Game Theoretic Model for Cybersecurity with Nonlinear Budget Constraints

ISENBERG SCHOOL OF MANAGEMENT

Anna Nagurney[a], Ladimer S. Nagurney[b], Patrizia Daniele[c], Shivani Shukla[a]

[a]Department of Operations and Information Management, University of Massachusetts, Amherst
[b]Department of Electrical and Computer Engineering, University of Hartford
[c] Department of Mathematics and Computer Science, University of Catania, Italy

The Virtual Center for Supernetworks
Supernetworks for Optimal Decision-Making and Improving the Global Quality of Life

Introduction

- Estimated annual cost to the global economy from cybercrime is more than \$400 billion, conservatively, \$375 billion in losses, more than the national income of most countries (Center for Strategic and International Studies (2014)).
- According to Mandiant (2014), in 2013, the median number of days cyberattackers were present on a victim's network before they were discovered was 229 days.
- Top Security Breaches of 2014: Home Depot attacked four times (employee information and credit/debit cards worth 56 million lost); JPMC (financial information worth 1 million stolen); Target (stolen credit cards sold for \$120 each on the black market; after weeks the price dropped to \$8)
- Each year \$15 billion is spent by organizations in the United States to provide cybersecurity (Gartner and Market Research (2013)). Worldwide spending in 2014 - \$71.1 billion.; Expected in 2015 - \$76.9 billion (Gartner (2014)).

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

Security Level of Firm i, s_i:

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

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:

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

Probability = vulnerability level of the retailer × vulnerability level of the network.

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

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

α_i quantifies size and needs of retailer i.

Demand Price Function for Consumer j, ρ_j:

$$\rho_j = \rho_j(d, \bar{s}) \equiv \hat{\rho}_j(Q, s), \quad j = 1, ..., n.$$

Price is a function of demand (d) and average security.

Profit of Retailer 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. Financial damage at i: D_i.

Expected Utility/Profit for Retailer $i, i = 1, ..., m$:

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

Theorem 1 (Variational Inequality Formulation) *Assume that, for each retailer i, the expected profit function is concave with respect to the variables $\{Q_{i1}, ..., Q_{in}\}$, and s_i, and is continuous and continuously differentiable. Then $(Q^*, s^*) \in K$, the feasible set, is a supply chain Nash equilibrium if and only if it satisfies the variational inequality $\forall (Q, s) \in K$*

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

The SCGT Model of Cybersecuirty Investments with Nonlinear Budget Constraints

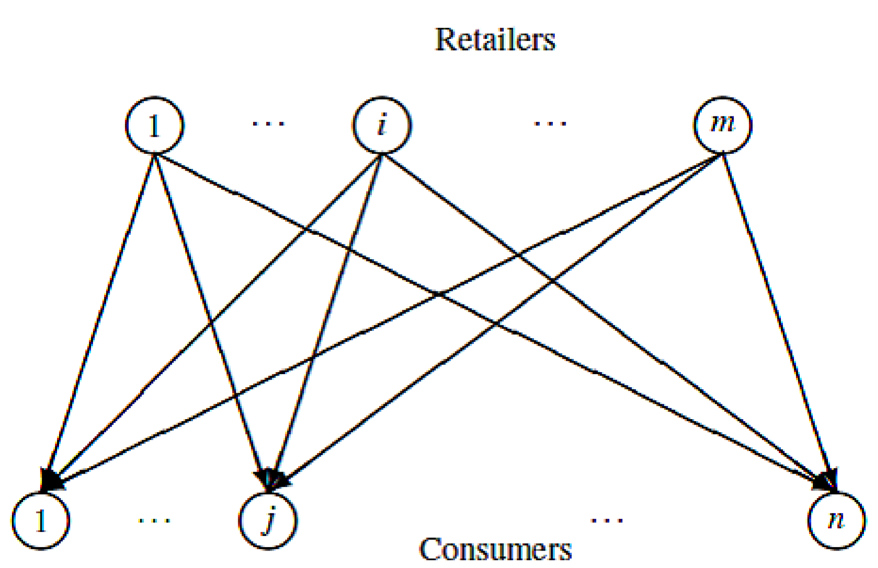
The network is envisioned as bipartite, similar to the one discussed in the previous study. While the overall notations, functional forms, and structure of the model remain the same, there are a *few* changes.

Security Level of Firm i, s_i:

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

where $u_{s_i} < 1$ indicating that perfect security level of 1 is unattainable.

Topology of the Network



Numerical Results for the SCGT Model

For computational purposes, we utilized the Euler method, which is induced by the general iterative scheme of Dupuis and Nagurney (1993). The convergence criterion was $\epsilon = 10^{-4}$. It was implemented using FORTRAN. Following are the results for a three retailer and two consumer instance.

Solution	Ex. 1	Var. 1.1	Var. 1.2	Var. 1.3	Var. 1.4
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

Variant 1.1: Consumer 1 is more sensitive to network security. Variant 1.2: Consumer 2 is more sensitive to average security. Variant 1.3: Demand price functions are increased. Variant 1.4: Both Consumers are substantially more sensitive to average security.

The Nonlinear Budget Constraint:

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

for all i Retailers. This indicates that a Retailer i cannot exceed its budget B_i.

Proving Convexity of the Feasible Set: Convexity of the feasible set gets established by first proving that the investment cost functions are convex (positive second derivative). We arrive at the following variational inequality formulation exactly like in Theorem 1, with an altered feasible set containing the nonlinear budget constraint.

Lagrange Multipliers to Include the Constraint into the Inequality:

Theorem 2 (Variational Inequality Formulation) *A vector (Q^*, s^*, λ^*) in feasible set containing nonegativity constraints is an equilibrium solution if and only if it satisfies the following variational inequality:*

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

$$+[B_i - \alpha_i(\frac{1}{\sqrt{1 - s_i}} - 1)] \times (\lambda_i - \lambda^*_i) \geq 0.$$

Assumption: The Slater Condition: 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.

Numerical Results for the SCGT Model with Nonlinear Constraints

The Euler method was implemented in FORTRAN and run on a Linux system. The convergence criterion ϵ was set to 10^{-4}. The following equilibrium results are for a two retailer and two demand market instance.

Solution	Ex.2	Ex.3
Q^*_{11}	24.27	24.27
Q^*_{12}	98.34	98.31
Q^*_{21}	21.27	21.27
Q^*_{22}	93.34	93.31
d^*_1	45.55	45.53
d^*_2	191.68	191.62
s^*_1	.91	.36
s^*_2	.91	.91
$\bar{s}^*$	.91	.63
λ^*_1	0.00	3.68
λ^*_2	0.00	1.06
$\rho_1(d^*_1, \bar{s}^*)$	54.55	54.53
$\rho_2(d^*_2, \bar{s}^*)$	104.34	104.32
$E(U_1)$	8137.38	8122.77
$E(U_2)$	7213.49	7207.47

Ex.2: Budgets of both retailers is \$2.5 mn (medium to large size firms). Lagrange multipliers are zero since both have unspent budget. Ex.3: Increase in investment cost function of retailer 1. Security level of retailer 1 drops and budgets are all spent.

Cybersecurity and the ChoiceNet Project

Results of both studies are consistent with those obtained in practice. The studies fulfill critical need for economic and game theoretic models in cybercrime space. The models and results make way for exploring potential law and policy interventions.

- ChoiceNet - Lack of infrastructure-centric cyber security (Network Providers) interpreted as lower quality - Might lead to lower business/profits.
- Lack of application-centric security (Content Providers) might also lead to lower profits, loss of reputation, and further manipulation.
- Tailored network packages or bundling of services, features of ChoiceNet, have significant economic and quality benefits, but might lead to: (i) Lack of ownership by network and/or content providers during a cyber attack, (ii) More damage across a (possibly) wider consumer base.
- Modeling cybersecurity in a ChoiceNet framework to quantify the economic benefits and losses.

Papers:

Nagurney, A., Daniele, P., Shukla, S.:A Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints. *S*ubmitted.

Nagurney, A., Nagurney L.S., Shukla, S.: A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability. Computation, Cryptography, and Network Security. Daras, Nicholas J., Rassias, Michael Th. (Eds.), Springer (2015)

References:

Center for Strategic and International Studies: Net losses: Estimating the global cost of cybercrime. Santa Clara, California (2014)

Dupuis, P., Nagurney, A.: Dynamical systems and variational inequalities. Annals of Operations Research, 44, 9-42 (1993)

Gartner: Gartner reveals Top 10 Security Myths, by Ellen Messmer, NetworkWorld, June 11 (2013)

Mandiant: M-trends: Beyond the breach. 2014 threat report. Alexandria, Virginia (2014)

Market Research: United States Information Technology Report Q2 2012, April 24 (2013)

Nagurney, A., Nagurney L.S., A Game Theory Model of Cybersecurity Investments with Information Asymmetry. Ac- cepted in Netnomics (2015)

Acknowledgment: This research 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. This support is gratefully acknowledged.