A Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints

Anna Nagurney[1], Patrizia Daniele[2], Shivani Shukla[1]

[1]Isenberg School of Management
University of Massachusetts Amherst
Amherst, Massachusetts 01003

[2]Department of Mathematics and Computer Science
University of Catania
6-95125 Catania

28th European Conference on Operational Research, Poznan, July 3-6, 2016

Session: Recent Advances in Dynamics of Variational Inequalities and Equilibrium Problems

Outline

1. Introduction
2. Motivation
3. Approach
4. The Model
5. Variational Inequalities
6. Computational Procedure
7. Numerical Results
8. Summary and Conclusions

Acknowledgements

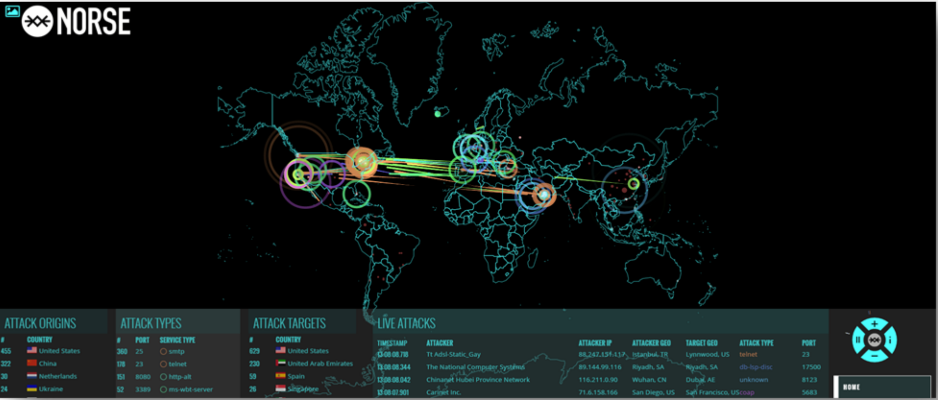
- The first author acknowledges support from All Souls College at Oxford University in England through its Visiting Fellows program.
- This research of the first author was supported by the National Science Foundation (NSF) grant CISE #1111276, for the NeTS: Large: Collaborative Research: Network Innovation Through Choice project awarded to the University of Massachusetts Amherst as well as by the Advanced Cyber Security Center through the grant: Cybersecurity Risk Analysis for Enterprise Security. This support is gratefully acknowledged.

This presentation is based on the paper, Nagurney A., Daniele P., & Shukla S. (2016). A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of Operations Research*. doi:10.1007/s10479-016-2209-1, where many references and additional theoretical and numerical results can be found.

Introduction

- An increasingly connected world may amplify the effects of a disruption.
- **Cyber threat management** is more than a strategic imperative, it is **fundamental to business**.
- Breaches are inevitable:
  - (i) **Tangible costs** - lost funds, regulatory and legal fines, compensation, recovery - information and infrastructure rehabilitation.
  - (ii) **Intangible costs** - loss of reputation, business, competitive advantage, intellectual property, personal information.

Cyber Attack Map

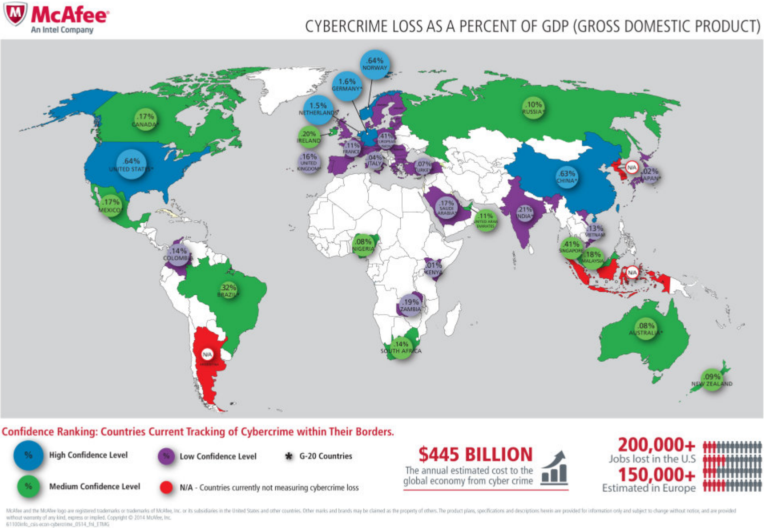


Snapshot of a real time view of cyberattacks - June 16, 2016

Cost of Cybercrime

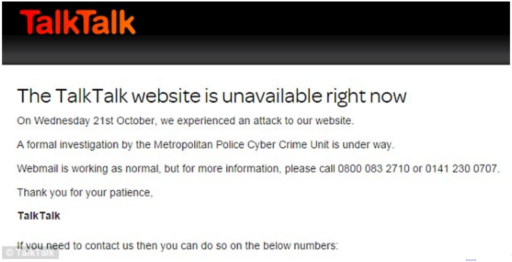
- Cybercrime climbs to 2nd most reported economic crime affecting **32% of organisations** globally (PwC Survey, 2016).
- Cost of data breaches to increase to **$2.1 trillion** globally by 2019 - four times the estimated cost of breaches in 2015 (Forbes, 2016).
- "Cyber threats are not just increasing, but **mutating**" (Forrester Research, 2016).

Cyber Loss as a Percent of GDP (2014)



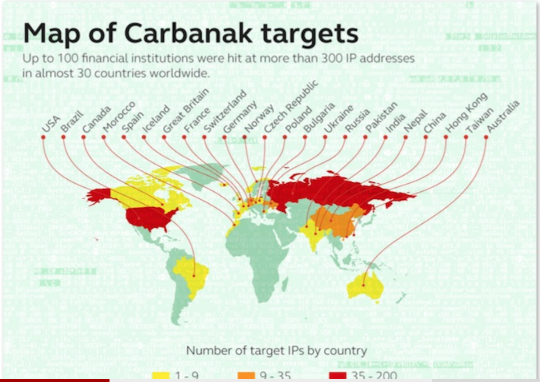
Major Cyberattacks

- **Hilton Worldwide**(2015) - POS terminals hacked, credit card holders' names, numbers, expiry date, and security codes stolen. Hackers shopped online (SecurityWeek, 2016).
- **TalkTalk** (2015) - Nearly 157,000 had data breached. Cost of crime was £60 m, customers chose to leave, bonuses slashed (The Guardian, 2016).
- **Sony Pictures** (2014) - 100 terabytes of sensitive data leaked, 5 Sony films put online for free, private emails, salary information of top executives, medical documents, and Sony's Twitter account also leaked. Cost of crime could be $100 m (Reuters, 2014).



Major Cyberattacks

- **JD Wetherspoon**(2015) - Names, email ids, birthdates and contact numbers of 656,723 customers hacked. Company became aware of the attack almost 5 months later (Telegraph, 2015).
- Kaspersky Lab reported a cyber heist **(Carbanak)** of $1 bn when hackers infiltrated 100 banks across 30 countries over a period of 2 years.
- Other notable attacks - Target, Home Depot, Michaels Stores, Staples, eBay.



Motivation

The **median number of days that attackers stay dormant** within a network before detection is **over 200** (Microsoft, 2015)

The majority of data breach victims surveyed, 81 percent, report they had **neither a system nor a managed security service** in place to ensure they could self-detect data breaches, **relying instead on notification from an external party**.

This was the case despite the fact that self-detected breaches take just 14.5 days to contain from their intrusion date, whereas **breaches detected by an external party take an average of 154 days to contain** (Trustwave, 2015).

Motivation

- Growing interest in the development of **rigorous scientific tools**.
- As reported in Glazer (2015), JPMorgan was expected to double its cybersecurity spending in 2015 to $500 million from $250 million in 2014.
- According to Purnell (2015), the research firm Gartner reported in January 2015 that the global information security spending would increase by 7.6% in 2015 to $790 billion.
- It is clear that making the best **cybersecurity investments is a very timely problem and issue**.

Approach

- We develop a supply chain network game theory model with **competing retailers**.

Approach

- We develop a supply chain network game theory model with **competing retailers**.
- Retailers seek to individually maximize their expected revenue and minimize financial losses in case of cyber attack, along with costs associated with **cyber investments**.

Approach

- We develop a supply chain network game theory model with **competing retailers**.
- Retailers seek to individually maximize their expected revenue and minimize financial losses in case of cyber attack, along with costs associated with **cyber investments**.
- **Nonlinear budget constraints** are considered, Nash equilibrium conditions discussed, and variational inequality formulations presented.

Approach

- We develop a supply chain network game theory model with **competing retailers**.
- Retailers seek to individually maximize their expected revenue and minimize financial losses in case of cyber attack, along with costs associated with **cyber investments**.
- **Nonlinear budget constraints** are considered, Nash equilibrium conditions discussed, and variational inequality formulations presented.
- We also discuss how to measure the **vulnerability of a firm to cyberattacks and that of the supply chain network**, as a whole.

Important References:

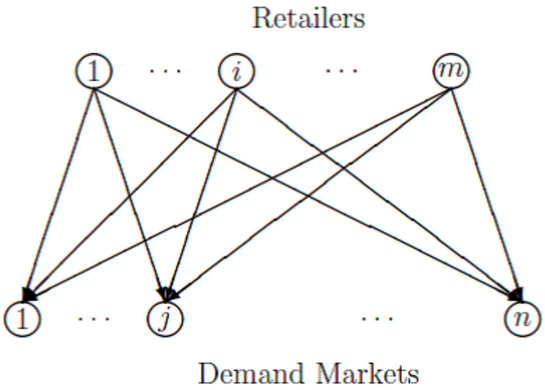
Nagurney, A. (2015). A multiproduct network economic model of cybercrime in financial services. *Service Science*, 7(1), 70-81.

Nagurney, A., Nagurney, L.S., Shukla, S. (2015). A supply chain game theory framework for cybersecurity investments under network vulnerability. In *Computation, Cryptography, and Network Security*, Daras, Nicholas J., Rassias, Michael Th. (Eds.), Springer, 381-398.

Nagurney, A., Nagurney, L. S. (2015). A game theory model of cybersecurity investments with information asymmetry. NETNOMICS: Economic Research and Electronic Networking, 16(1-2), 127-148.

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

Network Topology: Bipartite Structure



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

Network Security, s_i:

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

$u_{s_i} < 1$: Upper bound on security level of firm i.

Average Network Security of the Chain, $\bar{s}$:

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

Probability of a Successful Cyberattack on i, p_i:

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

Vulnerability, v_i:

$v_i = (1 - s_i), \quad i = 1, ..., m.$ Vulnerability of network, $\bar{v} = (1 - \bar{s})$.

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

Investment Cost Function to Acquire Security s_i, $h_i(s_i)$:

$$h_i(s_i) = \alpha_i(\frac{1}{\sqrt{(1-s_i)}} - 1), \quad \alpha_i > 0, \qquad i = 1, \dots, m.$$

α_i quantifies size and needs of retailer i; $h_i(0) = 0 =$ insecure retailer, and $h_i(1) = \infty =$ complete security at infinite cost.

Nonlinear Budget Constraint:

$$\alpha_i(\frac{1}{\sqrt{(1-s_i)}} - 1) \leq B_i, \qquad i = 1, \dots, m.$$

Each retailer cannot exceed his allocated cybersecurity budget, B_i.

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

Incurred financial damage if attack successful: D_i.
Expected Financial Damage after Cyberattack for Firm $i; i = 1, ..., m$**:**

$$D_i p_i, \quad D_i \geq 0.$$

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

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

where

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

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

In view of the demand, we can define **demand price functions**

$$\hat{\rho}_j(Q, s) \equiv \rho_j(d, \bar{s}), \forall j$$

. The consumers reflect their preferences through vector of demands and supply chain network security.

Profit of Retailer $i, i = 1, ..., m$ **in absence of cyberattack and investments,** f_i**:**

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

Q_{ij} : Quantity from i to j; c_i : Cost of processing at i; c_{ij} : Cost of transactions from i to j.

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

Expected Utility $i, i = 1, ..., m$**:**

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

Each $E(U_i(s))$ is strictly concave with respect to s_i and each $h_i(s_i)$ is strictly convex.

Feasible Set: $K \equiv \prod_{i=1}^{m} K^i$, where
$K^i \equiv \{(Q_i, s_i) | 0 \leq Q_i \leq \bar{Q}_{ij}; 0 \leq s_i \leq u_{s_i}$, and budget constraint$\}$

Definition 1: A Supply Chain Nash Equilibrium in Product Transactions and Security Levels

We 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.

Definition 1: Nash Equilibrium in Cybersecurity Levels

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

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

where

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

Nonlinear Budget Constraints in the Feasible Set

In our model, unlike in many network equilibrium problems from congested urban transportation networks to supply chains and financial networks, the feasible set contains nonlinear constraints.

Lemma 1

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

Variational Inequality Formulation

Theorem 1: Variational Inequality Formulation

$(Q^*, s^*) \in K$ is a Nash equilibrium if and only if it satisfies the variational inequality,

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

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

or, equivalently,

Variational Inequality Formulation

$(Q^*, s^*) \in K$ *is a Nash equilibrium if and only if it satisfies the variational inequality,*

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

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

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

Existence

Theorem 2: Existence

A solution (Q^*, s^*) to the variational inequality is guaranteed to exist.
The result follows from the classical theory of variational inequaliities (see Kinderlehrer and Stampacchia (1980)) since the feasible set K is compact, and the function that enters the variational inequality is continuous.

Uniqueness

We define the $(mn+m)$-dimensional column vector $X \equiv (Q, s)$ and the $(mn+m)$-dimensional column vector $F(X) = (F^1(X), F^2(X))$ with the (i,j)-th component, F^1_{ij} of $F^1(X)$ is $\frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}}$, and i-th component F^2_i of $F^2(X)$ is $\frac{\partial E(U_i(Q^*, s^*))}{\partial s_i}$.

Theorem 3: Uniqueness

A solution (Q^*, s^*) to the variational inequality is unique if $F(X)$ and $X \equiv (Q, s)$ is strictly monotone (see Kinderlehrer and Stampacchia (1980)).

Variational Inequality Formulation with Lagrange Multipliers

Feasible set: $\mathcal{K} \equiv \prod_{i=1}^{m} \mathcal{K}_i^1 \times R_+^m$,
where $\mathcal{K}_i^1 \equiv \{(Q_i, s_i) | 0 \leq Q_i \leq \bar{Q}_{ij}, \forall j; 0 \leq s_i \leq u_{s_i}\}$.

Theorem 4: Alternative Variational Inequality Formulation

A vector (Q^*, s^*, λ^*) in feasible set, $\mathcal{K}$, containing non-negativity constraints is an equilibrium solution if and only if it satisfies the following variational inequality,

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

$$-\sum_{i=1}^{m} \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \times (s_i - s_i^*)$$

$$+\sum_{i=1}^{m} [B_i - \alpha_i(\frac{1}{\sqrt{1 - s_i}} - 1)] \times (\lambda_i - \lambda_i^*) \geq 0, \forall (Q, s, \lambda) \in \mathcal{K},$$

or, equivalently,

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

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

$$-(1 - \sum_{k=1}^{m}\frac{s_k^*}{m} + \frac{1 - s_i^*}{m})D_i) + \frac{\lambda_i^*}{2}\alpha_i(1 - s_i^*)^{-\frac{3}{2}}] \times (s_i - s_i^*)$$

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

Assumption

The Slater Condition:

There exists a Slater vector $\tilde{X}_i \in K_1^i$ for each $i = 1, ..., m$, such that $g_i(\tilde{X}_i) < 0$.
It is a sufficient condition for strong duality to hold for a convex optimization problem. Informally, Slater's condition states that the feasible region must have an interior point.

The Algorithm

The Euler Method: At each iteration τ, one solves the following problem:

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

where $P_{\mathcal{K}}$ is the projection operator and F is the function that enters the Variational Inequality, $\langle F(X^*), X - X^* \rangle \geq 0$, where $X \equiv (Q, s, \lambda)$.

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 $\tau \to \infty$.

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

Closed form expression for the product transactions, $i = 1, \ldots, m; j = 1, \ldots, n$:

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

Closed form expression for security levels and Lagrange multipliers for $i = 1, \ldots, m$:

$$s_i^{\tau+1} = max\{0, min\{u_{s_i}, s_i^{\tau} + a_\tau(\sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^\tau, s^\tau)}{\partial s_i} Q_{ik}^{\tau} - \frac{\partial h_i(s_i^\tau)}{\partial s_i^\tau}$$

$$+(1 - \sum_{j=1}^{m} \frac{s_j^\tau}{m} + \frac{1 - s_i}{m})D_i) - \frac{\lambda_i^\tau}{2}\alpha_i(1 - s_i^\tau)^{\frac{-3}{2}}\}\},$$

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

Numerical Examples

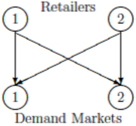
Convergence Criterion: $\epsilon = 10^{-4}$.

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.

Sequence a_τ: $.1(1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \ldots)$.

Initial Values: We initialized the Euler method 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 retailers budget constraint $\lambda_i = 0.00, \forall i$. The capacities $\bar{Q}_{ij}$ were set to 100 for all i, j.

Example 1



Cost functions:

$$c_1 = 5, \quad c_2 = 10,$$
$$c_{11}(Q_{11}) = .5Q_{11}^2 + Q_{11}, \quad c_{12}(Q_{12}) = .25Q_{12}^2 + Q_{12},$$
$$c_{21}(Q_{21}) = .5Q_{21}^2 + 2, \quad c_{22}(Q_{22}) = .25Q_{22}^2 + Q_{22}$$

.

Demand price functions:

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

Damage parameters: $D_1 = 50, D_2 = 70$. Budgets: $B_1 = B_2 = 2.5$.
Investment cost functions:

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

.

Example 1

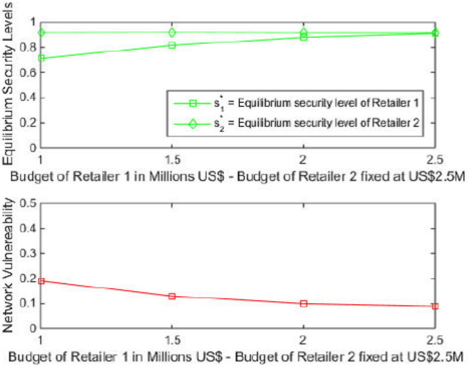
Results:

Solution	Ex.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
$\rho_2(d_2^*, \bar{s}^*)$	104.34
$E(U_1)$	8137.38
$E(U_2)$	7213.49

Example 1: Sensitivity Analysis

Base results showed that Retailer 1 has .21 (in millions) in unspent cybersecurity funds whereas Retailer 2 has .10(in millions). Hence, the associated Lagrange multipliers are 0.

For sensitivity analysis, we kept the budget of Retailer 2 fixed at 2.5 (in millions of US dollars), and we varied the budget of Retailer 1 in increments of .5.



Example 2

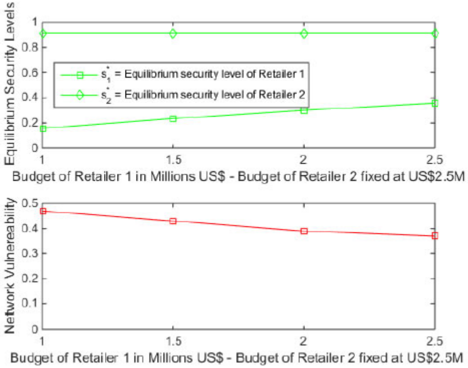
Example 2 was constructed from Example 1, except that the investment cost function of Retailer 1 was changed to: $h_1(s_1) = 10\frac{1}{\sqrt{(1-s_1)}} - 1$.

Solution	Ex.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
$\rho_1(d_1^*, \bar{s}^*)$	54.53
$\rho_2(d_2^*, \bar{s}^*)$	104.32
$E(U_1)$	8122.77
$E(U_2)$	7207.47

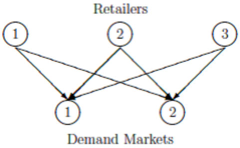
Example 2: Sensitivity Analysis

Base results showed that budgets were fully spent, so the Lagrange multipliers are no more 0. Retailer 1 invests less in security. Network vulnerability increased to .37.

For sensitivity analysis, Budget of Retailer 2 fixed at 2.5 and the budget of Retailer 1 varied in increments of .5.



Example 3



Example 3 was constructed from Example 1 with the following for Retailer 3. Cost functions:

$$c_3 = 3$$

,

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

.

Damage parameters: $D_3 = 80$. Budgets: $B_3 = 3.0$.
Investment cost functions:

$$h_3(s_3) = 3(\frac{1}{\sqrt{(1-s_3)}} - 1)$$

.

Example 3

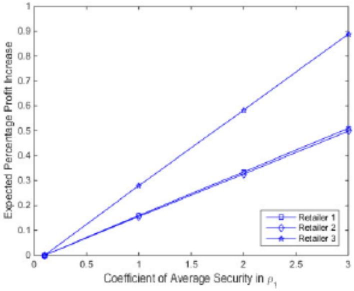
Results:

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

Example 3: Sensitivity Analysis

Base results showed that addition of Retailer 3 caused profits for all to drop, demands increase, and network vulnerability increase. Budgets were not exhausted. Retailer 3 turned out to be a "free rider".

For sensitivity analysis, demand price function coefficient for demand market 1 increased to 1.0, 2.0, and 3.0, and the percent increase in expected profits of the retailers reported.



Example 4

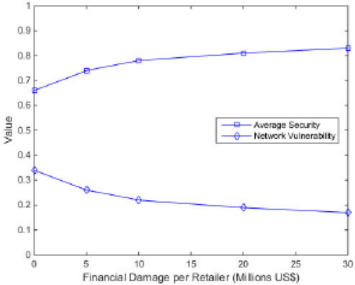
Example 4 constructed from Example 3. All damages at 0.00.

Q_{11}^*	20.80
Q_{12}^*	89.48
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

Example 4: Sensitivity Analysis

Base results showed that budgets were not fully spent due to:(i) information asymmetry, (ii) no damages.

For sensitivity analysis, damages for all are increased to 5.00, 10.00, followed by increments of 10.00 through 30.00



Summary and Conclusions

- Retailers, being in the forefront, have become highly susceptible to breaches and ensuing losses.

Summary and Conclusions

- Retailers, being in the forefront, have become highly susceptible to breaches and ensuing losses.
- Our paper provides a basis for quantifying security investments in the backdrop of **competing retailers** trying to **maximize their expected profits** subject to **strict budget constraints**.

Summary and Conclusions

- Retailers, being in the forefront, have become highly susceptible to breaches and ensuing losses.
- Our paper provides a basis for quantifying security investments in the backdrop of **competing retailers** trying to **maximize their expected profits** subject to **strict budget constraints**.
- The retailers compete noncooperatively until a **Nash equilibrium** is achieved, whereby **no retailer can improve** upon his expected profit.

Summary and Conclusions

- Retailers, being in the forefront, have become highly susceptible to breaches and ensuing losses.
- Our paper provides a basis for quantifying security investments in the backdrop of **competing retailers** trying to **maximize their expected profits** subject to **strict budget constraints**.
- The retailers compete noncooperatively until a **Nash equilibrium** is achieved, whereby **no retailer can improve** upon his expected profit.
- **Probability of a successful attack** on a retailer **depends not only on his security level**, but also on that of the others.

Summary and Conclusions

- Retailers, being in the forefront, have become highly susceptible to breaches and ensuing losses.
- Our paper provides a basis for quantifying security investments in the backdrop of **competing retailers** trying to **maximize their expected profits** subject to **strict budget constraints**.
- The retailers compete noncooperatively until a **Nash equilibrium** is achieved, whereby **no retailer can improve** upon his expected profit.
- **Probability of a successful attack** on a retailer **depends not only on his security level**, but also on that of the others.
- **Consumers reveal preferences** through functions that depend on **demand and network security**.

Summary and Conclusions

- **Nonlinear budget constraints** incorporated through **two variational inequality** formulations.

Summary and Conclusions

- **Nonlinear budget constraints** incorporated through **two variational inequality** formulations.
- Various data instances are evaluated through the algorithm, with relevant managerial insights and sensitivity analysis.

Summary and Conclusions

- **Nonlinear budget constraints** incorporated through **two variational inequality** formulations.
- Various data instances are evaluated through the algorithm, with relevant managerial insights and sensitivity analysis.
- The generalized framework of cybersecurity investments in a supply chain network game theory context with nonlinear budget constraints is a **novel contribution to the literature of both variational inequalities and game theory, and cybersecurity investments**.

Thank You!

For more information, please visit:
http://supernet.isenberg.umass.edu/default.htm.