Game Theory and Cybercrime

Anna Nagurney

John F. Smith Memorial Professor and Director of the Virtual Center for Supernetworks
Isenberg School of Management
University of Massachusetts
Amherst, Massachusetts 01003

Introductory Lectures in Security and Privacy
UMass Amherst
November 24, 2015

Thank you for the invitation to speak with you.

I also acknowledge support for some of the research in this presentation, which has been provided by the Advanced Cyber Security Center (ACSC) and the National Science Foundation (NSF) through the project: *Collaborative Research: Network Innovation Through Choice*, which envisions a Future Internet Architecture.

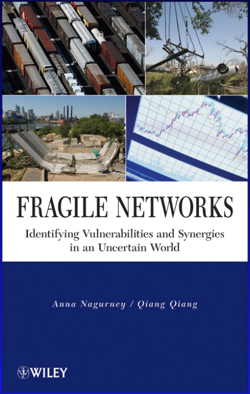
Outline

- Background and Motivation
- Networks and Behavior
- Which Nodes and Links Really Matter
- Game Theory
- A Network Economic Model of Cybercrime
- Some Extensions and Models of Cybersecurity Investments
- Envisioning a New Kind of Internet – ChoiceNet
- Summary and Conclusions

Background and Motivation

How I Became Interested in Cybersecurity

One of my books, written with a UMass Amherst alum, was "hacked" and digital copies of it posted on websites around the globe.



In a sense, this may be viewed as a compliment since clearly someone had determined that it has some sort of *value*.

The publisher John Wiley & Sons was notified and lawyers got involved but how do you contact and then influence those responsible for postings on rather anonymous websites?

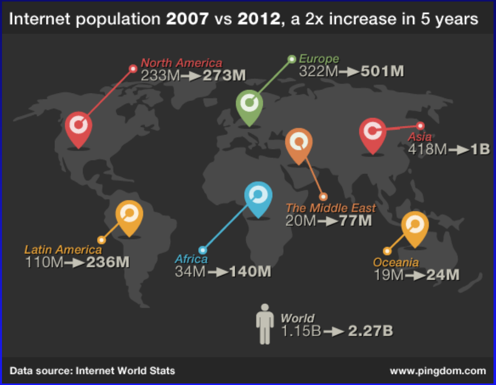
About the same time news about cyberattacks was getting prominent attention in the media and there were those interested in working with us on related research on cybersecurity.

My first jobs after graduating Brown University (and while going to grad school), were in the high technology defense sector working in consulting on naval submarine problems in Newport, Rhode Island.

Issues of security and defense are topics that are of great interest to me. Plus, I love networks and game theory and believe that these tools can help out in modeling, analysis, and solution of cyber and related security problems.

The Internet has transformed the ways in which individuals, groups, organizations communicate, obtain information, access entertainment, and conduct their economic and social activities.

70% of households and 94% of businesses with 10 or more employees are online with an immense growth in mobile devices and social media. In 2012, there were over 2.4 billion users. In 2015, there are 3 billion users, almost half of the world population



The Cost of Cybercrime

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.

Cybercrime

- Cybercrimes are costly for organizations. According to the Ponemon Institute (2015), 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.

Cybercrime

- Cybercrimes are costly for organizations. According to the Ponemon Institute (2015), 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.

- All industries fall victim to cybercrime, but to different degrees with defense, energy and utilities, and financial service companies experiencing higher cybercrime costs than organizations in retail, hospitality, and consumer products.

Cybercrime

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 (The New York Times (2015)).

Since financial gains, through the subversion of processes and controls, are one of the most attractive benefits emerging from cyberattacks, financial service firms are targeted incessantly.

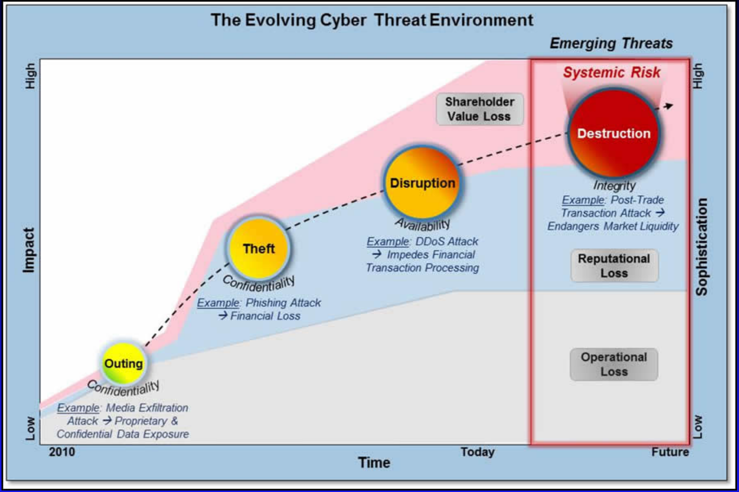
The large-scale data breach of JP Morgan Chase, Kaspersky Lab's detection of a two-year infiltration of 100 banks across the world costing $1 billion (USA Today (2015)), and the Dridex malware related losses of $100 million worldwide (The Guardian (2015)) are some of the widely accepted cautionary tales in this sector.

Cybercrime

More than 76 million households and seven million small businesses were compromised because of JP Morgan attacks.

Clearly, hackers go where there is money.

The most costly cybercrimes (58% annually) are those caused by denial of service, malicious insider and web-based attacks. Mitigation may require enabling technologies, intrusion prevention systems, applications security testing solutions and enterprise solutions.



Source: Sarnowski for Booz Allen and Hamilton

Putting Cybercrime in Context

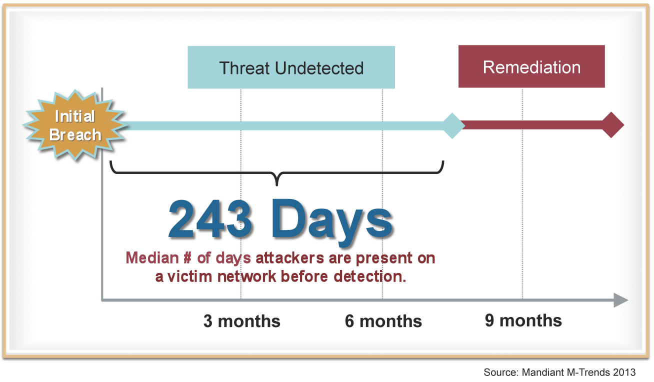
Putting Malicious Cyber Activity in Context

CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Source: The Economic Impact of Cybercrime and Cyber Espionage, Center for Strategic and International Studies, July 2013, sponsored by McAfee.

Cyberattacks

Every minute, of every hour, of ever day, a major financial institution is under attack (Wilson in *The Telegraph*, October 6, 2013).



Preparation, prediction, and protection are key - which are the weakest links?

Cybercrime and Financial Institutions

According to a recent survey cybercrime is placing heavy strains on the global financial sector, with cybercrime now the second most commonly reported economic crime affecting financial services firms.

Cybercrime and Financial Institutions

According to a recent survey cybercrime is placing heavy strains on the global financial sector, with cybercrime now the second most commonly reported economic crime affecting financial services firms.

Cybercrime accounted for 38% of all economic crimes in the financial sector, as compared to an average of 16% across all other industries.

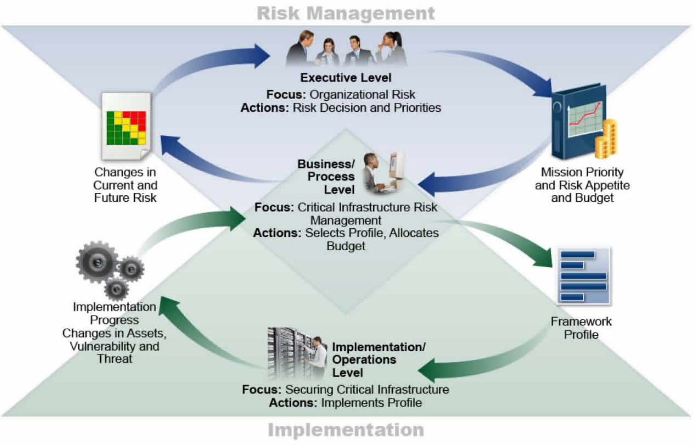
Cybercrime and Financial Institutions

According to a recent survey cybercrime is placing heavy strains on the global financial sector, with cybercrime now the second most commonly reported economic crime affecting financial services firms.

Cybercrime accounted for 38% of all economic crimes in the financial sector, as compared to an average of 16% across all other industries.

Cyberattacks are intrusive and economically costly. In addition, they may adversely affect a companys most valuable asset its reputation.

It's About Risk Management

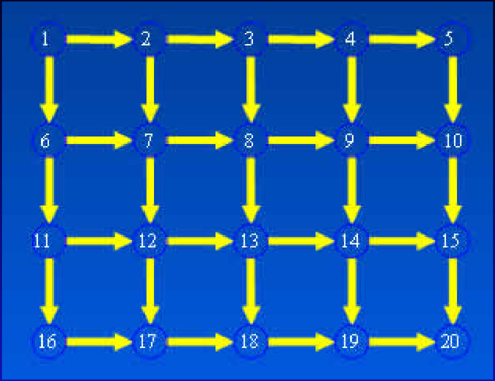


Source: Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), February 12, 2014

Networks and Behavior

Our enterprises and organizations are critically dependent on infrastructure network systems including the Internet.

Network Components



The components of networks as a theoretical (modeling, analysis, and solution) construct include: nodes, links, and flows. We use such a representation to conceptualize, formulate, and study network systems in the real-world.

Components of Common Physical Networks

Network System	Nodes	Links	Flows
Transportation	Intersections, Homes, Workplaces, Airports, Railyards	Roads, Airline Routes, Railroad Track	Automobiles, Trains, and Planes,
Manufacturing and logistics	Workstations, Distribution Points	Processing, Shipment	Components, Finished Goods
Communication	Computers, Satellites, Telephone Exchanges	Fiber Optic Cables Radio Links	Voice, Data, Video
Energy	Pumping Stations, Plants	Pipelines, Transmission Lines	Water, Gas, Oil, Electricity

Decision-makers select their cost-minimizing routes.

		User-Optimized
Decentralized	Selfish	U–O
vs. ⟺	vs. ⟺	vs.
Centralized	Unselfish	S–O
		System-Optimized

Flows are routed so as to minimize total cost to society.

Two fundamental principles of travel behavior, due to Wardrop (1952), with terms coined by Dafermos and Sparrow (1969).

User-optimized (U-O) (network equilibrium) Problem – each user determines his/her cost minimizing route of travel between an origin/destination, until an equilibrium is reached, in which no user can decrease his/her cost of travel by unilateral action (in the sense of Nash).

System-optimized (S-O) Problem – users are allocated among the routes so as to minimize the total cost in the system, where the total cost is equal to the sum over all the links of the link's user cost times its flow.

The U-O problems, under certain simplifying assumptions, possesses optimization reformulations. But now we can handle cost asymmetries, multiple modes of transport, and different classes of travelers, without such assumptions.

We Can State These Conditions Mathematically!

The U-O and S-O Conditions

Definition: U-O or Network Equilibrium – Fixed Demands
A path flow pattern x^*, with nonnegative path flows and O/D pair demand satisfaction, is said to be U-O or in equilibrium, if the following condition holds for each O/D pair $w \in W$ and each path $p \in P_w$:

$$C_p(x^*) \begin{cases} = \lambda_w, & \text{if} \quad x_p^* > 0, \\ \geq \lambda_w, & \text{if} \quad x_p^* = 0. \end{cases}$$

Definition: S-O Conditions
A path flow pattern x with nonnegative path flows and O/D pair demand satisfaction, is said to be S-O, if for each O/D pair $w \in W$ and each path $p \in P_w$:

$$\hat{C}'_p(x) \begin{cases} = \mu_w, & \text{if} \quad x_p > 0, \\ \geq \mu_w, & \text{if} \quad x_p = 0, \end{cases}$$

where $\hat{C}'_p(x) = \sum_{a \in \mathcal{L}} \frac{\partial \hat{c}_a(f_a)}{\partial f_a} \delta_{ap}$, and μ_w is a Lagrange multiplier.

The importance of behavior will now be illustrated through a famous example known as the Braess paradox which demonstrates what can happen under *U-O* as opposed to *S-O* behavior.

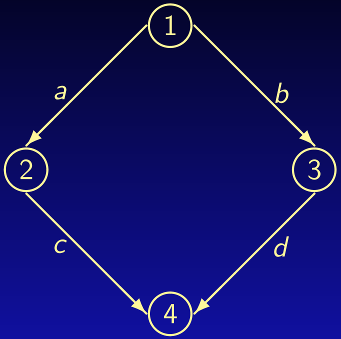
Although the paradox was presented in the context of transportation networks, it is relevant to other network systems in which decision-makers act in a noncooperative (competitive) manner.

The Braess (1968) Paradox

Assume a network with a single O/D pair (1,4). There are 2 paths available to travelers: $p_1 = (a, c)$ and $p_2 = (b, d)$.

For a travel demand of **6**, the equilibrium path flows are $x^*_{p_1} = x^*_{p_2} = 3$ and

The equilibrium path travel cost is $C_{p_1} = C_{p_2} = 83$.



$$c_a(f_a) = 10 f_a, \quad c_b(f_b) = f_b + 50,$$

$$c_c(f_c) = f_c + 50, \quad c_d(f_d) = 10 f_d.$$

Adding a Link Increases Travel Cost for All!

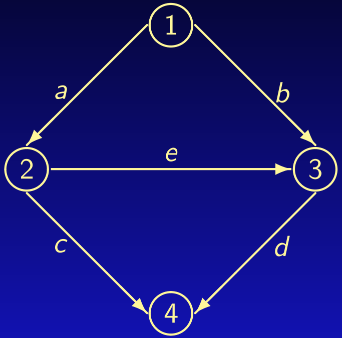
Adding a new link creates a new path $p_3 = (a, e, d)$.

The original flow distribution pattern is no longer an equilibrium pattern, since at this level of flow the cost on path p_3, $C_{p_3} = 70$.

The new equilibrium flow pattern network is

$x^*_{p_1} = x^*_{p_2} = x^*_{p_3} = 2$.

The equilibrium path travel cost: $C_{p_1} = C_{p_2} = C_{p_3} = 92$.



$c_e(f_e) = f_e + 10$

The 1968 Braess article has been translated from German to English and appears as:

On a Paradox of Traffic Planning,

Dietrich Braess, Anna Nagurney, and Tina Wakolbinger, *Transportation Science* 39 (2005), pp 446-450.

Über ein Paradoxon aus der Verkehrsplanung

Von D. BRAESS, Münster [1])

Eingegangen am 28. März 1968

Zusammenfassung: Für die Straßenverkehrsplanung möchte man den Verkehrsfluß auf den einzelnen Straßen des Netzes abschätzen, wenn die Zahl der Fahrzeuge bekannt ist, die zwischen den einzelnen Punkten des Straßennetzes verkehren. Welche Wege am günstigsten sind, hängt nun nicht nur von der Beschaffenheit der Straße ab, sondern auch von der Verkehrsdichte. Es ergeben sich nicht immer optimale Fahrzeiten, wenn jeder Fahrer nur für sich den günstigsten Weg heraussucht. In einigen Fällen kann sich durch Erweiterung des Netzes der Verkehrsfluß sogar so umlagern, daß größere Fahrzeiten erforderlich werden.

Summary: For each point of a road network let be given the number of cars starting from it, and the destination of the cars. Under these conditions one wishes to estimate the distribution of the traffic flow. Whether a street is preferable to another one depends not only upon the quality of the road but also upon the density of the flow. If every driver takes that path which looks most favorable to him, the resultant running times need not be minimal. Furthermore it is indicated by an example that an extension of the road network may cause a redistribution of the traffic which results in longer individual running times.

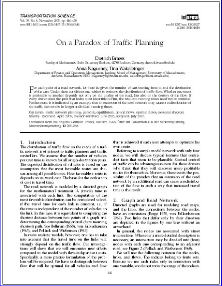
1. Einleitung

Für die Verkehrsplanung und Verkehrssteuerung interessiert, wie sich der Fahrzeugstrom auf die einzelnen Straßen des Verkehrsnetzes verteilt. Bekannt sei dabei die Anzahl der Fahrzeuge für alle Ausgangs- und Zielpunkte. Bei der Berechnung wird davon ausgegangen, daß von den möglichen Wegen jeweils der günstigste gewählt wird. Wie günstig ein Weg ist, richtet sich nach dem Aufwand, der zum Durchfahren nötig ist. Die Grundlage für die Bewertung des Aufwandes bildet die Fahrzeit.

Für die mathematische Behandlung wird das Straßennetz durch einen gerichteten Graphen beschrieben. Zur Charakterisierung der Bögen gehört die Angabe des Zeitaufwandes. Die Bestimmung der günstigen Stromverteilungen kann als gelöst betrachtet werden, wenn die Bewertung konstant ist, d. h., wenn die Fahrzeiten unabhängig von der Größe des Verkehrsflusses sind. Sie ist dann äquivalent mit der bekannten Aufgabe, den kürzesten Abstand zweier Punkte eines Graphen und den zugehörigen kritischen Pfad zu bestimmen [1], [5], [7].

Will man das Modell aber realistischer gestalten, ist zu berücksichtigen, daß die benötigte Zeit stark von der Stärke des Verkehrs abhängt. Wie die folgenden Untersuchungen zeigen, ergeben sich dann gegenüber dem Modell mit konstanter (belastungsunabhängiger) Bewertung z. T. völlig neue Aspekte. Dabei erweist sich schon eine Präzisierung der Problemstellung als notwendig; denn es ist zwischen dem Strom zu unterscheiden, der für alle am günstigsten ist,, und dem, der sich einstellt, wenn jeder Fahrer nur seinen eigenen Weg optimalisiert.

[1]) Priv.-Doz. Dr. Dietrich BRAESS, Institut für numerische und instrumentelle Mathematik, 44 Münster, Hüfferstr. 3 a.



TRANSPORTATION SCIENCE

On a Paradox of Traffic Planning

Dietrich Braess

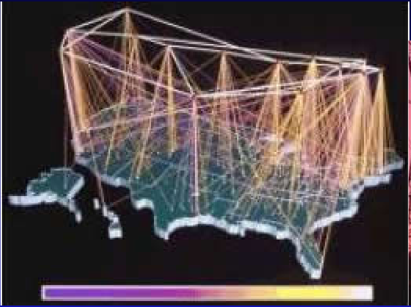
Anna Nagurney, Tina Wakolbinger

1. Introduction

Under S-O behavior, the total cost in the network is minimized, and the new route p_3, under the same demand, would not be used.

The Braess paradox never occurs in S-O networks.

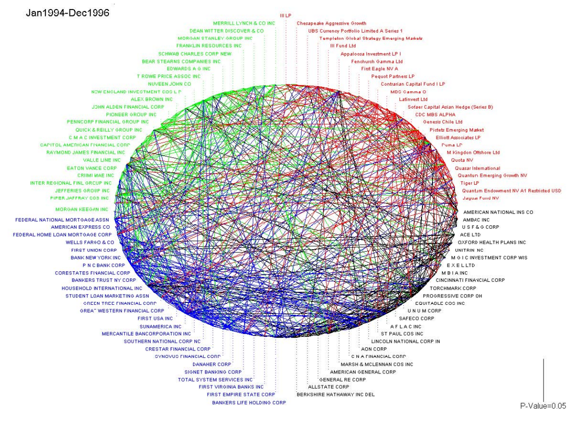
Other Networks that Behave like Traffic Networks



The Internet and electric power networks and even supply chains!

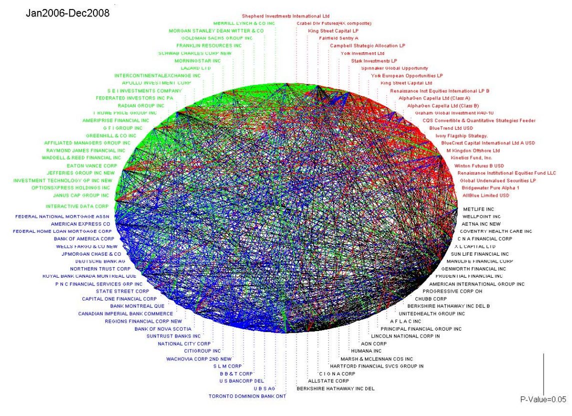
Which Nodes and Links Really Matter?

Empirical Evidence: Jan. 1994 - Dec. 1996 - Connectivity, Vulnerability



Granger Causality Results: Green Broker, Red Hedge Fund, Black Insurer, Blue Bank Source: Billio, Getmansky, Lo, and Pelizzon (2011)

Empirical Evidence: Jan. 2006 - Dec. 2008 - Connectivity, Vulnerability



Granger Causality Results: Green Broker, Red Hedge Fund, Black Insurer, Blue Bank Source: Billio, Getmansky, Lo, and Pelizzon (2011)

The Financial Network Model

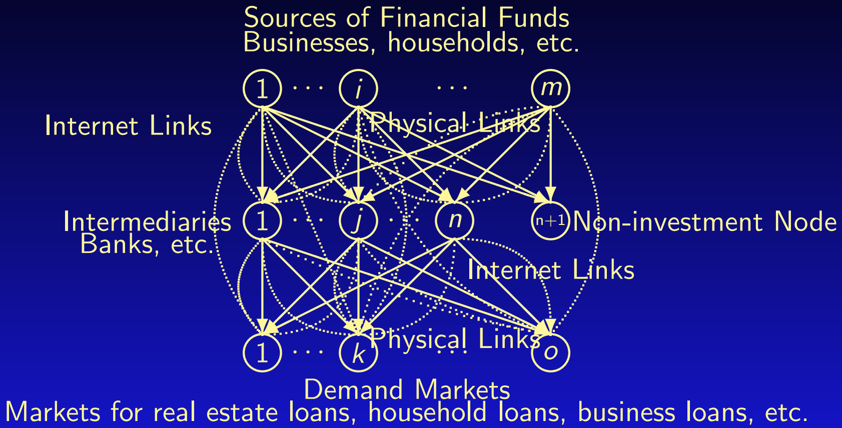


Figure 1: The Structure of the Financial Network with Intermediation

The Nagurney and Qiang (N-Q) Network Performance Measure

Definition: A Unified Network Performance Measure
The network performance/efficiency measure, $\mathcal{E}(G,d)$, for a given network topology G and the equilibrium (or fixed) demand vector d, is:

$$\mathcal{E} = \mathcal{E}(G,d) = \frac{\sum_{w \in W} \frac{d_w}{\lambda_w}}{n_W},$$

where recall that n_W is the number of O/D pairs in the network, and d_w and λ_w denote, for simplicity, the equilibrium (or fixed) demand and the equilibrium disutility for O/D pair w, respectively.

Anna Nagurney and Qiang Qiang, A Network Efficiency Measure with Application to Critical Infrastructure Networks, *Journal of Global Optimization* 40 (2008), pp 261-275.

The Importance of Nodes and Links

Definition: Importance of a Network Component

The importance of a network component $g \in G$, $I(g)$, is measured by the relative network efficiency drop after g is removed from the network:

$$I(g) = \frac{\triangle \mathcal{E}}{\mathcal{E}} = \frac{\mathcal{E}(G,d) - \mathcal{E}(G-g,d)}{\mathcal{E}(G,d)}$$

where $G - g$ is the resulting network after component g is removed from network G.

Approach to Identifying the Importance of Network Components

The elimination of a link is treated in the N-Q network efficiency measure by removing that link while the removal of a node is managed by removing the links entering and exiting that node.

In the case that the removal results in no path connecting an O/D pair, we simply assign the demand for that O/D pair to an abstract path with a cost of infinity.

The N-Q measure is well-defined even in the case of disconnected networks.

The Ranking of Links in the Braess Network

Table 1: Link Results for the Braess Network

Link	N-Q Measure		L-M Measure	
	Importance Value	Importance Ranking	Importance Value	Importance Ranking
a	.2069	1	.1056	3
b	.1794	2	.2153	2
c	.1794	2	.2153	2
d	.2069	1	.1056	3
e	-.1084	3	.3616	1

N-Q (Nagurney-Qiang); L-M (Latora-Marchiori)

The Ranking of Nodes in the Braess Network

Table 2: Nodal Results for the Braess Network

Node	N-Q Measure		L-M Measure	
	Importance Value	Importance Ranking	Importance Value	Importance Ranking
1	1.0000	1	—	—
2	.2069	2	.7635	1
3	.2069	2	.7635	1
4	1.0000	1	—	—

Advantages of the N-Q Network Efficiency Measure

- The measure captures *demands, flows, costs, and behavior of users*, in addition to network topology.

- The resulting importance definition of network components is applicable and *well-defined even in the case of disconnected networks*.

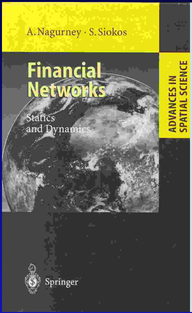
- It can be used to identify the *importance (and ranking) of either nodes, or links, or both*.

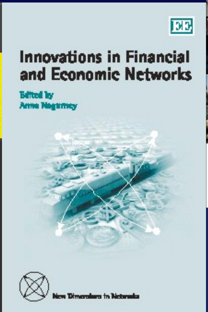
- It can be applied to *assess the efficiency/performance of a wide range of network systems, including financial systems and supply chains under risk and uncertainty*.

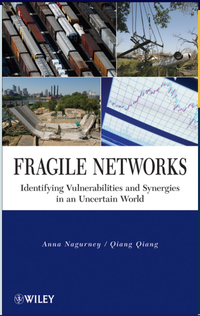
- It is applicable also to *elastic demand networks*.

- It is *applicable to dynamic networks*, *including the Internet*.

Financial Networks and Game Theory







Game Theory

Game Theory

There are many game theory problems and tools for solving such problems. There is noncooperative game theory, in which the players or decision-makers compete with one anther, and cooperative game theory, in which players cooperate with one another.


John F. Nash

In noncooperative games, the governing concept is that of Nash equilibrium. In cooperative games, we can apply Nash bargaining theory.

Game Theory

Game theory is very useful.

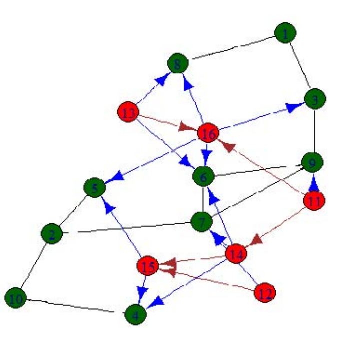
In order to set up a game theory model, you need to identify the players, their strategic variables (strategies), the constraints on their strategies, and their pay-off functions.

Pay-off functions can be profit functions, for example.

A Network Economic Model of Cybercrime

Network Economics of Cybecrime

Green Nodes represent Institutions
Red Nodes the Attackers
Red Edges between Attackers can represent collusion or transactions of stolen goods.
Black Edges between Institutions can show sharing of information and mutual dependence.
Blue Edges between the Attacker and Institution can represent threats and attacks.



We lay the foundation for the development of network economics based models for cyberccrime in financial services.

Our view is that financial firms produce/possess commodities (or products) that hackers (criminals) seek to obtain.

Both financial services firms as well as hackers are economic agents.

We assume that the firms (as well as the hackers) can be located in different regions of a country or in different countries. Financial service firms may also be interpreted as prey and the hackers as predators.

Commodities or products that the hackers seek to acquire may include: credit card numbers, password information, specific documents, etc.

The financial firms are the producers of these commodities whereas the hackers act as agents and "sell" these products, if they acquire them, at the "going" market prices.

There is a "price" at which the hackers acquire the financial commodity from a financial institution and a price at which they sell the hacked product in the demand markets. The former we refer to as the supply price and the latter is the demand price.

In addition, we assume that there is a transaction cost associated between each pair of financial and demand markets for each commodity. These transaction costs can be generalized costs that also capture risk.

Indeed, if the cyber criminals do not find demand markets for their acquired financial commodities (since there are no consumers willing to pay the price) then there is no economic incentive for them to acquire the financial commodities.

Indeed, if the cyber criminals do not find demand markets for their acquired financial commodities (since there are no consumers willing to pay the price) then there is no economic incentive for them to acquire the financial commodities.

To present another criminal network analogue – consider the market for illegal drugs, with the U.S. market being one of the largest, if not the largest one. If there is no demand for the drugs then the suppliers of illegal drugs cannot recover their costs of production and transaction and the flows of drugs will go to zero.

Network Economics of Cybercrime

Indeed, if the cyber criminals do not find demand markets for their acquired financial commodities (since there are no consumers willing to pay the price) then there is no economic incentive for them to acquire the financial commodities.

To present another criminal network analogue – consider the market for illegal drugs, with the U.S. market being one of the largest, if not the largest one. If there is no demand for the drugs then the suppliers of illegal drugs cannot recover their costs of production and transaction and the flows of drugs will go to zero.

According to a recent Rand report, for many, the cyber black market can be more profitable than the illegal drug trade.

The Model

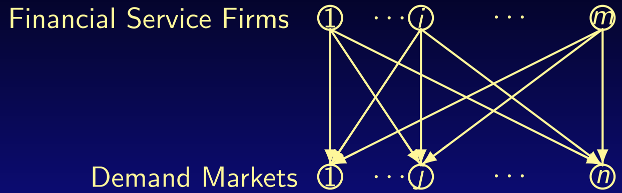


Figure 2: A bipartite network of the model with financial institutions and demand markets for hacked products

Denote a typical financial institution by i and a typical demand market by j. Let s_i denote the supply of the commodity associated with i and let π_i denote the supply price of the commodity associated with i. Let d_j denote the demand associated with demand market j and let ρ_j denote the demand price associated with demand market j.

The Model

Let Q_{ij} denote the possible illicit nonnegative commodity trade flow between the firm and demand market pair (i, j) and let c_{ij} denote the nonnegative unit transaction cost associated with obtaining the product between (i, j).

Definition: Market Equilibrium Conditions
The market equilibrium conditions, assuming perfect competition, take the following form: For all pairs of firms and demand markets $(i, j) : i = 1, \ldots, m; j = 1, \ldots, n$:

$$\pi_i + c_{ij} \begin{cases} = \rho_j, & \text{if} \quad Q^*_{ij} > 0 \\ \geq \rho_j, & \text{if} \quad Q^*_{ij} = 0. \end{cases} \tag{1}$$

The Model

The feasibility conditions must hold for every i and j:

$$s_i = \sum_{j=1}^{n} Q_{ij} \tag{2}$$

and

$$d_j = \sum_{i=1}^{m} Q_{ij}. \tag{3}$$

(2) and (3) state that the markets clear and that the supply at each supply market is equal to the sum of the financial commodity flows to all the demand markets. Also, the demand at a demand market must be satisfied by the sum of the commodity shipments from all the supply markets. Let K denote the closed convex set where $K \equiv \{(s, Q, d) | (2) \text{ and } (3) \text{ hold}\}$.

The Model

The supply price, demand price, and transaction cost structure is now discussed. Assume that the commodity price associated with a firm may depend upon the supply of the commodity at every firm:

$$\pi = \pi(s) \tag{4}$$

where π is a known smooth function.

The demand price associated with a demand market may depend upon, in general, the demand of the commodity at every demand market:

$$\rho = \rho(d) \tag{5}$$

where ρ is a known smooth function.

The transaction cost between a pair of supply and demand markets may, in general, depend upon the shipments of the commodity between every pair of markets:

$$c = c(Q) \tag{6}$$

where c is a known smooth function.

We now present the variational inequality formulation of the equilibrium conditions (1).

Theorem 1. A commodity production, shipment, and consumption pattern $(s^*, Q^*, d^*) \in K$ is in equilibrium if and only if it satisfies the variational inequality problem:

$$\pi(s^*)\cdot(s-s^*)+c(Q^*)\cdot(Q-Q^*)-\rho(d^*)\cdot(d-d^*) \geq 0, \quad \forall (s, Q, d) \in K. \tag{7}$$

Numerical Example

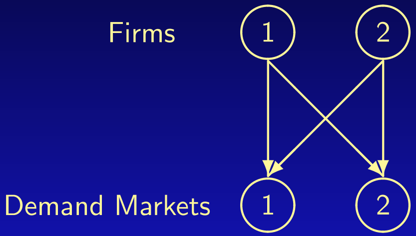


Figure 3: Example Network Topology

Numerical Example

The supply price functions are:

$$\pi_1(s) = 5s_1 + s_2 + 2, \quad \pi_2(s) = 2s_2 + s_1 + 3.$$

The transaction cost functions are:

$$c_{11}(Q) = Q_{11} + .5Q_{12} + 1, \quad c_{12}(Q) = 2Q_{12} + Q_{22} + 1.5,$$

$$c_{21}(Q) = 3Q_{21} + 2Q_{11} + 15, \quad c_{22}(Q) = 2Q_{22} + Q_{12} + 10.$$

The demand price functions are:

$$\rho_1(d) = -2d_1 - d_2 + 28.75, \quad \rho_2(d) = -4d_2 - d_1 + 41.$$

The equilibrium supply, shipment, and consumption pattern is then given by:

$$s_1^* = 3, \quad s_2^* = 2,$$

$$Q_{11}^* = 1.5, \quad Q_{12}^* = 1.5, \quad Q_{21}^* = 0, \quad Q_{22}^* = 2,$$

$$d_1^* = 1.5, \quad d_2^* = 3.5.$$

Numerical Example

The incurred equilibrium supply prices, costs, and demand prices are:

$$\pi_1 = 19, \quad \pi_2 = 10,$$

$$c_{11} = 3.25, \quad c_{12} = 6.5, \quad c_{21} = 18, \quad c_{22} = 15.5,$$

$$\rho_1 = 22.25, \quad \rho_2 = 25.5.$$

Numerical Example

Firm 2 does not "trade" with Demand Market 1. This is due, in part, to the high fixed cost associated with trading between this market pair. Hence, one can interpret this as corresponding to a sufficiently high transaction cost (which can also capture in a generalized setting, the risk of being caught).

The above single commodity model we have generalized to multiple financial commodities.

In addition, we have included a variety of policy interventions.

We have solved problems of this type using variational inequality algorithms with more than 250,000 variables.

Some Extensions and Models of Cybersecurity Investments

Some Extensions

Interestingly, there is a short time window during which the value of a financial product acquired through cybercrime is positive but it decreases during the time window.

Hence, financial products such as credit cards that are hacked can be treated as perishable products such as fruits, vegetables, etc.

Some Extensions

- After the major Target breach, credit cards obtained thus initially sold for $120 each on the black market, but, within weeks, as banks started to cancel the cards, the price dropped to $8 and, seven months after Target learned about the breach, the cards had essentially no value.

Some Extensions

- After the major Target breach, credit cards obtained thus initially sold for \$120 each on the black market, but, within weeks, as banks started to cancel the cards, the price dropped to \$8 and, seven months after Target learned about the breach, the cards had essentially no value.

- In addition, different brands of credit cards can be viewed as different products since they command different prices on the black market. For example, according to Leinwand Leger (2014) credit cards with the highest credit limits, such as an American Express Platinum card, command the highest prices.

Some Extensions

• After the major Target breach, credit cards obtained thus initially sold for $120 each on the black market, but, within weeks, as banks started to cancel the cards, the price dropped to $8 and, seven months after Target learned about the breach, the cards had essentially no value.

• In addition, different brands of credit cards can be viewed as different products since they command different prices on the black market. For example, according to Leinwand Leger (2014) credit cards with the highest credit limits, such as an American Express Platinum card, command the highest prices.

• A card number with a low limit might sell for $1 or $2, while a high limit card number can sell for $15 or considerably more, as noted above. Hacked credit card numbers of European credit cards can command prices five times higher than U.S. cards (see Peterson (2013)).

Perishability and Cybercrime in Financial Products

In the paper, A Multiproduct Network Economic Model of Cybercrime in Financial Services, Anna Nagurney, *Service Science* 7(1) (2015) pp 70-81, I handle multiple products and show how prices decrease as a function of the average time to deliver the cyber hacked financial product.

Perishability and Cybercrime in Financial Products

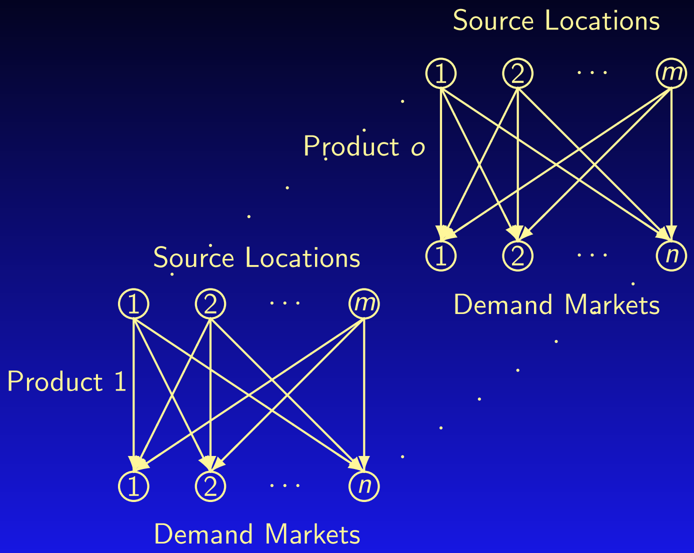


Figure 4: Structure of the Network Economic Problem

Cybersecurity Investments and Game Theory

In the papers below, we demonstrate competition among firms in terms of product delivery and cybersecurity investments.

A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability, Anna Nagurney, Ladimer S. Nagurney, and Shivani Shukla (2015), in: *Computation, Cryptography, and Network Security*, Nicholas J.Daras and Michael Th. Rassias, (Eds.), Springer, pp 381-398.

A Game Theory Model of Cybersecurity Investments with Information Asymmetry, Anna Nagurney, Ladimer S. Nagurney (2015), *Netnomics* 16(1-2), pp 127-148.

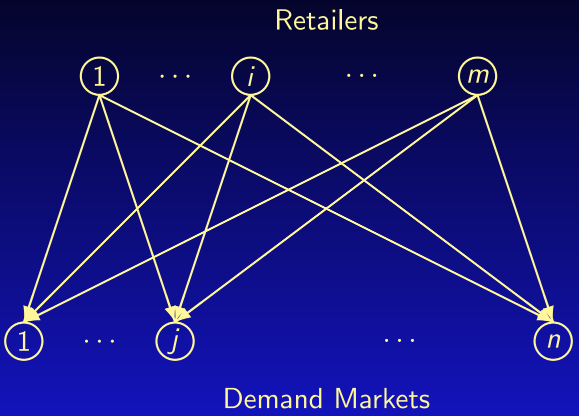


Figure 5: The Structure of the Supply Chain Network Game Theory Model

Cybersecurity Investments and Game Theory

In our most recent paper, Multifirm Models of Cybersecurity Investment Competition vs. Cooperation and Network Vulnerability, Anna Nagurney and Shivani Shukla (2015), Isenberg School of Management, University of Massachusetts Amherst, we investigate the potential gains among firms in the same industry of information sharing through the exchange of cybersecurity investment information.

We show how the Nash bargaining solution provides the highest expected profits and the lowest network vulnerability as compared to the Nash equilibrium and system-optimization solution.

Envisioning a New Kind of Internet – ChoiceNet

Envisioning a New Kind of Internet – ChoiceNet

We are one of five teams funded by NSF as part of the Future Internet Architecture (FIA) project. Our project is: *Network Innovation Through Choice* and the envisioned architecture is *ChoiceNet*.

Team:

- University of Kentucky: Jim Griffioen, Ken Calvert
- North Carolina State University: Rudra Dutta, George Rouskas
- RENCI/UNC: Ilia Baldine
- University of Massachusetts Amherst: Tilman Wolf, Anna Nagurney

Network Economic Conundrums and Operations Research to the Rescue

- New architectures are focusing on networking technology, and not on economic interactions. Also, they lack in mechanisms to introduce competition and market forces.

Network Economic Conundrums and Operations Research to the Rescue

- New architectures are focusing on networking technology, and not on economic interactions. Also, they lack in mechanisms to introduce competition and market forces.

- Existing economic models cannot be deployed in today's Internet: no mechanisms in order to create and discover contracts with any provider and to do so on short-time scales, and time-scales of different lengths.

Network Economic Conundrums and Operations Research to the Rescue

- New architectures are focusing on networking technology, and not on economic interactions. Also, they lack in mechanisms to introduce competition and market forces.

- Existing economic models cannot be deployed in today's Internet: no mechanisms in order to create and discover contracts with any provider and to do so on short-time scales, and time-scales of different lengths.

- We have developed multitiered network economic game theory models using novel operations research methodologies, including that of *projected dynamical systems* to study ChoiceNet and to explore the evolution of prices and flows among content and service providers.

USA NSF Future Internet Architecture (FIA) Projects

• Named Data Networking (NDN) – UCLA (lead) – Content-centric, focus on "what" not "where"

• MobilityFirst – Rutgers University (lead) – Cellular convergence (4-5B devices) interconnected vehicles

• NEBULA – University of Pennsylvania (lead) – Reliable, high-speed core interconnecting data centers

• eXpressive Internet Architecture (XIA) – Carnegie Mellon University (lead) – Rich set of communication entities as network principals

• ChoiceNet – University of Massachusetts Amherst (lead) – project started September 2011; assigned FIA status in 2012.

ChoiceNet Goals

- Expose choices throughout the network
- – Network is no longer a "black box"

- Interactions between technological alternatives and relationships
- – Introduction of a dynamic "economy plane"
- – Money as a driver to overcome inertia by providers
- – Market forces can play out within the network itself

- Services are at the core of ChoiceNet – "everything is a service"
- – Services provide a benefit but entail a cost
- – Services are created, composed, sold, verified, etc.

The focus of ChoiceNet is on *choices* and *network economics.* Choice criteria can also include privacy, minimization of risk, even environmental impact minimization.

Transparency associated with ChoiceNet and having more refined routing options can also aid in cybersecurity.

ChoiceNet Principles

Competition Drives Innovation!

ChoiceNet Principles

Competition Drives Innovation!

Services are at core of ChoiceNet
("everything is a service")

Services provide a benefit, have a cost
Services are created, composed, sold, verified, etc.

ChoiceNet Principles

Competition Drives Innovation!

Services are at core of ChoiceNet ("everything is a service")

Services provide a benefit, have a cost
Services are created, composed, sold, verified, etc.

"Encourage alternatives" Provide building blocks for different types of services

ChoiceNet Principles

Competition Drives Innovation!

Services are at core of ChoiceNet
("everything is a service")

Services provide a benefit, have a cost
Services are created, composed, sold, verified, etc.

"Encourage alternatives" Provide building blocks for different types of services

"Know what happened" Ability to evaluate services

ChoiceNet Principles

Competition Drives Innovation!

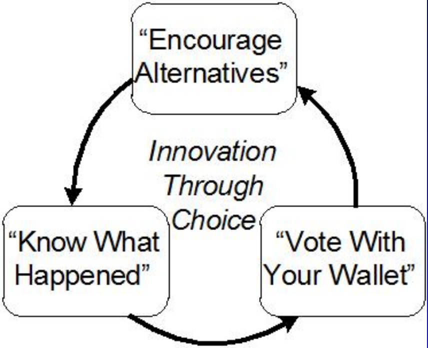
Services are at core of ChoiceNet ("everything is a service")

Services provide a benefit, have a cost
Services are created, composed, sold, verified, etc.

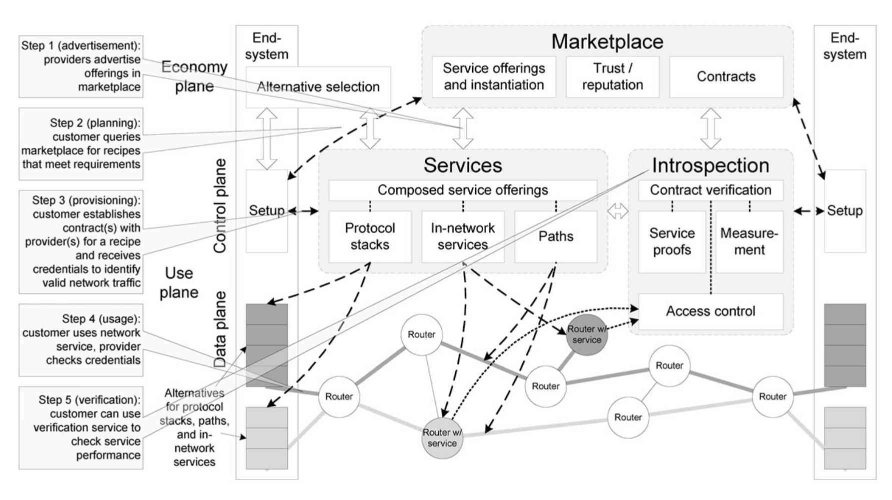
"Encourage alternatives" Provide building blocks for different types of services

"Know what happened" Ability to evaluate services

"Vote with your wallet" Reward good services!



ChoiceNet Architecture



Entities in ChoiceNet

- ChoiceNet enables the composition of services and economic relationships
  - Economy plane: customer-provider relationships
  - Use plane: client-service relationships
  - Positive feature is the ability to reflect real-world relationships.

Provider Ecosystem

- Incentives for participation?
- – Everyone can be rewarded (host, verifier, author, integrator)
- – Innovative and good services get rewarded

- Payments among actors to sustain viability
- – Economy plane distributes value (i.e., money)

- Same commercial entities as today?
- – Similar providers, but also finer-grained providers
- – New providers for composition and verification.

ChoiceNet Technologies

- Economy plane

– Methods for describing composing, and instantiating services

– Market places for connecting customers and providers (i.e., search for services)

– IDs associated with entities

- Use plane

– Verification of the economy plane contracts in use plane

– Measurement services to verify offerings.

Use Cases Enabled by ChoiceNet

- ChoiceNet / economy plane enables new business models in the Internet

– Very dynamic economic relationships are possible
– All entities get rewarded.

- Examples

– Movie streaming
– reading *The New York Times* or *The Boston Globe* in a coffee shop (short-term and long-term contracts)
–Customers as providers.

Our Network Models Utilize Game Theory - Flow of Content

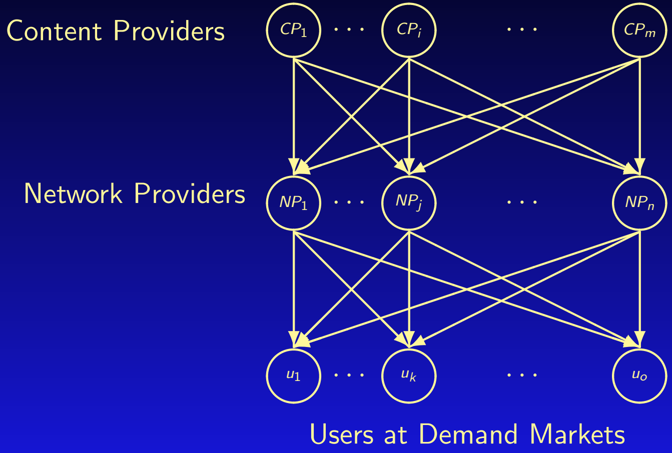


Figure 6: The Network Structure of the Multi-Provider Model's Content Flows

Our Network Models Utilize Game Theory - Flow of Payments

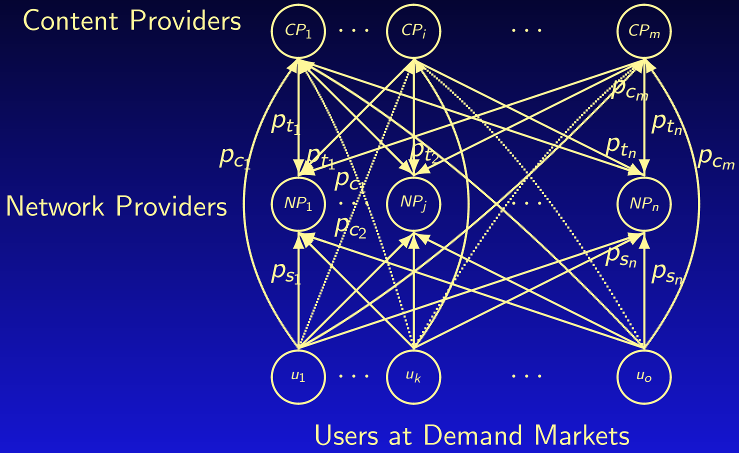


Figure 7: Graphic of the Multi-Provider Model with a Focus on Payments

Some of Our Publications on the NSF Project

[1] Nagurney, A., Li, D., 2013. A Dynamic Network Oligopoly Model with Transportation Costs, Product Differentiation, and Quality Competition. *Computational Economics* 44(2), 201-229.

[2] Nagurney, A., Li, D., Wolf, T., Saberi, S., 2013. A Network Economic Game Theory Model of a Service-Oriented Internet with Choices and Quality Competition. *Netnomics* 14(1-2), 1-25. Notable Computing Article Published in 2013 ACM Computing Reviews - in the Computer Applications category.

[3] Rouskas, G. N., Baldine, I., Calvert, K., Dutta, R., Griffioen, J., Nagurney, A., Wolf, T., 2013. ChoiceNet: Network Innovation through Choice. In *Proceedings of the 17th Conference on Optical Network Design and Modeling* (ONDM 2013), April 16-19, Brest, France. (Invited paper).

Some of Our Publications on the NSF Project

[4] Saberi, S., Nagurney, A., Wolf, T., 2014. A Network Economic Game Theory Model of a Service-Oriented Internet with Price and Quality Competition in Both Content and Network Provision. *Service Science* 6(4), 229-250.

[5] Wolf, T., Griffioen, J., Calvert, K., Dutta, R., Rouskas, G., Baldine, I., Nagurney, A., 2012. Choice as a Principle in Network Architecture. In *Proceedings of ACM SIGCOMM 2012*, Helsinki, Finland, August 13-17.

[6] Wolf, T., Zink, M., Nagurney, A., 2013. The Cyber-Physical Marketplace: A Framework for Large-Scale Horizontal Integration in Distributed Cyber-Physical Systems. In *Proceedings of The Third International Workshop on Cyber-Physical Networking Systems*, Philadelphia, PA, July 11-13.

Some of Our Publications on the NSF Project

[7] Wolf, T., Griffioen, J., Calvert, K., Dutta, R., Rouskas, G., Baldine, I., Nagurney, A., 2014. ChoiceNet: Toward an Economy Plane for the Internet. *ACM SIGCOMM Computer Communication Review* 44(3), 58-65.

[8] Nagurney, A., Li, D., Saberi, S., Wolf T., 2014. A Dynamic Network Economic Model of a Service-Oriented Internet with Price and Quality Competition. In *Network Models in Economics and Finance*, V. A. Kalyagin, P. M. Pardalos, and T. M. Rassias, Editors, Springer International Publishing Switzerland (2014) pp 239-264.

[9] Nagurney, A., Li, D., 2014. Equilibria and Dynamics of Supply Chain Network Competition with Information Asymmetry in Quality and Minimum Quality Standards. *Computational Management Science* 11(3), 285-315.

Summary and Conclusions

- In this presentation, we overviewed our work on network vulnerability from a cybersecurity perspective from both a system and a cybercrime perspective. Our "clients" were financial service firms, who have also encountered a growing number of cyberattacks.

Summary and Conclusions

• In this presentation, we overviewed our work on network vulnerability from a cybersecurity perspective from both a system and a cybercrime perspective. Our "clients" were financial service firms, who have also encountered a growing number of cyberattacks.

• We gave some background on game theory and also discussed cybersecurity investment models at a high level.

Summary and Conclusions

• In this presentation, we overviewed our work on network vulnerability from a cybersecurity perspective from both a system and a cybercrime perspective. Our "clients" were financial service firms, who have also encountered a growing number of cyberattacks.

• We gave some background on game theory and also discussed cybersecurity investment models at a high level.

• We provided an overview of our work on a Future Internet Architecture, known as ChoiceNet, which may provide not only greater flexibility for innovation but also added security in terms of verification and authentication.

Summary and Conclusions

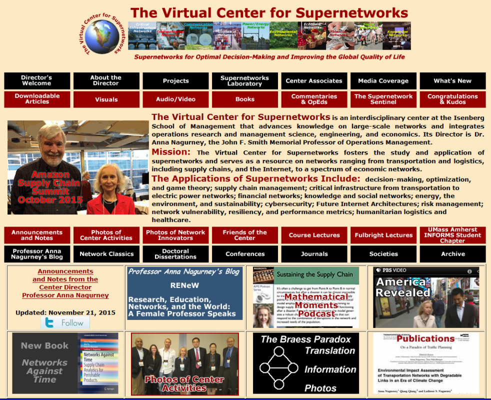
• In this presentation, we overviewed our work on network vulnerability from a cybersecurity perspective from both a system and a cybercrime perspective. Our "clients" were financial service firms, who have also encountered a growing number of cyberattacks.

• We gave some background on game theory and also discussed cybersecurity investment models at a high level.

• We provided an overview of our work on a Future Internet Architecture, known as ChoiceNet, which may provide not only greater flexibility for innovation but also added security in terms of verification and authentication.

• Our research integrates inputs from practitioners with the goal of providing prescriptive analytics for decision-making.

THANK YOU!



For reference materials, see: http://supernet.isenberg.umass.edu