitor to the market in the form of a second FSP, as depicted in Figure 6.3.

The data for FSP 1 remain as in Example 6.1 except that there is now a new demand price function due to competition.

The demand price functions for the FSPs are:

$$\rho_{111} = -2q_{111} - q_{211} + 10s_{111} + 100, \quad \rho_{211} = -3q_{211} - 2q_{111} + 10s_{211} + 110.$$

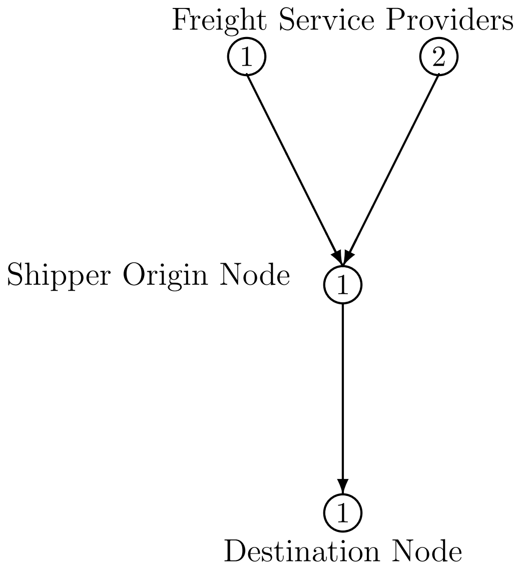

Figure 6.3: Two Freight Service Providers, One Shipper, and One Destination

Also, the total cost function for the second, new, FSP is:

$$\hat{c}_{211} = .5q_{211}^2 + 5q_{211}.$$

The security investment cost function for FSP 2 is of the form (6.3) with $\alpha_{211} = 10$ and the upper bound on the cargo shipment $\bar{q}_{211} = 120$. The damage $D_{211} = 40,000$.

The Euler method converges to the following equilibrium shipment and security level pattern:

$$q_{111}^* = 15.49, \quad q_{211}^* = 11.99, \quad s_{111}^* = .99, \quad s_{211}^* = .99.$$

The demand prices at the equilibrium solution are:

$$\rho_{111} = 66.94, \quad \rho_{211} = 52.96.$$

FSP 1 now has an expected utility, $E(U_1) = 129.36$, whereas FSP 2 has an expected utility $E(U_2) = 58.16$. With increased competition, FSP 1 now has a lower expected utility than in Example 6.1. Moreover, FSP 1 now charges a lower price for high-value cargo shipment than he did in Example 6.1, when there was no competition. The total volume of shipments from the shipper origin node to the destination node increases. This may be viewed as the shipper diversifying his risk.

Example 6.3: Two Freight Service Providers, One Shipper, and Two Destination Nodes

Example 6.3 now introduces another destination node. Hence, in Example 6.3 there are two FSPs, one shipper, and two destination nodes, as depicted in Figure 6.4.

The data remain as in Example 6.2 but with new data added as per below.

The total cost functions that are added are:

$$\hat{c}_{112} = 1.5q_{112}^2 + 5q_{112}, \quad \hat{c}_{212} = q_{212}^2 + 5q_{212}.$$

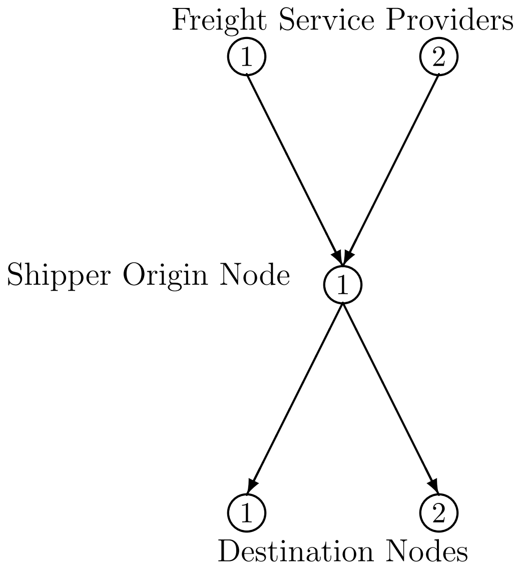

Figure 6.4: Two Freight Service Providers, One Shipper, and Two Destination Nodes

The added demand price functions are:

$$\rho_{112} = -3q_{112} - q_{212} + 5s_{112} + 270, \quad \rho_{212} = -2q_{212} - q_{112} + 5s_{212} + 200.$$

At the new destination node 2, shippers are willing to pay more per unit of freight service provision, given the distance to destination node 2 and the more challenging transport environment.

The damages associate with transport to destination node 2 are:

$$D_{112} = 5600, \quad D_{212} = 10000.$$

FSP 1 has purchased some insurance, as has FSP 2, so possible damages are lower for destination node 2 than for destination node 1.

The form of the investment cost functions is, again, as in (6.3) with

$$\alpha_{112} = 12, \quad \alpha_{212} = 10.$$

The upper bounds on the high-value cargo shipments on the new links are:

$$\bar{q}_{112} = 80, \quad \bar{q}_{212} = 100.$$

The Euler method converges to the equilibrium solution:

$$q^*_{111} = 15.49, \quad q^*_{112} = 26.64, \quad q^*_{211} = 11.99, \quad q^*_{212} = 28.89,$$

$$s^*_{111} = .99, \quad s^*_{112} = .46, \quad s^*_{211} = s^*_{212} = .99.$$

The demand prices at the computed equilibrium pattern are:

$$\rho_{111} = 66.94, \quad \rho_{112} = 163.48, \quad \rho_{211} = 52.96, \quad \rho_{212} = 120.54.$$

The expected utilities of the freight service providers are now:

$$E(U_1) = 237.83, \quad E(U_2) = 2371.25.$$

With a new destination node to ship the high-value cargo to, both FSPs garner enhanced expected utilities in comparison to their values in Example 6.2. FSP 2 especially benefits from the new destination node requiring freight service provision. The prices that are paid for the freight service provision at destination node 2 are more than double those paid for at destination node 1 to a given FSP. This is due to the fact that the fixed components (intercepts) of the demand price functions to the new destination are higher than to destination node 1, demonstrating that shippers are willing to pay a higher price for delivery to destination node 2. The quantities of the high-value cargo reaching destination node 2 are, thus, higher as well, and this is due to both the demand price functions and the total cost functions, which are lower to destination node 2 than to destination node 1.

FSP 2 provides maximum security levels for transportation for both destinations and earns a higher expected utility than does FSP 1 who has a security level about one half that at destination node 2 than at destination node 1. This is due, in part, to FSP 1's lower damages as compared to those that would be accrued for FSP 2, given an attack, at destination node 2.

Example 6.4: Two Freight Service Providers, Two Shippers, and Two Destination Nodes

Example 6.4 is constructed from Example 6.3 and has the same data except that now there is an additional shipper who wishes to explore freight service provision from the two freight service providers. The underlying network is as in Figure 6.5.

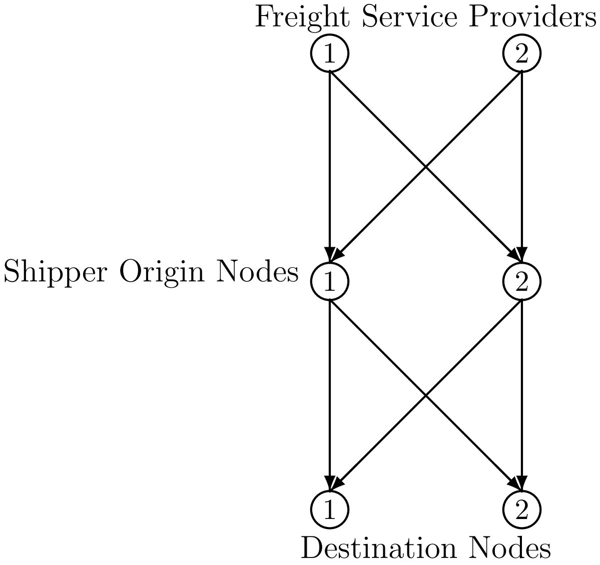

Figure 6.5: Two Freight Service Providers, Two Shippers, and Two Destination Nodes

The added data for Example 6.4 are below.

The total cost functions associated with the second shipper are:

$$\hat{c}_{121} = q_{121}^2 + q_{121}, \quad \hat{c}_{122} = .5q_{122}^2 + q_{122}, \quad \hat{c}_{221} = q_{221}^2 + 2q_{221}, \quad \hat{c}_{222} = 1.5q_{222}^2 + 3q_{222}.$$

The demand price functions associated with transacting with the second shipper are:

$$\rho_{121} = -2q_{121} - q_{221} + s_{121} + 150, \quad \rho_{122} = -3q_{122} - q_{222} + 2s_{122} + 130,$$

$$\rho_{221} = -4q_{221} - q_{121} + 5s_{221} + 120, \quad \rho_{222} = -5q_{222} - 2q_{112} + 3s_{222} + 140.$$

As in all the previous examples, the security investment functions are as in (6.3) with the following coefficients for the new possible investments:

$$\alpha_{121} = 5, \quad \alpha_{122} = 4, \quad \alpha_{221} = 3, \quad \alpha_{222} = 12.$$

The additional damage terms are:

$$D_{121} = 20000, \quad D_{122} = 15000, \quad D_{221} = 25000, \quad D_{222} = 2000.$$

The upper bounds on the cargo shipments from the second shipper to the two destinations are:

$$\bar{q}_{121} = 100, \quad q_{122} = 80, \quad q_{221} = 70, \quad q_{222} = 60.$$

The Euler method converges to the following equilibrium shipment and security level pattern:

$$q^*_{111} = 15.71, \quad q^*_{112} = 26.64, \quad q^*_{121} = 23.34, \quad q^*_{122} = 17.78,$$

$$q^*_{211} = 10.65, \quad q^*_{212} = 28.89, \quad q^*_{221} = 9.96, \quad q^*_{222} = 6.56.$$

$$s^*_{11} = .99, \quad s^*_{112} = .46, \quad s^*_{121} = .99, \quad s^*_{122} = .99,$$

$$s^*_{211} = .99, \quad s^*_{212} = .99, \quad s^*_{221} = .99, \quad s^*_{222} = .00.$$

The demand prices incurred at the equilibrium pattern are:

$$\rho^*_{111} = 67.83, \quad \rho^*_{112} = 163.48, \quad \rho^*_{121} = 94.35, \quad \rho^*_{122} = 72.10,$$

$$\rho^*_{211} = 47.61, \quad \rho^*_{212} = 120.54, \quad \rho^*_{221} = 61.77, \quad \rho^*_{222} = 53.94.$$

The expected utilities of the freight service providers are: $E(U^1) = 2567.49$ and $E(U^2) = 708.97$.

With a second shipper node added, there is the potential for increased business for the two FSPs. Although FSP 1 now enjoys an expected utility that is more than tenfold higher than that in Example 6.3, FSP 2 experiences a high security investment cost function associated with destination node 2 and his security level associated with shipping from shipper 2 to destination node 2 is .00 at the equilibrium. FSP 1 handles three times the volume of cargo from the two shippers to destination node 2. The lowest cargo shipment is q^*_{222} with security level $s^*_{222} = .00$.

6.3. Summary and Conclusions

In this chapter, a game theory model was developed in which freight service providers compete for business and also invest in security. The focus is on high-value cargo, which has been the target of attacks globally, from luxury items of clothing and jewelry to food and high tech products. Although there is a rich literature on supply chain risk and vulnerability, the focus is on freight security investment and competition and this section fills the gap in the literature in several ways, which are itemized below.

1. Security investment cost functions were quantified which may differ for distinct freight service provider/shipper/destination node combinations.

2. Shippers reveal their preferences and sensitivity to investments in security through the prices that they are will to pay for freight service provision and these also can be distinct for different freight service provider/shipper/destination node combinations.

3. The freight service providers seek to maximize their expected utilities, which capture the probability of an attack associated with different links and are a function of the security level associated with that link. Hence, risk is also captured in the competitors' objective functions.

4. The model is not limited to the number of freight service providers, shippers, and/or destination nodes.

5. The equilibrium conditions, which correspond to a Nash Equilibrium, are formulated as a variational inequality problem for which a solution is guaranteed to exist.

6. The model is computable and numerical examples reveal the equilibrium high-value cargo shipments plus security levels that the freight service

providers deliver and invest in, respectively.

There is potential to extend the research in several directions. One may include multiple links or pathways from shipper nodes to destination nodes. One could also introduce other tiers in a supply chain network context such as manufacturers and also consider whether their investments in security may be worthwhile. Finally, the issue of security and freight service provision in disaster relief is also a timely topic.

CHAPTER 7

DIRECTIONS FOR FUTURE WORK

While this dissertation has demonstrated the potential of using the techniques of competitive and cooperative game theory in the field of network security from both cyber and physical standpoints, many opportunities to extend the scope of this work remain. This chapter presents some of those directions.

7.1. Multiple Tiers in the Supply Chain Network

Nonselective and undirected internetworking is one of the most important issues facing manufacturing. The intermediary devices which are core to providing internetworking and data communication may lead to cybersecurity issues with far-reaching implications. Secure network planning and design for such network synthesis is crucial. In addition to IT integration, considerable amount of Operational Technology (OT) integration is taking place (Atos (2012)). The continuous attempt to connect networks that operate on different paradigms and levels of security-related trust is complicating network security (PricewaterhouseCoopers (2015)). Firewalls and encryption could be the way to go for IT networks but maybe not for the OT networks. A successful attack on an OT network can have major consequences that go beyond financial losses. Prolonged outages of critical services, loss of critical infrastructure, loss of intellectual property, environmental damage, and even the loss of human life. If an attacker alters a setpoint at a pasteurization unit, there are health consequences for thousands. If there is an attack on a mobile robot, there could be incorrect assemblies or may result in faulty parts causing massive recalls.

Within the cybersecurity research, as shown in Chapters 3, 4, and 5, the focus was on the interactions of retailers and consumers. In Chapter 6, freight service providers were included. I plan to add manufacturers into the supply chain network to analyze the effect of cybersecurity/security investments in technology such as unidirectional security gateways or other preventive measures. The probability of attacks will be extended to being exogenous. More specifically, the security investments do affect the probability of an attack; however, other factors such as valuation of the goods, accessibility, proximity, impact, etc. will also be considered.

Manufacturers must identify and understand the suppliers' capabilities to protect sensitive information and products, and manage cybersecurity risk. Suppliers vary in their abilities to manage cyber threats and intellectual property. Inclusion of suppliers into the network, thereby accounting for the complexity in the system pertaining to security, is also a possible area of extension. Li and Nagurney (2017) include suppliers into a competitive supply chain network and give supplier and component importance identification.

7.2. Cooperation in Freight Security Investment

Corporations across the world would agree that partnerships (or cooperation) are imperative to growth in today's scale-driven and technology intensive economies. Manufacturers are buying more components from their suppliers than they used to. Moreover, they rely on their suppliers to reduce costs, improve quality, and develop products/processes. In many industries, the power has shifted from buyers to suppliers (Paranikas et al. (2015)). As manufacturers, suppliers, and contractors are increasingly targeted by attackers, cooperation to share threat, risk, and sensitivity information could be preventive.

I demonstrated the security and financial implications of cooperation among retailers in Chapter 5. An area of exploration is cooperation between the suppliers and the manufacturers, and the effect on network vulnerability.

The technology-driven manufacturers are coming together to develop a security framework through the Industrial Internet Consortium (IIC). The framework considers that growing internetworking, automation revolution and industrial internet of things, are transforming attacks too. The objectives of IIC's security working group are to drive industry consensus, promote best practices and accelerate adoption (IIC (2017)).

The consortium is on the path of sharing information and resources to protect against attacks of all nature. From a cybersecurity standpoint, I intend to add manufacturers into the retailer-consumer dynamic as discussed in Chapter 5, and evaluate the impact of cooperation among manufacturers on the supply chain network.

7.3. Extensions of Cooperative Game Theory

An extension on Nash Bargaining theory, as provided by Nagarajan and Sosic (2008), was the inclusion of bargaining powers of each of the firms in a cooperative scenario. I would like to add that to my current work in Chapter 5 and consider its relevance in my future work on cooperative game theory. The principal idea in such models is that before embarking on the process of negotiation, the firms can take actions that partially commit them to bargaining positions that correspond with their bargaining powers. This also means that the firms would be unwilling to accept anything lower than the commitment. This would provide a new perspective to the work in Chapter 5 in which the current influence is only the point of disagreement or the Nash Equilibrium solution.

As my methodological explorations and addition of complexity to the models progress, I intend to use some of this work for various other application areas, primarily, in supply chains and logistical networks.

BIBLIOGRAPHY

Aggarwal P., Maqbool Z., Grover A., Pammi V.S., Singh S., & Dutt V. (2015). Cyber Security: A game-theoretic analysis of defender and attacker strategies in defacing-website games. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment, IEEE*, 1-8.

Akerlof, G.A. (1970). The market for lemons: Quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, 84(3), 488-500.

Albers, M. (2008). Human-information interaction. *Proceedings of the 26th Annual ACM International Conference on Design of Communication*, 117-124.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610-613.

Anshelevich, E., Dasgupta, A., Kleinberg, J., Tardos, E., Wexler, T., & Roughgarden, T. (2004). The price of stability for network design with selfish agents. *IEEE Symposium on Foundations of Computer Science*, 295-304.

AON Risk Services and Ponemon Institute. 2015 global cyber impact report. (2015). http://www.aon.com/attachments/risk-services/2015-Global-Cyber-Impact-Report-Final.pdf/ Accessed 12.04.16.

Atos. The convergence of IT and operational technology. (2012). https://atos.net/content/dam/global/ascent-whitepapers/ascent-whitepaper-the-convergence-of-it-and-operational-technology.pdf/ Accessed 04.25.17.

Automation Federation. Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC). (2013). https://logiic.automationfederation.org/public/default.aspx/ Accessed 14.09.15.

Autry, C. W., & Michelle Bobbitt, L. (2008). Supply chain security orientation: Conceptual development and a proposed framework. *The International Journal of Logistics Management*, 19(1), 42-64.

Azad, A.P., Altman, E., & El-Azouzi, R. (2009). From altruism to non-cooperation in routing games. *Proceedings of Networking and Electronic Commerce Research Conference 2009.*

Bakır, N. O. (2011). A Stackelberg game model for resource allocation in cargo container security. *Annals of Operations Research*, 187(1), 5-22.

Bakshi N, & Kleindorfer P. (2009). Co-opetition and investment for supply-chain resilience. *Production and Operations Management*, 18(6), 583-603.

Bartol, N. (2014). Using Cybersecurity Metrics in Utilities. *Natural Gas & Electricity*, 31(5), 1-7.

Bichou, K., & Talas, R. (2014). Overview of contemporary supply chain security initiatives. *Maritime Transport Security*, 24-39.

Bier, V. (2006). Game-theoretic and reliability methods in counterterrorism and security. In *Statistical Methods in Counterterrorism* (pp. 23-40). Springer: New York.

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.

Binmore K., Rubinstein A., & Wolinsky A. (1989). The Nash bargaining solution in economic modelling. *The Rand Journal of Economics* 17(2): 176-188.

Bloomberg. HSBC loses 2.7 million customers data in Turkey-attack. (2014a). http://www.bloomberg.com/news/articles/2014-11-13/hsbc-loses-2-7-million -customers-data-in-turkey-attack/ Accessed 14.09.15.

Bloomberg. UglyGorilla hack of U.S. utility exposes cyberwar threat. (2014b). http://www.bloomberg.com/news/articles/2014-06-13/uglygorilla-hack-of-u-s-utility-exposes-cyberwar-threat/ Accessed 02.09.15.

Boonen, T. J. (2016). Nash equilibria of over-the-counter bargaining for insurance risk redistributions: The role of a regulator. *European Journal of Operational Research*, 250(3), 955-965.

Boyd, S., & Vandenberghe, L. (2004). *Convex Optimization.* Cambridge, England: Cambridge University Press.

Boyson, S. (2014). Cyber supply chain risk mana gement: Revolutionizing the strategic control of critical IT systems. *Technovation* 34(7), 342-353.

Burges, B. (2013). *Cargo Theft, Loss Prevention, and Supply Chain Security.* Waltham, Massachusetts: Butterworth-Heinemann.

CargoNet. 2015 cargo theft trends analysis. (2015). http://cargonet.com/2015-cargo-theft-trends/ Accessed 09.29.16.

CargoNet. 2016 Cargo Theft Trend Analysis. (2017). https://www.ajot.com/news/cargonets-2016-cargo-theft-trend-analysis/ Accessed 03.21.17.

CBS News. Why $250 million didn't protect JP Morgan from hackers. (2014). http://www.cbsnews.com/news/why-250m-didnt-protect-jp-morgan-from-hackers/ Accessed 09.29.16.

Center for Strategic and International Studies. Net losses: Estimating the global cost of cybercrime. (2014). http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf/ Accessed 12.04.16.

Chen, H. & Roughgarden, T. (2006). Network design with weighted players. *Proceedings of the Eighteenth Annual ACM Symposium on Parallelism in Algorithms and Architectures*, 29-38.

CNN. Cyber security: It's not just about Yahoo. (2016). http://www.cnn.com /2016/09/30/yahoo-data-breach-vishwanath/index.html/ Accessed 09.30.16.

ComputerWeekly.com. Business disruption cyber attacks set to spur defence plans, says Gartner. (2015). http://www.computerweekly.com/news/22402411-29/Business-disruption-cyber-attacks-set-to-spur-defence-plans-says-Gartner/ Accessed 12.04.16.

Cournot, A. A. (1838). *Researches into the Mathematical Principles of the Theory of Wealth*, English translation. London, England: MacMillan.

Dafermos S., & Nagurney, A. (1987). Oligopolistic and competitive behavior of spatially separated markets. *Regional Science and Urban Economics*, 17, 245-254.

Dafermos, S. C., & Sparrow, F. T. (1969). The traffic assignment problem for a general network. *Journal of Research of the National Bureau of Standards*, 73B(2), 91-118.

Damco. Fradulent use of the Damco brand. (2012). http://www.damco.com/ en/aboutdamco/press/press-releases?year=2012/ Accessed 09.23.16.

Daniele, P. (2006). *Dynamic Networks and Evolutionary Variational Inequalities.* Cheltenham, England: Edward Elgar Publishing.

Daras N. J., & Rassias M. T. (2015). *Computation, Cryptography, and Network Security.* Switzerland: Springer International Publishing.

Das S. (2015). The cyber security ecosystem: Post-global financial crisis. In *Managing in Recovering Markets* (pp 453-459). New Delhi: Springer India.

Deloitte Center for Financial Services. Transforming cybersecurity: New approaches for an evolving threat landscape. (2014). http://www2.deloitte.com/ content/dam/Deloitte/global /Documents/Financial-Services/dttl-fsi-TransformingCybersecurity-2014-02.pdf/ Accessed 12.04.16.

Dodd, V. Cyber-attack warning after millions stolen from UK bank accounts. (2015).
http://www.theguardian.com/technology/2015/oct/13/nca-in-safety-warning-after-millions-stolen-from-uk-bank-accounts/ Accessed 10.09.15.

Dupuis P., & Nagurney A. (1993). Dynamical systems and variational inequalities. *Annals of Operations Research* 44: 9-42.

Elias, J., Martignon, F., Avrachenkov, K., & Neglia, G. (2010). Socially-aware network design games. *INFOCOM, 2010 Proceedings IEEE*, 1-5.

Ekwall, D. (2012). Supply chain security - threats and solutions. In *Risk Management - Current Issues and Challenges.* Banaitiene, N., Editor, (pp. 157-184). InTechOpen Publishers: Open Access.

EY. Under cyber attack: EY's global information security report. (2013). http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf/ Accessed 09.20.16.

FastCompany. For the first time, cyber attack causes widespread electricity blackout. (2016). https://www.fastcompany.com/3055108/for-first-time-cyber-attack-causes-widespread-electricity-blackout/ Accessed 09.28.16.

FBI. Statistics on 2014 cargo thefts released. (2016). https://www.fbi.gov/news/stories/statistics-on-2014-cargo-thefts-released/ Accessed 09.30.16.

FleetOwner. Cargo theft now a tougher nut to crack. (2016). http://fleetowner.com/fleet-management/cargo-theft-now-tougher-nut-crack/ Accessed 09.29.16.

Forrester. Security research statistics from 2015. (2016). https://newtecservices.com/cyber-threats-not-just-increasing-mutating-irish-smes-easy-target/ Accessed 09.30.16.

Gabay D., & Moulin H. (1980). On the uniqueness and stability of Nash equilibria in noncooperatiive games. In Bensoussan A., Kleindorfer P., & Tapiero C.S. (Eds.), *Applied Stochastic Control in Econometrics and Management Science* (pp. 271-294). North Holland: Elsevier Science Ltd.

Gal-Or, E., & Ghose, A. (2004). The economic consequences of sharing security information. *Economics of Information Security*, 95-104.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research*, 16(2), 186-208.

Gartner. Gartner reveals Top 10 Security Myths, by Ellen Messmer. (2013). http://www.networkworld.com/article/2167176/lan-wan/gartner-reveals-top-10-it-security-myths.html/ Accessed 09.28.16.

Garvey P.R., Moynihan R.A., & Servi L. (2013). A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach. *Systems Engineering* 16(3): 313-328.

Gordon L.A., Loeb M.P., Lucyshyn W., & Zhuo L. (2015). Externalities and the magnitude of cybersecurity underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security* 6: 24-30.

Gkonis, K. G., & Psaraftis, H. N. (2010). Container transportation as an interdependent security problem. *Journal of Transportation Security*, 3(4), 197-211.

Glazer, E. (2015). J.P.Morgan to accelerate timeline for cybersecurity spending boost. http://www.wsj.com/articles/j-p-morgan-to-accelerate-timeline-for-cybersecurity-spending-boost-1438641746/ Accessed 09.30.16.

Granville, K. (2015). 9 recent cyberattacks against big businesses. http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html/ Accessed 12.09.15.

Handfield, R., & McCormack, K. P. (2007). *Supply Chain Risk Management: Minimizing Disruptions in Global Sourcing*. Florida: CRC Press.

Harrington J.E., Hobbs B.F., Pang J.S., Liu A., & Roch G. (2005). Collusive game solutions via optimization. *Mathematical Programming*, 104(2-3): 407-435.

Harsanyi, J. C. (1963). A simplified bargaining model for the n-person cooperative game. *International Economic Review*, 4(2), 194-220.

Harsanyi J.C. (1977). *Rational Behavior and Bargaining Equilibrium in Games an Social Situations*. Cambridge, England: Cambridge University Press.

Hartman, P., & Stampacchia, G. (1966). On some non-linear elliptic differential-functional equations. *Acta Mathematica*, 115(1), 271-310.

Heyn, S. (2014). Cargo security: Protecting the supply chain. Inbound Logistics. http://www.inboundlogistics.com/cms/article/cargo-security-protecting-the-supply-chain/ Accessed on 04.25.17.

IIC. The industrial internet of things connectivity framework. (2017). http://www.iiconsortium.org/IICF.htm Accessed 04.26.17.

Inbound Logistics. Scrutinizing supply chain security. (2012). http://www.inboundlogistics.com/cms/article/scrutinizing-supply-chain-security/ Accessed 09.20.16.

IT Security. Sony spends $15 million on security industry views. (2015). http://www.itsecurityguru.org/2015/02/04/sony-spends-15-million-security-industry-views/ Accessed 09.29.16.

Jiang W., Zhang-Shen R., Rexford J., & Chiang M. (2009). Cooperative content distribution and traffic engineering in an ISP network. *ACM SIGMETRICS Performance Evaluation Review*, 37(1): 239-250.

Juniper Research. Cybercrime will cost businesses over $2 trillion by 2019. (2015). http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion/ Accessed 09.30.16.

Karamardian, S. (1969). Nonlinear complementary problem with applications, Parts I and II. *Journal of Optimization Theory and Applications*, 4(2), 87-98, 167-181.

Kardes, E. (2007). Discounted robust stochastic games with applications to homeland security and flow control. *PhD Dissertation*, University of Southern California, Los Angeles, California.

Kinderlehrer D., & Stampacchia G. (1980). *Variational Inequalities and their Applications*. New York: Academic Press.

Korpelevich G.M. (1977) The extragradient method for finding saddle points and other problems. *Matekon*, 13, 35-49.

Koshal, J., Nedic, A., & Shanbhag, U.V. (2011). Multiuser optimization, distributed algorithms and error analysis. *SIAM Journal on Optimization*, 21(3), 1046-1081.

Kunreuther H., & Heal G. (2003). Interdependent security. *The Journal of Risk and Uncertainty*, 26(2/3), 231-249.

Leshem A., & Zehavi E. (2008). Cooperative game theory and the Gaussian interference channel. *IEEE Journal on Selected Areas in Communications*m, 26(7), 1078-1088.

Li, D., & Nagurney, A. (2017). Supply chain performance assessment and supplier and component importance identification in a general competitive multitiered supply chain network model. *Journal of Global Optimization*, 67(1), 223-250.

Manshaei M.H., Alpcan T., Basar T., & Hubaux J.P. (2013). Game theory meets networks security and privacy. *ACM Computing Surveys*, 45(3), 25.

Markmann, C., Darkow, I. L., & von der Gracht, H. (2013). A Delphi-based risk analysis—Identifying and assessing future challenges for supply chain security in a multi-stakeholder environment. *Technological Forecasting and Social Change*, 80(9), 1815-1833.

Market Research. United States Information Technology Report Q2 2012. (2013). http://www.researchandmarkets.com/reports/3754033/united-states-information-technology-report-q2#rela2/ Accessed 06.12.15.

Maughan, D., Balenson, D., Lindqvist, U., & Tudor, Z. (2013). Crossing the "Valley of Death": Transitioning cybersecurity research into practice. *IEEE Security & Privacy*, 11(2), 14-23.

Meixell, M.J., & Norbis, M. (2011). Integrating carrier selection with supplier selectin decisions to improve supply chain security. *International Transactions in Operational Research*, 19, 5, 711-732.

McKinsey & Company Quarterly. The rising strategic risks of cyberattacks. (2014). http://www.mckinsey.com/business-functions/business-technology/our-insights/the-rising- strategic-risks-of-cyberattacks/ Accessed 12.04.16.

Muthoo A. (1999). *Bargaining Theory with Applications.* Cambridge, England: Cambridge University Press.

Nagarajan M., & Sosic G. (2008). Game-theoretic analysis of cooperation among supply chain agents: Review and extensions. *European Journal of Operational Research*, 187(3), 719-745.

Nagurney A. (1999). *Network Economics: A Variational Inequality Approach.* (2nd and revised ed.). Boston: Kluwer Academic Publishers.

Nagurney A. (2006). *Supply Chain Network Economics: Dynamics of Prices, Flows and Profits*. Cheltenham, England: Edward Elgar Publishing.

Nagurney A. (2015). A multiproduct network economic model of cybercrime in financial services. *Service Science*, 7(1), 70-81.

Nagurney A., Daniele P., & Shukla S. (2017). A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of Operations Research*, 248(1), 405-427.

Nagurney A., & Nagurney L.S. (2015). A game theory model of cybersecurity investments with information asymmetry. *Netnomics*, 16(1-2), 127-148.

Nagurney A., Nagurney L.S., & Shukla S. (2015). A supply chain game theory framework for cybersecurity investments under network vulnerability. In Daras N.J., Rassias, M.T. (Eds.), *Computation, Cryptography, and Network Security* (pp. 381-398). Switzerland: Springer International Publishing.

Nagurney, A., Saberi, S., Shukla, S., & Floden, J. (2015). Supply chain network competition in price and quality with multiple manufacturers and freight service providers. *Transportation Research Part E: Logistics and Transportation Review*, 77, 248-267.

Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investments competition vs. cooperation. *European Journal of Operational Research*, 260(2), 588-600.

Nagurney, A., Shukla, S., Nagurney, L.S., & Saberi, S. (2017). A game theory model for freight service provision security investments for high-value cargo. *University of Massachusetts Amherst.*

Nagurney A., & Zhang D. (1996). *Projected Dynamical Systems and Variational Inequalities with Applications.* Boston: Kluwer Academic Publishers.

Nagurney, A., & Zhang, D. (1997). Projected dynamical systems in the formulation, stability analysis, and computation of fixed-demand traffic network equilibria. *Transportation Science*, 31(2), 147-158.

Nash J.F. (1950a). Equilibrium points in n-person games. *Proceedings of the National Academy of Sciences, USA*, 36, 48-49.

Nash J.F. (1950b). The bargaining problem. *Econometrica*, 18, 155-162.

Nash J.F. (1951). Noncooperative games. *Annals of Mathematics*, 54, 286-298.

Nash J.F. (1953). Two person cooperative games. *Econometrica*, 21, 128-140.

Neowin. $2.7 million stolen in Citigroup hack attack. (2011). http://
www.neowin.net/news/27-million-stolen-in-citigroup-hack-attack/
Accessed 11.09.15.

NTT Group Security. 2016 NTT group global threat intelligence report. (2016). https://www.solutionary.com/threat-intelligence/threat-reports/annual-threat-report/ntt-group-global-threat-intelligence-report-2016/ Accessed 10.18.16.

OffShore Engineer. Cyber war opens new front. (2013). http://www.oedigital .com/energy/
item/1366-cyber-war-opens-new-front/ Accessed 12.09.15.

Pagliery, J. JPMorgan's accused hackers had vast $100 million operation. (2015). http://money.cnn.com/2015/11/10/technology/jpmorgan-hack-charges/ Accessed 10.18.16.

Panaousis, E., Fielder, A., Malacaria, P., Hankin, C., & Smeraldi, F. (2014). Cybersecurity games and investments: A decision support approach. *International Conference on Decision and Game Theory for Security*, 266-286.

Paranikas, P., Whiteford, G. P., Tevelson, B., & Belz, D. (2015). How to negotiate with powerful suppliers. *Harvard Business Review*, 93(7/8), 90-96.

Patrascu A., & Simion E. (2014). Applied cybersecurity using game theory elements. *Proceedings of 10th International Conference on Communications, IEEE*, 1-4.

Ponemon Institute. 2013 cost of data breach study: Global analysis. (2013). https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf/ Accessed 12.04.16.

Ponemon Institute. 2015 cost of cybercrime study: United States. (2015). http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states/ Accessed 12.04.16.

PricewaterhouseCoopers. US cybercrime: Rising, risks, reduced readiness, Key findings from the 2014 US State of Cybercrime Survey. (2014). https://collabra.email/wp-content/uploads/2015/04/2014-us-state-of-cybercrime.pdf/ Accessed 09.30.16.

PricewaterhouseCoopers. Cybersavvy: Securing operational technology assets. (2015). http://www.pwc.com.au/pdf/cyber-savvy-securing-operational-technology-assets.pdf/ Accessed 04.26.17.

Purnell, N. Cyberdefense spending rises amid high profile hacks. (2015). http://www.wsj.com/articles/cyberdefense-spending-rises-amid-high-profile-hacks-1428487519/ Accessed 09.30.16.

RAND National Security Division. Markets for cybercrime tools and stolen data. (2014).
http://www.rand.org/content/dam/rand/pubs/research_reports/
RR600/RR610/RAND_ RR610.pdf/ Accessed 12.04.16.

RILA. Retailers launch comprehensive cyber intelligence sharing center. (2014).
http://www.rila.org/news/topnews/Pages/RetailersLaunchComprehensive CyberIntelligenceSharingCenter.aspx/ Accessed 12.09.15.

Riley, C, & Pagliery, J. Target will pay hack victims $10 million. (2015).
http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/ Accessed 10.18.16.

Rinehart, L. M., Myers, M. B., & Eckert, J. A. (2004). Supplier relationships: The impact on security. *Supply Chain Management Review*, 8, 6, 52-59.

Rosen, J. B. (1965). Existence and uniqueness of equilibrium points for concave nperson games. *Econometrica*, 33(3), 520-533.

Rue, R., Pfleeger, S.L., & Ortiz, D. (2007). A framework for classifying and comparing models of cyber security investment to support policy and decision-making. *Proceedings of The Sixth Workshop on the Economics of Information Security (WEIS 2007)*, Pittsburgh, Pennsylvania.

SAS. SAS/OR software and mathematical programming tools.
https://support.sas.com/rnd/app/or/MP.html/ Accessed 09.30.16.

SIFMA. SIFMA statement on completion of the Quantum Dawn 3 cybersecurity exercise. (2015). http://www.sifma.org/newsroom/2015/sifma-statement-on-completion-of-the-quantum-dawn-3-cybersecurity-exercise/ Accessed 10.09.15.

Sodhi, M. S., Son, B. G., & Tang, C. S. (2012). Researchers' perspectives on supply chain risk management. *Production and Operations Management*, 21(1), 1-13.

Sheffi, Y. (2007). Building a resilient organization. *The Bridge: Linking Engineering and Society*, (37), 32-38.

Shetty N.G. (2010). Design of network architectures: Role of game theory and economics. *PhD dissertation*, technical report no. UCB/EECS-2010-91, Electrical Engineering and Computer Sciences, University of California at Berkeley, June 4.

Shetty N., Schwartz G., Felegyhazi M., & Walrand J. (2009). Competitive cyber-insurance and internet security. In *Economics of Information Security and Privacy* (pp. 229-247). New York: Springer US.

Silver-Greenberg, J., Goldstein, M, & Perlroth, N. JPMorgan Chase hacking affects 76 million households. (2014). http://dealbook.nytimes.com/2014/10/02/jpmorgandiscovers-further-cyber-security-issues/?-r=1/ Accessed 21.08.15.

Statista. Industrial information security budget in 2013 and 2014, by company size (in million U.S. dollars). (2015). http://www.statista.com/statistics/387861/cyber-security-budget-company-size/ Accessed 08.21.15.

Tatsumi, K. I., & Goto, M. (2010). Optimal timing of information security investment: A real options approach. In *Economics of Information Security and Privacy* (pp. 211-228). New York: Springer US.

The Cargo Security Alliance. Theft of cargo is constant worry for trucking. (2012). https://www.securecargo.org/news/press-releases/ Accessed 09.25.16.

The Verge. European Commission approves new investment in cybersecurity. (2016). http://www.theverge.com/2016/7/5/12094438/european-union-cybersecurity-public-private-partnership/ Accessed 09.29.16.

The Wall Street Journal. Retailers' dilemma: Innovation vs. cyber security risk. (2014). http://deloitte.-wsj.com/cio/2014/11/24/retails-digital-dilemma-innovation-vs-cyber-security-risk/ Accessed 12.09.15.

Thun, J. H., & Hoenig, D. (2011). An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics*, 131(1), 242-249.

Tobias, S. 2014: The year in cyberattacks. (2014). http://www.newsweek.com/2014-year-cyber-attacks-295876/ Accessed 14.09.15.

Toyasaki, F., Daniele, P., & Wakolbinger, T. (2014). A variational inequality formulation of equilibrium models for end-of-life products with nonlinear constraints. *European Journal of Operational Research*, 236, 340-350.

Terry, L. (2014). Protecting high-value cargo: A sense of security. Inbound Logistics. http://www.inboundlogistics.com/cms/article/protecting-high-value-cargo-a-sense-of-security/ Accessed 04.25.17.

US Department of Energy. Energy department invests over $34 Million to improve protection of the nation's energy infrastructure. (2015). http://www.-energy.gov/articles/energy-department-invests-over-34-million-improve - protection-nation-s-energy - infrastructure/ Accessed 14.09.15.

US Department of Homeland Security. Incident response/vulnerability coordination in 2014. (2015). National Cybersecurity and Communications Integration Center. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf/ Accessed 12.04.16.

USA Today. Regulator warns of 'Armageddon' cyber attack on banks. (2015). http://www.usatoday.com/story/money/business/2015/02/25/lawsky-goldman-sachs-banks/23995979/ Accessed 12.09.15.

Vishwanath, A. Cyber security: It's not just about Yahoo. (2016). http://www.cnn.com/2016/09/30/opinions/yahoo-data-breach-vishwanath/ index.html/ Accessed 10.18.16.

Voss, M.D., Page, T.J., Keller, S.B., & Ozmet, J. (2006). Determining important carrier attributes: A fresh perspective using the theory of reasoned action. *Transportation Journal*, 45, 3, 7-19.

Voss, M. D., & Williams, Z. (2013). Public–Private partnerships and supply chain security: C-TPAT as an indicator of relational security. *Journal of Business Logistics*, 34(4), 320-334.

Wagner S., Berg E.V.D., Giacopelli J., Ghetie A., Burns J., Tauil M., Lan T., Sen S., Wang M., Chiang M., Laddaga R., Robertson P., & Manghwani P. (2012). Autonomous, collaborative control for resilient cyber defense (ACCORD). *Sixth International Conference on Self-Adaptive and Self-Organizing Systems Workshops, IEEE*, 39-46.

Wagner, S.M., Bode, C. (2009). *Managing Risk and Security: The Safeguard of Long-Term Success for Logistics Service Providers.* Berne, Germany: Haupt Publishers.

Waters, D. (2011). *Supply Chain Risk Management: Vulnerability and Resilience in Logistics.* London, England: Kogan Page Publishers.

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

Wright, S. (1997). *Primal-Dual Interior-Point Methods.* Philadelphia: SIAM.

Yakowicz, W. Be prepared to up your cybersecurity budget. (2014). http://www.inc.com/will-yakowicz/60-percent-of-large-companies-across-us-up-cyber-security.html/ Accessed 09.30.16.

Zailani, S. H., Seva Subaramaniam, K., Iranmanesh, M., & Shaharudin, M. R. (2015). The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy: Security culture as moderator. *International Journal of Physical Distribution & Logistics Management*, 45(7), 652-673.

Zhang, D., & Nagurney, A. (1995). On the stability of projected dynamical systems. *Journal of Optimization Theory and its Applications*, 85, 97-124.