Game Theory and Variational Inequalities: From Transportation and Supply Chains to Financial Networks and the Internet

Professor Anna Nagurney

Eugene M. Isenberg Chair in Integrative Studies
Director – Virtual Center for Supernetworks
Isenberg School of Management, University of Massachusetts Amherst

4th ACM International Critical Infrastructure Network Security (CINS) Workshop at ACM Sigmetrics, June 14, 2021

ISENBERG
UMASS AMHERST

Acknowledgments

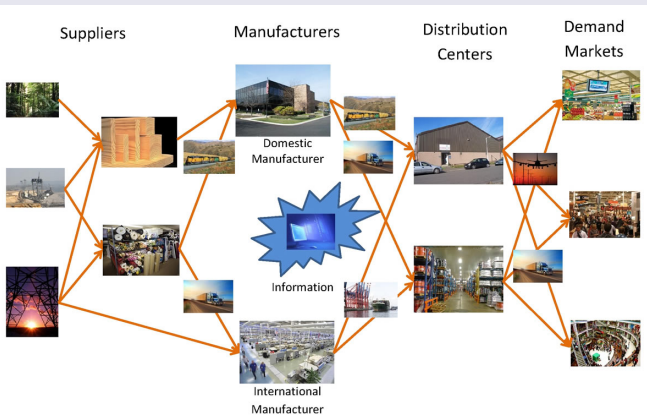
Many thanks to the Organizers - Professors Sergiy Butenko and Pavlo Krokhmal – for the invitation to speak to you today at this very interesting workshop!

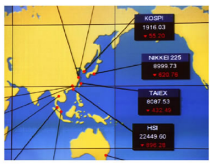
Outline of Presentation

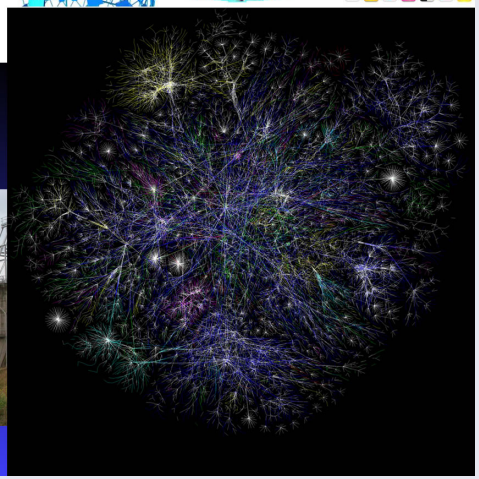
- Motivation Including Transportation Networks
- Variational Inequality Fundamentals
- A Multidisciplinary Approach to Supply Chain Networks
- A Supply Chain Game Theory Model with Labor Inspired by the COVID-19 Pandemic
- Cybercrime
- Which Nodes and Links Really Matter?
- A Predictive Network Economic Model of Cybercrime
- Cybersecurity Investments
- A Retail Case Study
- Envisioning a New Kind of Internet – ChoiceNet
- Summary

Motivation Including Transportation Networks

I Work on the Modeling of Network Systems



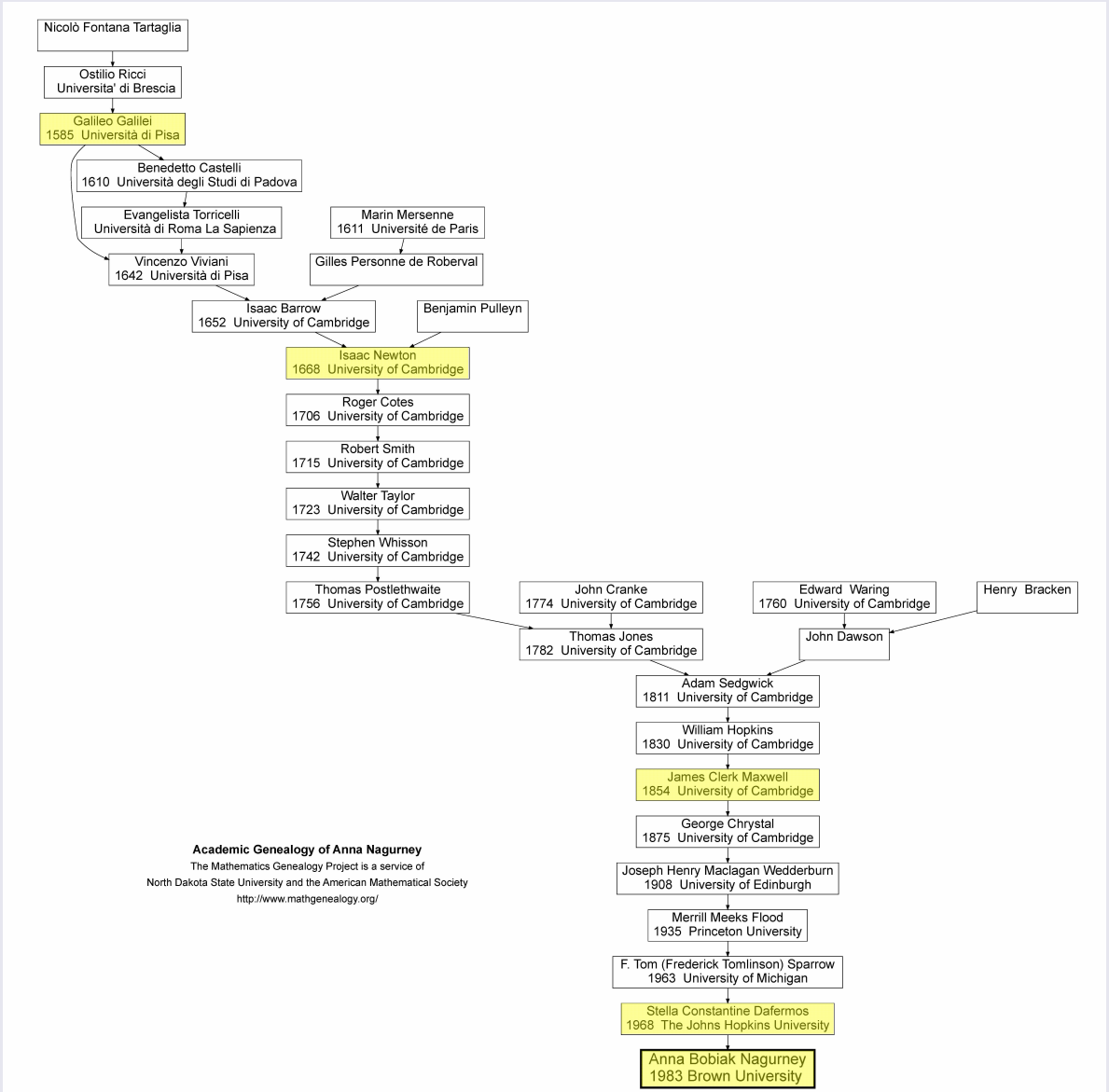




Much of My Recent Research Has Been on Supply Chains

Some of My Books

On the Shoulders of Giants - Academic Genealogy



Professor Stella Dafermos

Dr. Stella Dafermos was the only female professor in either Engineering or Applied Mathematics at Brown University, when I became her first PhD student.

EQUILIBRIUM MODELING, ANALYSIS AND COMPUTATION: THE CONTRIBUTIONS OF STELLA DAFERMOS

ANNA NAGURNEY
University of Massachusetts, Amherst, Massachusetts
(Received June 1990; accepted August 1990)

This memorial tribute to the late Stella Dafermos summarizes her contributions to equilibrium modeling, analysis, and computation, and provides a list of her published papers.

On April 5, 1990, with the death at 49 of Stella Dafermos, Professor of Applied Mathematics and Engineering at Brown University, Providence, Rhode Island, the operations research community lost one of its early woman doctorates. Throughout her quarter-century career she dedicated herself to developing rigorous mathematical formalisms for modeling, analyzing and making computations related to competitive equilibrium systems that spanned applications from congested urban transportation networks to multicommodity trade. Beginning with her 1968 doctoral dissertation, "Traffic Assignment and Resource Allocation in Transportation Networks," directed by F. T. Sparrow at Johns Hopkins University, which focused on the study of system-optimized and user-optimized transportation networks, she initiated a theme of advancement of methodologies by which the behavior of complex systems could be captured and studied.

EQUILIBRIUM MODELING

In her first paper, based on her thesis and published in 1969, she proposed convergent equilibration algorithms that simulated the adjustment behavior of travelers on a congested network operating in their own self-interest in choosing their routes. The governing equilibrium conditions, due to Wardrop, reflected that only the minimum cost routes connecting each origin/destination pair would be used. These algorithms took advantage of the problem structure and were later extended in papers published in 1971 and 1972 to network models that allowed for interaction among users of the system via the link cost functions. In her 1969 paper she also focused on stability issues, which began the theme of qualitative analysis of equilibrium patterns that was also to pervade her scholarly work.

These network equilibrium models, as well as the integrated models that allowed for both location and route choice, developed in her paper of 1976, were formulated as optimization problems, with the observation that the equilibrium conditions governing these problems were actually the Kuhn-Tucker conditions of an appropriately constructed optimization problem. Interestingly, parallel to these developments in nonlinear networks, the economics community was reformulating spatial price equilibrium problems, in which commodities are produced, consumed and traded, subject to transportation or transaction costs, as optimization problems. However, the assumption required for such a transformation—that of *symmetry*, in which cross-effects of various interactions had to be identical—precluded the realistic modeling of multiple modes of transportation and different classes of users of a given system, as well as multiple commodities. Moreover, the objective function thus constructed, although convenient and essential given the state-of-the-art at the time, was artificial. Furthermore, equilibrium problems, by their very nature, involve more than a single agent and objective function, with interactions among the agents, and, hence, the objective functions being the rule rather than the exception. To overcome such shortcomings, a methodological advance was needed.

In 1980 Stella made a fundamental discovery by observing that the equilibrium conditions of the traffic assignment problem actually had the structure of a variational inequality problem. Although the theory of variational inequalities had been introduced over a decade earlier for the study of partial differential equations, the emphasis there was on infinite-dimensional problems arising in mechanics, and its use as a powerful tool for equilibrium analysis in operations research was left unrealized. Stella's identification of network equilibrium conditions with a variational inequality problem opened up new horizons for mathematical modeling, analysis and the efficient computation of more general equilibrium systems than had heretofore been possible. With this

Subject classifications: Economics: solution of equilibrium problems. Networks/graphs: equilibrium modeling and computation. Transportation: formulation and solution of multimodal problems.

0030-364X/91/3901-0008 $01.25

Stella was the second female to have received a PhD in Operations Research in the US and that was from Johns Hopkins University.

Characteristics of Many Networks Today

- **large-scale nature** and complexity of network topology;
- **congestion**, which leads to nonlinearities;
- **alternative behavior of users of the networks**, which may lead to paradoxical phenomena;
- **possibly conflicting criteria associated with optimization**;
- **interactions among the underlying networks themselves**, such as the Internet with electric power networks, financial networks, and transportation and logistical networks;
- recognition of **their fragility and vulnerability**;
- policies surrounding networks today may have major impacts not only economically, but also **socially, politically, and security-wise**.

In this talk, I will be covering a variety of **nonlinear network flow problems**. The concept of *network equilibrium* owes much to **the study of congested transportation networks**, so we will begin with this topic, since this area of application has also driven many methodological advances, including advances in variational inequality theory.

Interestingly, the topic of congestion and its management was even a major issue in Roman times.

The Study of Congested Transportation Networks Must Capture the Behavior of Users

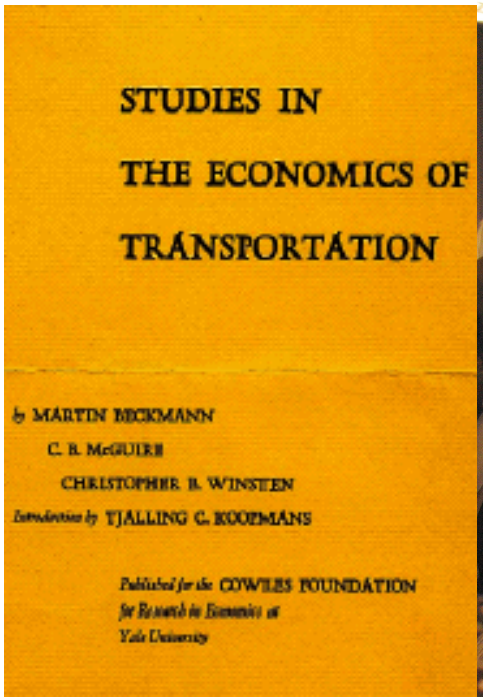
Two fundamental principles of travel behavior, due to Wardrop (1952), with terms coined by Dafermos and Sparrow (1969).

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, possess optimization reformulations. **But now we can handle cost asymmetries, multiple modes of transport, and different classes of travelers, without such assumptions, because of variational inequality theory.**

First Rigorous Formulation of U-O (Decentralized) and S-O (Centralized) Behavior



In 1956, Yale University Press published *Studies in the Economics of Transportation* **by Beckmann, McGuire, and Winsten. in 2005, we celebrated the 50th anniversary of its publication at the 2005 INFORMS Meeting, San Francisco. Professor Nagurney with Professors Beckmann, McGuire, and many others!**

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 $p \in P_w$:

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

The S-O Conditions

Definition: S-O Conditions

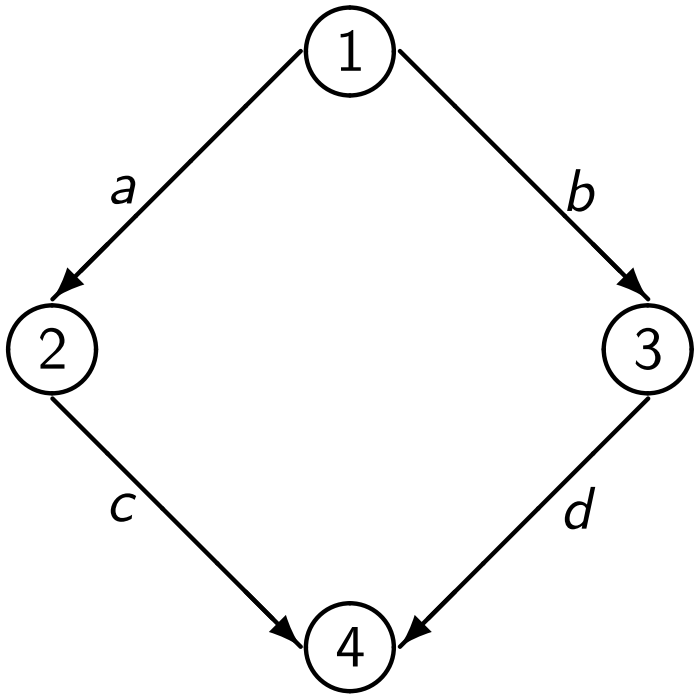
A path flow pattern x with nonnegative path flows and O/D pair demand satisfaction, is said to be S-O, if for each O/D pair $w \in W$ and each path $p \in P_w$:

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

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.

Importance of Capturing Behavior on Networks - The Braess (1968) Paradox and User-Optimizing (U-O) Behavior

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

$C_{p_1} = C_{p_2} = 83.$

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

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

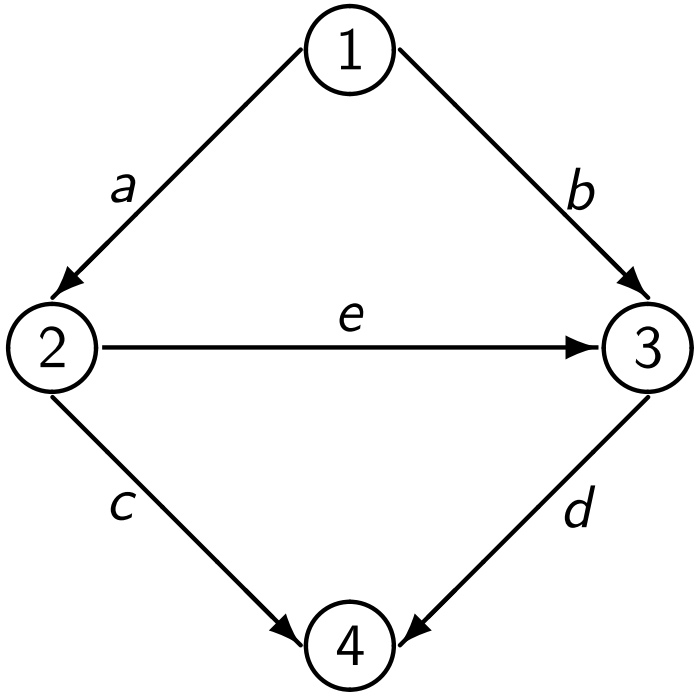
Adding a Link Increases Travel Cost for All!

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: "On a Paradox of Traffic Planning," D. Braess, A. Nagurney, and T. 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.

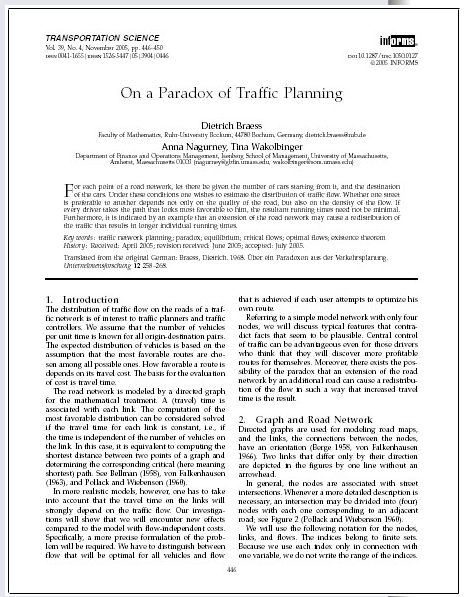
1. Einleitung

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
Vol. 39, No. 4, November 2005, pp. 446–450
issn 0041-1655 | eissn 1526-5447 | 05 | 3904 | 0446

informs
doi 10.1287/trsc.1050.0127
© 2005 INFORMS

On a Paradox of Traffic Planning

Dietrich Braess
Faculty of Mathematics, Ruhr-University Bochum, 44780 Bochum, Germany, dietrich.braess@ruhr.de
Anna Nagurney, Tina Wakolbinger
Department of Finance and Operations Management, Isenberg School of Management, University of Massachusetts, Amherst, Massachusetts 01003 {nagurney@gbfin.umass.edu, wakolbin@gbfinsun.umass.edu}

For each point of a road network, let there 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 traffic flow. Whether one street is preferable to another depends not only on the quality of the road, but also on the density of the flow. If every driver takes the path that 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 that results in longer individual running times.

Key words: traffic network planning; paradox; equilibrium; critical flows; optimal flows; existence theorem
History: Received: April 2005; revision received: June 2005; accepted: July 2005.

Translated from the original German: Braess, Dietrich. 1968. Über ein Paradoxon aus der Verkehrsplanung. *Unternehmensforschung* **12** 258–268.

1. Introduction

The distribution of traffic flow on the roads of a traffic network is of interest to traffic planners and traffic controllers. We assume that the number of vehicles per unit time is known for all origin-destination pairs. The expected distribution of vehicles is based on the assumption that the most favorable routes are chosen among all possible ones. How favorable a route is depends on its travel cost. The basis for the evaluation of cost is travel time.

The road network is modeled by a directed graph for the mathematical treatment. A (travel) time is associated with each link. The computation of the most favorable distribution can be considered solved if the travel time for each link is constant, i.e., if the time is independent of the number of vehicles on the link. In this case, it is equivalent to computing the shortest distance between two points of a graph and determining the corresponding critical flows meaning shortest) path. See Bellman (1958), von Falkenhausen (1963), and Pollack and Wiebenson (1960).

In more realistic models, however, one has to take into account that the travel time on the links will strongly depend on the traffic flow. Our investigations will show that we will encounter new effects compared to the model with flow-independent costs. Specifically, a more precise formulation of the problem will be required. We have to distinguish between flow that will be optimal for all vehicles and flow that is achieved if each user attempts to optimize his own route.

Referring to a simple model network with only four nodes, we will discuss typical features that contradict facts that seem to be plausible. Central control of traffic can be advantageous even for those drivers who think that they will discover more profitable routes for themselves. Moreover, there exists the possibility of the paradox that an extension of the road network by an additional road can cause a redistribution of the flow in such a way that increased travel time is the result.

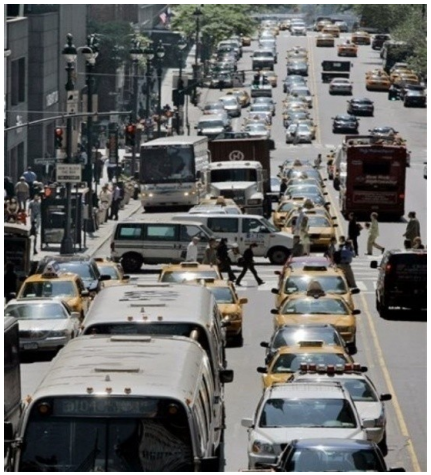
2. Graph and Road Network

Directed graphs are used for modeling road maps, and the links, the connections between the nodes, have an orientation (Berge 1958, von Falkenhausen 1964). Two links that differ only by their direction are depicted in the figures by one line without an arrowhead.

In general, the nodes are associated with street intersections. Whenever a more detailed description is necessary, an intersection may be divided into (four) nodes with each one corresponding to an adjacent road; see Figure 2 (Pollack and Wiebenson 1960).

We will use the following notation for the nodes, links, and flows. The indices belong to finite sets. Because we use each index only in connection with one variable, we do not write the range of the indices.

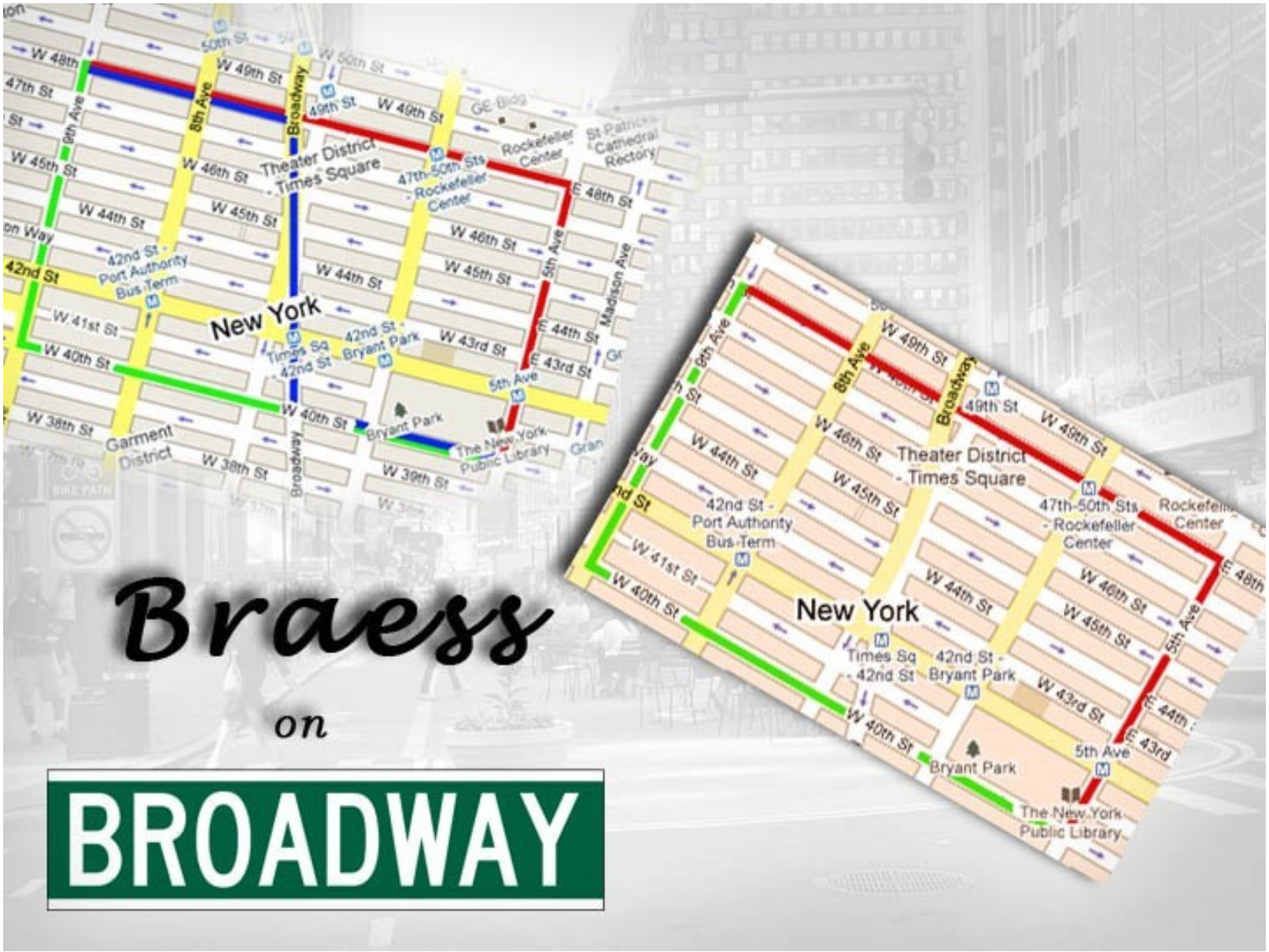
The Braess Paradox Around the World



1969 - Stuttgart, Germany - The traffic worsened until a newly built road was closed.

1990 - Earth Day - New York City - 42^{nd} Street was closed and traffic flow improved.

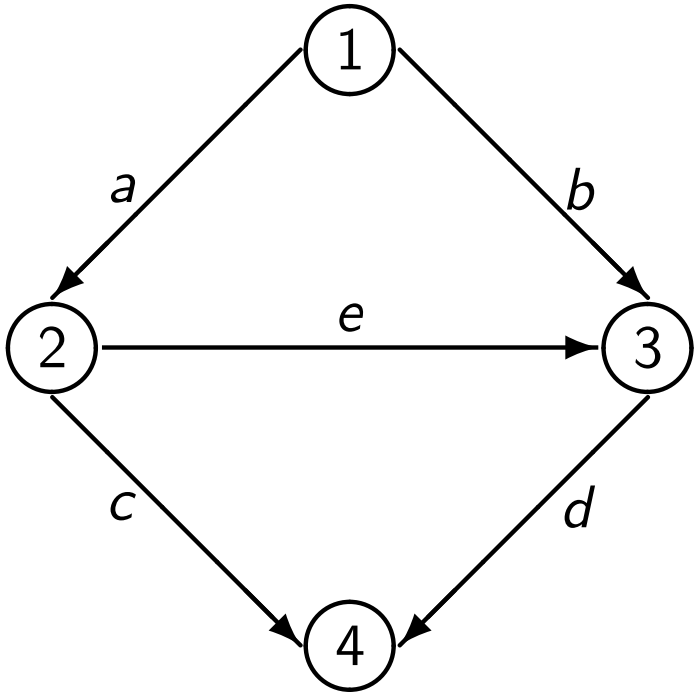
2002 - Seoul, Korea - A 6 lane road built over the Cheonggyecheon River that carried 160,000 cars per day and was perpetually jammed was torn down to improve traffic flow.


Braess
on
BROADWAY
New York
Theater District
- Times Square
42nd St -
Port Authority
Bus Term
47th-50th Sts
- Rockefeller
Center
Rockefeller
Center
Times Sq
- 42nd St
42nd St -
Bryant Park
Bryant Park
The New York
Public Library
Garment
District
5th Ave
6th Ave
8th Ave
Broadway
Madison Ave
W 49th St
W 48th St
W 47th St
W 46th St
W 45th St
W 44th St
W 43rd St
W 41st St
W 40th St
W 39th St
W 38th St
E 48th St
E 44th St
E 43rd St

Interview on Broadway for *America Revealed* on March 15, 2011

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.

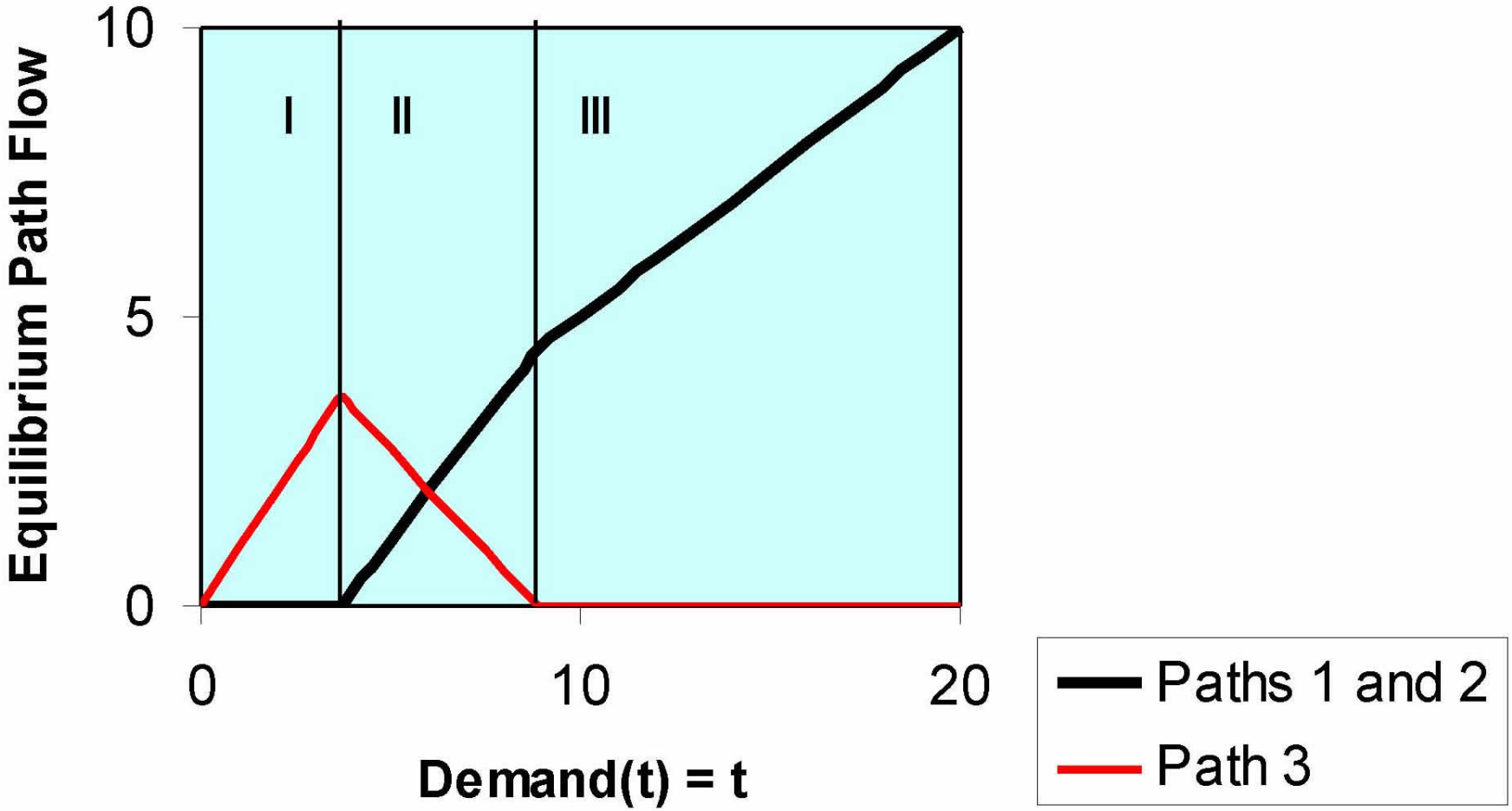
The Braess paradox never occurs in S-O networks.



Recall the Braess network with the added link e.

What happens as the demand changes?

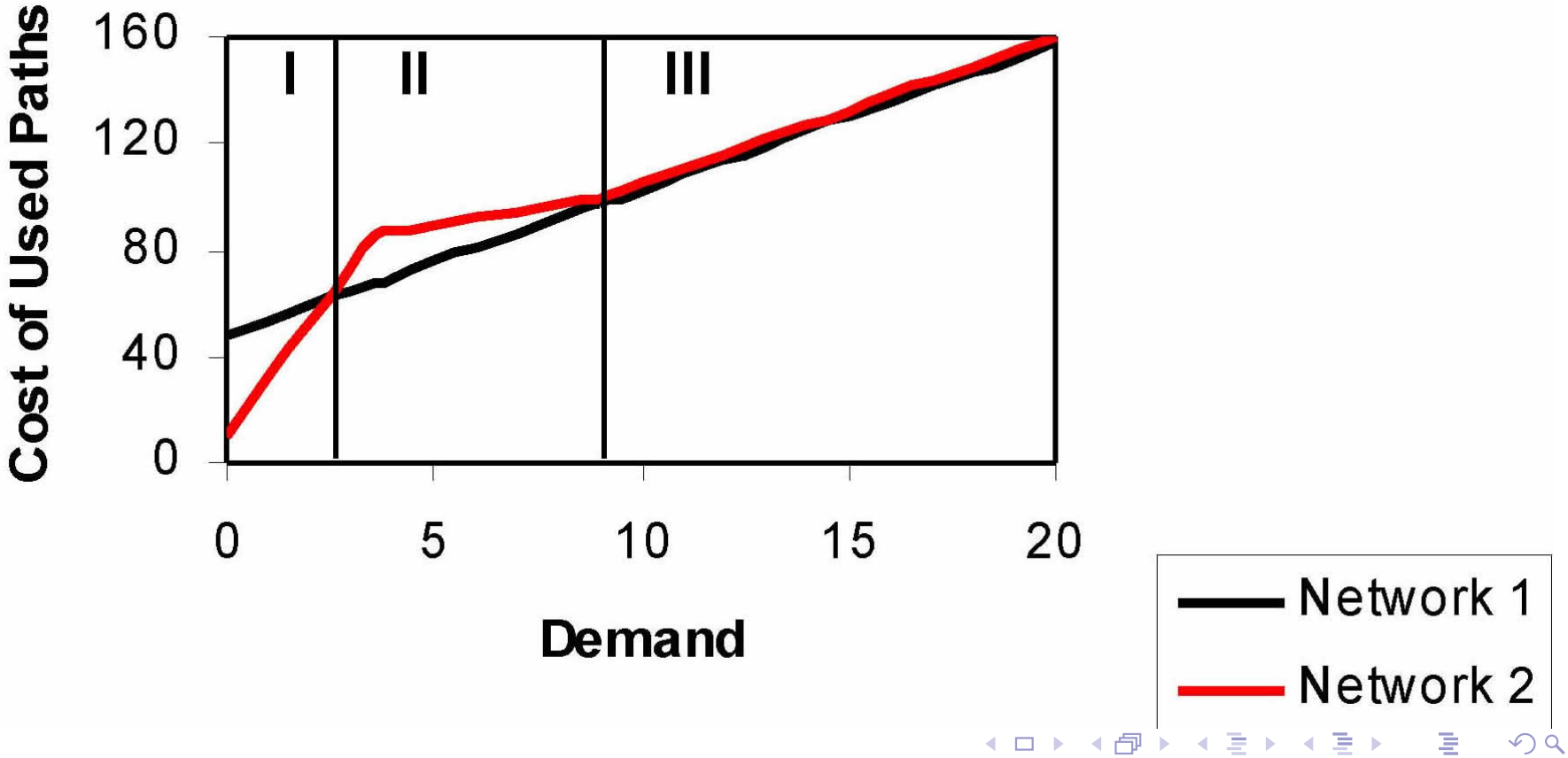
The U-O Solution of the Braess Network with Added Link (Path) and Time-Varying Demands Solved as an *Evolutionary Variational Inequality* (A. Nagurney, P. Daniele, and D. Parkes, *Computational Management Science* **4** (2007), pp 355-375).



In Demand Regime I, **Only the New Path is Used**.

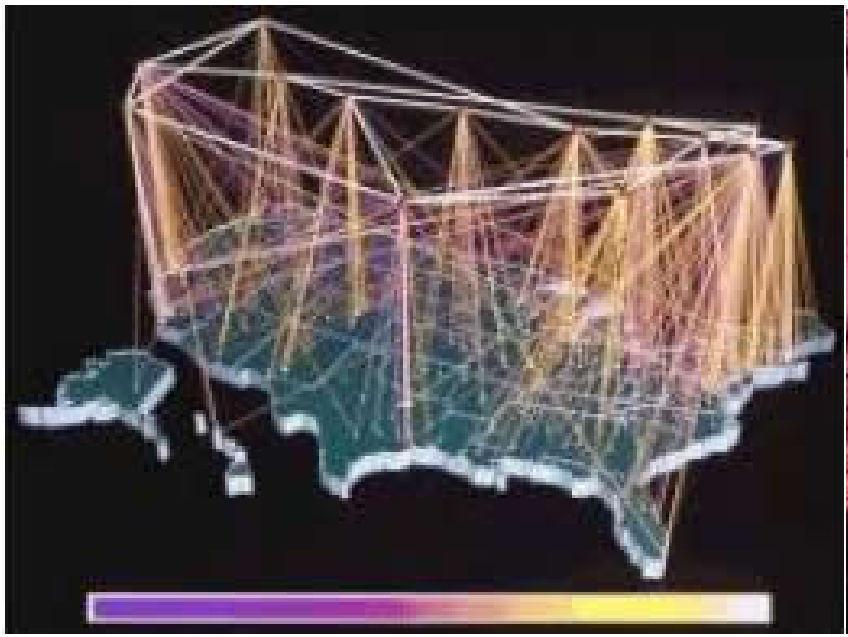
In Demand Regime II, the travel demand lies in the range [2.58, 8.89], and **the Addition of a New Link (Path) Makes Everyone Worse Off**!

In Demand Regime III, when the travel demand exceeds 8.89, **Only the Original Paths are Used!**



The new path is never used, under U-O behavior, when the demand exceeds 8.89, even when the demand goes out to infinity!

Other Networks that Behave like Traffic Networks



The Internet and electric power networks and even supply chains!

Variational Inequality Fundamentals

Variational Inequalities

Dafermos (1980) identified that the traffic network equilibrium conditions, as formulated by Smith (1979)), were a VI problem. This unveiled the theory for the formulation, analysis, and computation of solutions to numerous equilibrium problems in OR, economics, engineering, and other disciplines.

The paper, available for free download, S. Dafermos (1980), "Traffic Equilibrium and Variational Inequalities," *Transportation Science* **14(1)**, pp 42-54,

was selected by the Editors as one of the 12 most impactful in 50 years!

Background

To-date, problems which have been formulated and studied as variational inequality problems include:

- traffic network equilibrium problems
- spatial price equilibrium problems
- oligopolistic market equilibrium problems
- financial equilibrium problems
- migration equilibrium problems, as well as
- environmental network and ecology problems,
- knowledge network problems,
- electric power generation and distribution networks,
- supply chain network equilibrium problems, and even
- the Internet!

Variational Inequality Theory

Variational inequality (VI) theory provides us with a tool for:

- formulating a variety of equilibrium problems;
- qualitatively analyzing the problems in terms of existence and uniqueness of solutions, stability and sensitivity analysis, and
- providing us with algorithms with accompanying convergence analysis for computational purposes.

It contains, as special cases, such well-known problems in mathematical programming as: systems of nonlinear equations, optimization problems, complementarity problems, and is also related to fixed point problems.

Definition: Variational Inequality Problem

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

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

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, as does "·".*

Here we assume that all vectors are column vectors, except where noted.

The Variational Inequality Problem

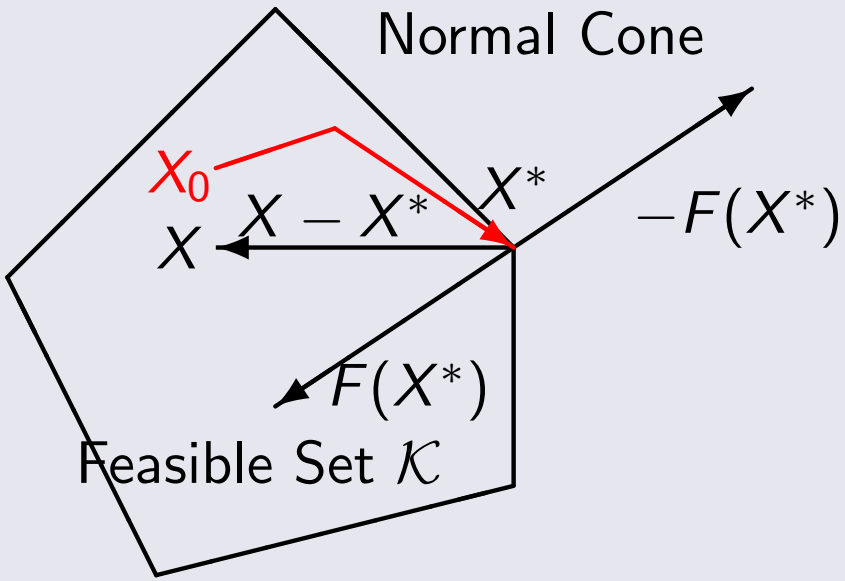
Another equivalent way of writing (1) is:

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

$\mathcal{K}$ is the feasible set, X^* is the vector of solution values of the variables, and F is sometimes referred to as the function that enters the variational inequality.

Geometric Interpretation of VI($F, \mathcal{K}$) and a Projected Dynamical System

As shown by Dupuis and Nagurney (1993), there is associated with a VI problem, a *projected dynamical system*, which provides a natural underlying dynamics until an equilibrium state is achieved, under appropriate conditions. In particular, $F(X^*)$ is "orthogonal" to the feasible set $\mathcal{K}$ at the point X^*.



To model the **dynamic behavior of complex network systems**, including supply chains, we utilize *projected dynamical systems* (PDSs) advanced by Dupuis and Nagurney (1993) in the *Annals of Operations Research* and by Nagurney and Zhang (1996) in our book *Projected Dynamical Systems and Variational Inequalities with Applications*.

Such nonclassical dynamical systems are now being used in:

- **evolutionary games** (Sandholm (2005, 2011)),
- **ecological predator-prey networks** (Nagurney and Nagurney (2011a, b)),
- even **neuroscience** (Girard et al. (2008),
- **dynamic spectrum model for cognitive radio networks** (Setoodeh, Haykin, and Moghadam (2012)),
- **Future Internet Architectures** (Saberi, Nagurney, and Wolf (2014); see also Nagurney et al. (2015)).

Variational Inequality Formulations of Traffic Network Equilibrium

Theorem: Path Flow Formulation

A vector of path flows $x^* \in K^1$, where $K^1 \equiv \{x | x \geq 0, \text{ and } \sum_{p \in P_w} x_p = d_w, \forall w\}$ is a Traffic Network Equilibrium (U-O pattern) if and only if it satisfies the VI problem:

$$\sum_w \sum_{p \in P_w} C_p(x^*) \times (x_p - x_p^*) \geq 0, \quad \forall x \in K^1.$$

Variational Inequality Formulations of Traffic Network Equilibrium

Theorem: Link Flow Formulation

A vector of link flows $f^* \in K^2$, where $K^2 \equiv \{\exists x | x \geq 0$, and $\sum_{p \in P_w} x_p = d_w, \forall w, f_a = \sum_{p \in P} x_p \delta_{ap}, \forall a\}$ is a Traffic Network Equilibrium (U-O pattern) if and only if it satisfies the VI problem:

$$\sum_{a \in L} c_a(f^*) \times (f_a - f_a^*) \geq 0, \quad \forall f \in K^2.$$

Nash Equilibrium and Game Theory

Nash (1950, 1951) subsequently generalized Cournot's concept of an equilibrium for a behavioral model consisting of n agents or players, each acting in his/her own self-interest, which has come to be called a noncooperative game.

The Nobel Laureate John F. Nash

www.search.tvnz.co.nz

Specifically, consider m players, each player i having at his/her disposal a strategy vector $X_i = \{X_{i1}, \ldots, X_{in}\}$ selected from a closed, convex set $K_i \subset R^n$, with a utility function $U_i : K \mapsto R^1$, where $K = K_1 \times K_2 \times \ldots \times K_m \subset R^{mn}$.

Rationality Postulate

The rationality postulate is that each player i selects a strategy vector $X_i \in K_i$ that maximizes his/her utility level $U_i(X_1, \ldots, X_{i-1}, X_i, X_{i+1}, \ldots, X_m)$ given the decisions $(X_j)_{j \neq i}$ of the other players.

In this framework one then has:

Definition: Nash Equilibrium

A Nash equilibrium is a strategy vector

$$X^* = (X_1^*, \ldots, X_m^*) \in K,$$

such that

$$U_i(X_i^*, \hat{X}_i^*) \geq U_i(X_i, \hat{X}_i^*), \quad \forall X_i \in K_i, \forall i,$$

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

Variational Inequality Formulation of Nash Equilibrium

It has been shown (cf. Hartman and Stampacchia (1966) and Gabay and Moulin (1980)) that Nash equilibria satisfy variational inequalities. In the present context, under the assumption that each U_i is continuously differentiable on K and concave with respect to X_i, one has

Theorem: Variational Inequality Formulation of Nash Equilibrium

Under the previous assumptions, X^* is a Nash equilibrium if and only if $X^* \in K$ is a solution of the variational inequality

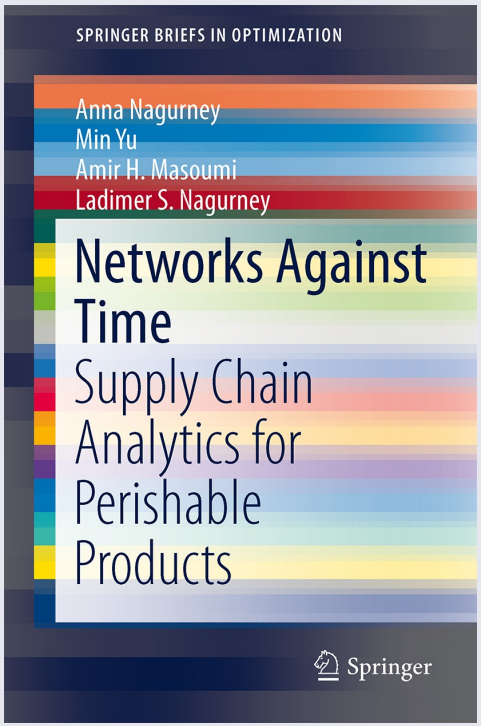
$$\langle F(X^*), X - X^* \rangle \geq 0, \quad \forall X \in K,$$

where $F(X) \equiv (-\nabla_{X_1} U_1(X), \ldots, -\nabla_{X_m} U_m(X))$ is a row vector and where $\nabla_{X_i} U_i(X) = (\frac{\partial U_i(X)}{\partial X_{i1}}, \ldots, \frac{\partial U_i(X)}{\partial X_{in}})$.

A Multidisciplinary Approach to Supply Chain Networks

A Multidisciplinary Approach

In our research on perishable and time-sensitive product supply chains, we utilize results from physics, chemistry, biology, and medicine in order to capture the perishability of various products over time from healthcare products such as blood, medical nucleotides, and pharmaceuticals to food.



Food Supply Chains

Food is essential to our health and well-being. During the Covid-19 pandemic, declared on March 11, 2020 by the World Health Organization, the associated supply chains have suffered major disruptions.

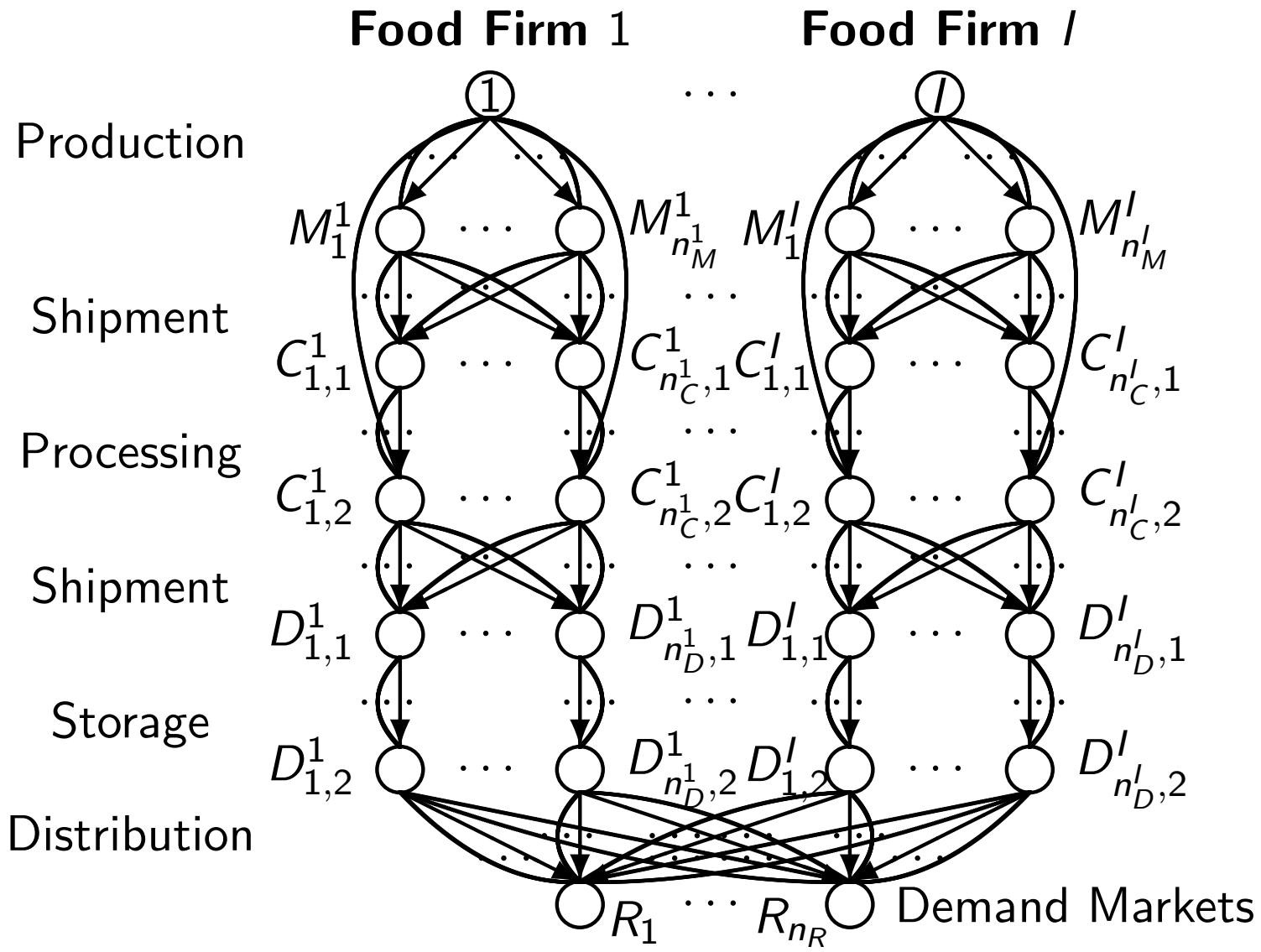
Fresh Produce Food Supply Chains

Our fresh produce supply chain network oligopoly model:

1. captures the deterioration of fresh food along the entire supply chain from a network perspective;
2. handles the time decay through the introduction of arc multipliers;
3. formulates oligopolistic competition with product differentiation;
4. includes the disposal of the spoiled food products, along with the associated costs;
5. allows for the assessment of alternative technologies involved in each supply chain activity.

M. Yu and A. Nagurney, "Competitive Food Supply Chain Networks with Application to Fresh Produce," *European Journal of Operational Research* **224(2) (2013), pp 273-282.**

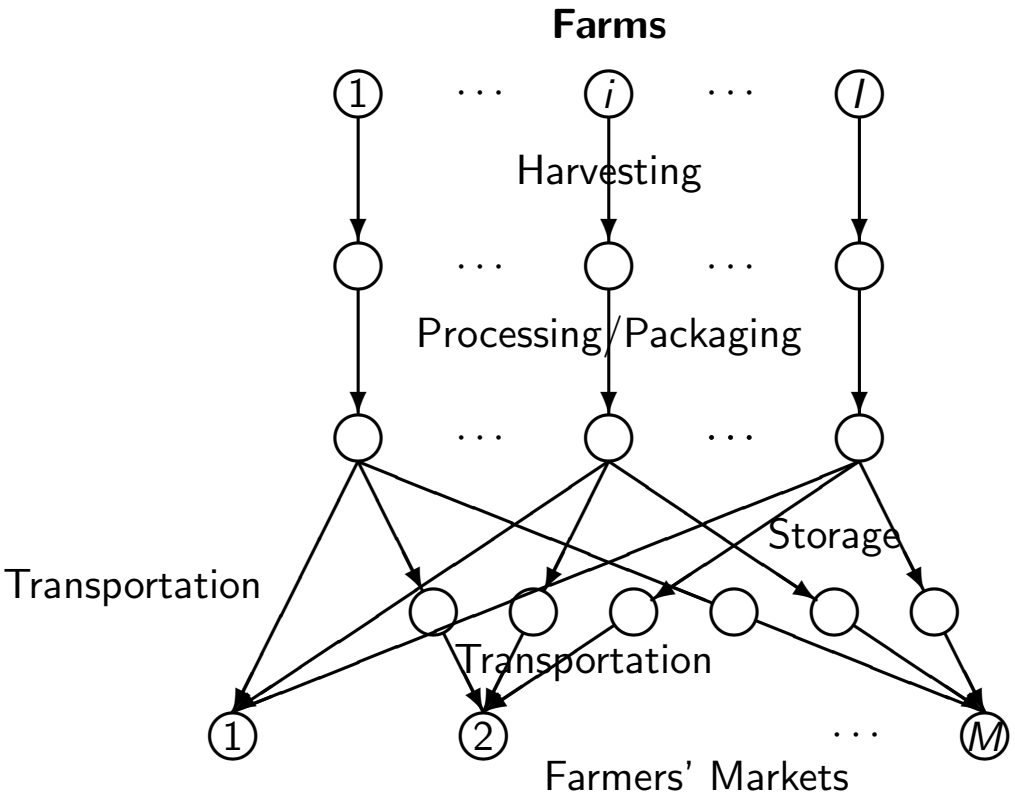
Fresh Produce Food Supply Chains

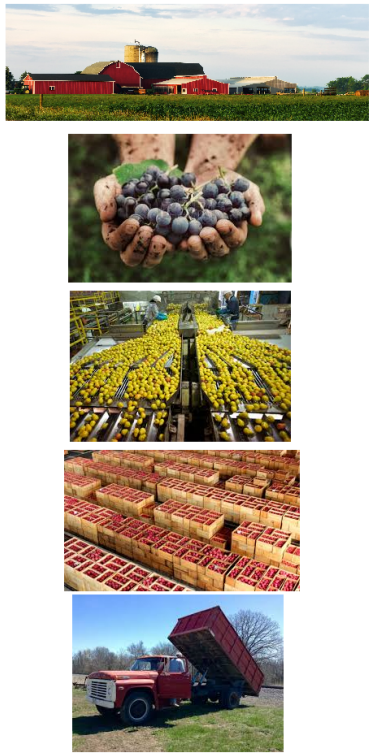


The Fresh Produce Supply Chain Network Topology

Farmers' Markets and Fresh Produce Supply Chains

- The I farms compete **noncooperatively** in an **oligopolistic** manner.
- Products are differentiated based on **quality** at the farmers' markets.





D. Besik and A. Nagurney, "Quality in Competitive Fresh Produce Supply Chains with Application to Farmers' Markets," *Socio-Economic Planning Sciences* **60 (2017), pp 62-76.**

Pharmaceutical Supply Chains

The supply chain generalized network oligopoly model has the following novel features:

1. it handles the perishability of the pharmaceutical product through the introduction of arc multipliers;
2. it allows each firm to minimize the discarding cost of waste / perished medicine;
3. it captures product differentiation under oligopolistic competition through the branding of drugs, which can also include generics as distinct brands.

A.H. Masoumi, M. Yu, and A. Nagurney, "A Supply Chain Generalized Network Oligopoly Model for Pharmaceuticals Under Brand Differentiation and Perishability," *Transportation Research E* **48 (2012), pp 762-780.**

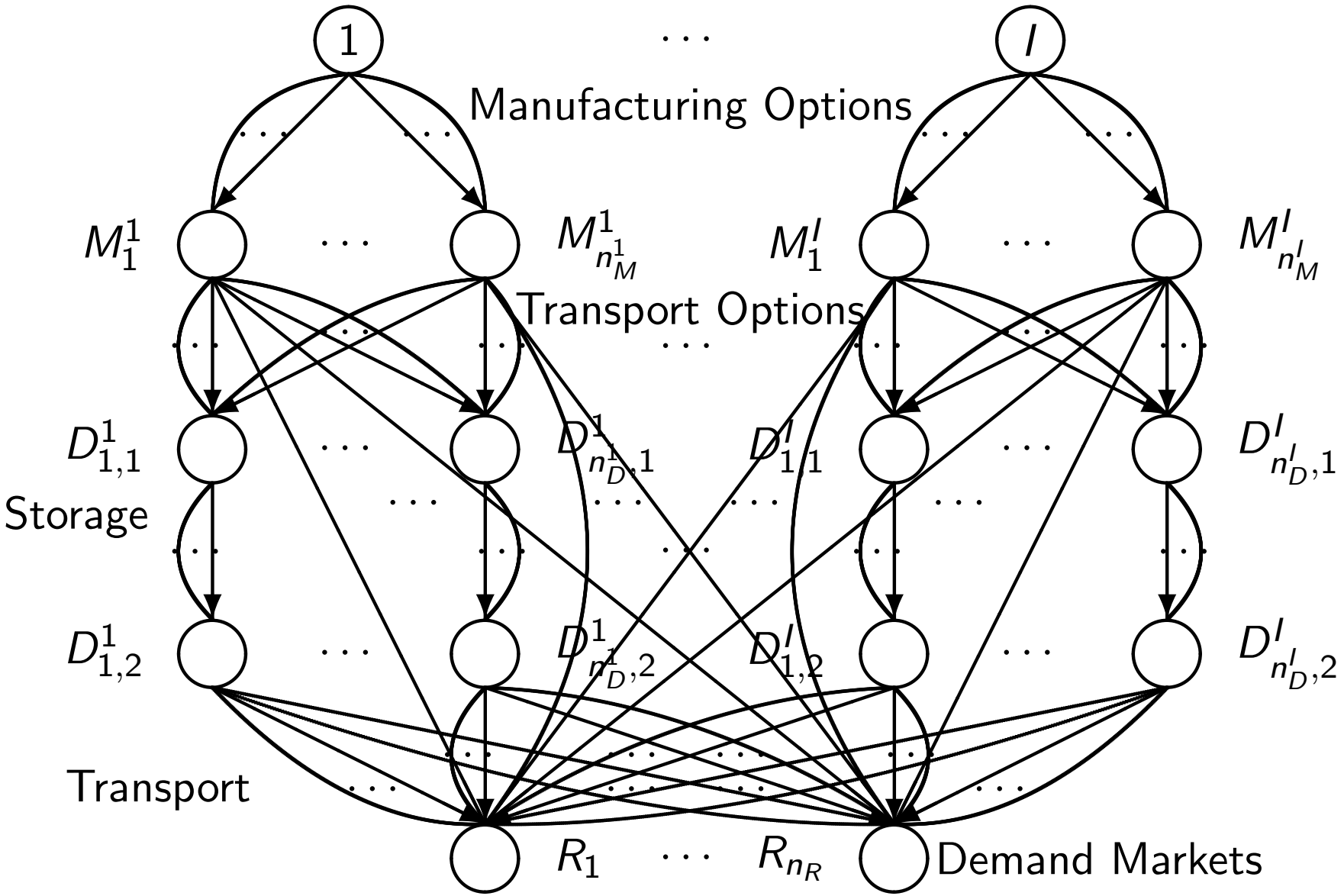


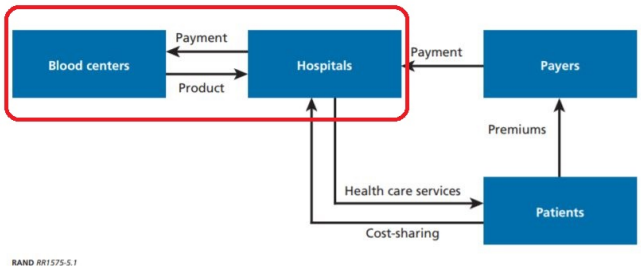
Figure: The Pharmaceutical Supply Chain Network Topology

Blood Supply Chains

Even prior to the pandemic the blood services sector was facing many challenges. This supply chain is unique in that the product cannot be produced but must be donated.

A. Nagurney and P. Dutta, "Supply Chain Network Competition Among Blood Service Organizations: A Generalized Nash Equilibrium Framework," *Annals of Operations Research* **275(2) (2019), pp 551-586.**

Operational challenges faced by blood service organizations.



A. Nagurney and P. Dutta, "Competition for Blood Donations," *Omega* **212 (2019), pp 103-114.**

A Supply Chain Game Theory Model with Labor Inspired by the COVID-19 Pandemic

Game Theory Supply Chain Network Model with Labor

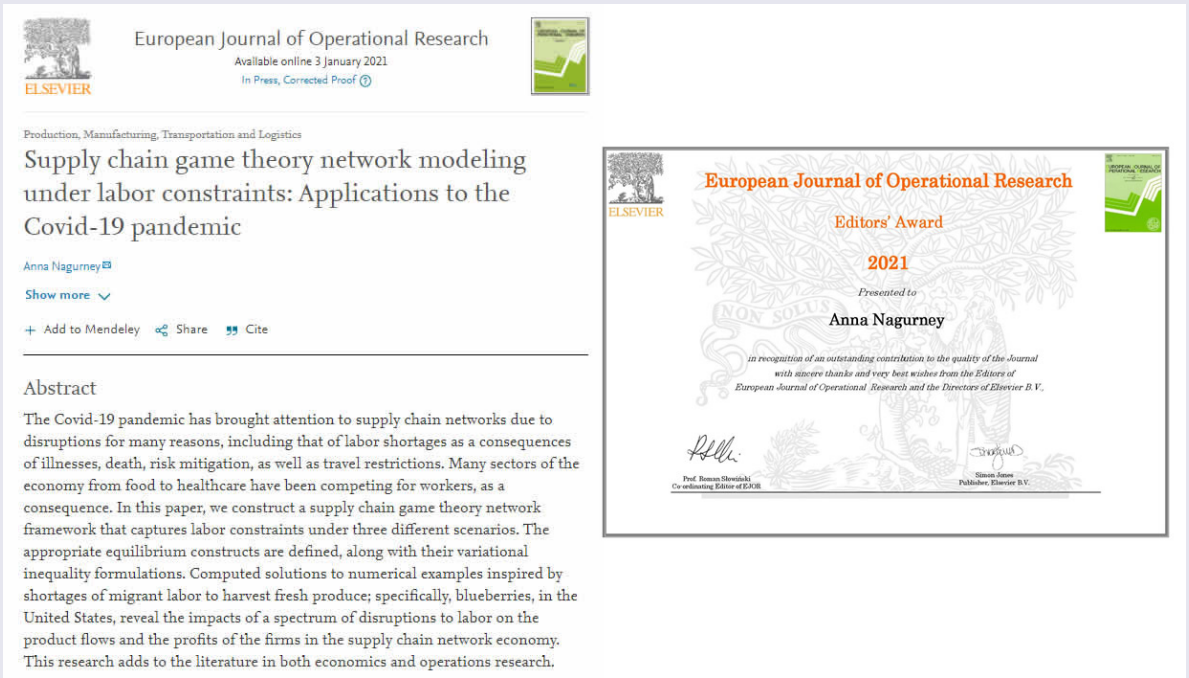
The Covid-10 pandemic has dramatically illustrated the importance of including labor (and associated possible disruptions) into the analysis of supply chain networks.

In addition, the pandemic has, in such essential sectors as food and healthcare, demonstrated the competition for labor resources!

In the paper, **"Supply Chain Game Theory Network Modeling Under Labor Constraints: Applications to the Covid-19 Pandemic," A. Nagurney,** *European Journal of Operational Research* **293(3) (2021), pp 880-891**, a game theory model for supply chains with labor was constructed, under three different sets of constraints, building on our previous work.

Game Theory Supply Chain Network Model with Labor

In the paper, we present a series of numerical examples documenting the potential impacts of labor disruptions under different scenarios.



European Journal of Operational Research

Available online 3 January 2021

In Press, Corrected Proof

Production, Manufacturing, Transportation and Logistics

Supply chain game theory network modeling under labor constraints: Applications to the Covid-19 pandemic

Anna Nagurney

Show more

+ Add to Mendeley Share Cite

Abstract

The Covid-19 pandemic has brought attention to supply chain networks due to disruptions for many reasons, including that of labor shortages as a consequences of illnesses, death, risk mitigation, as well as travel restrictions. Many sectors of the economy from food to healthcare have been competing for workers, as a consequence. In this paper, we construct a supply chain game theory network framework that captures labor constraints under three different scenarios. The appropriate equilibrium constructs are defined, along with their variational inequality formulations. Computed solutions to numerical examples inspired by shortages of migrant labor to harvest fresh produce; specifically, blueberries, in the United States, reveal the impacts of a spectrum of disruptions to labor on the product flows and the profits of the firms in the supply chain network economy. This research adds to the literature in both economics and operations research.

European Journal of Operational Research

Editors' Award

2021

Presented to

Anna Nagurney

in recognition of an outstanding contribution to the quality of the Journal with sincere thanks and very best wishes from the Editors of European Journal of Operational Research and the Directors of Elsevier B.V.

Prof. Roman Slowinski
Co-ordinating Editor of EJOR

Simon Jones
Publisher, Elsevier B.V.

Game Theory Supply Chain Network Model with Labor

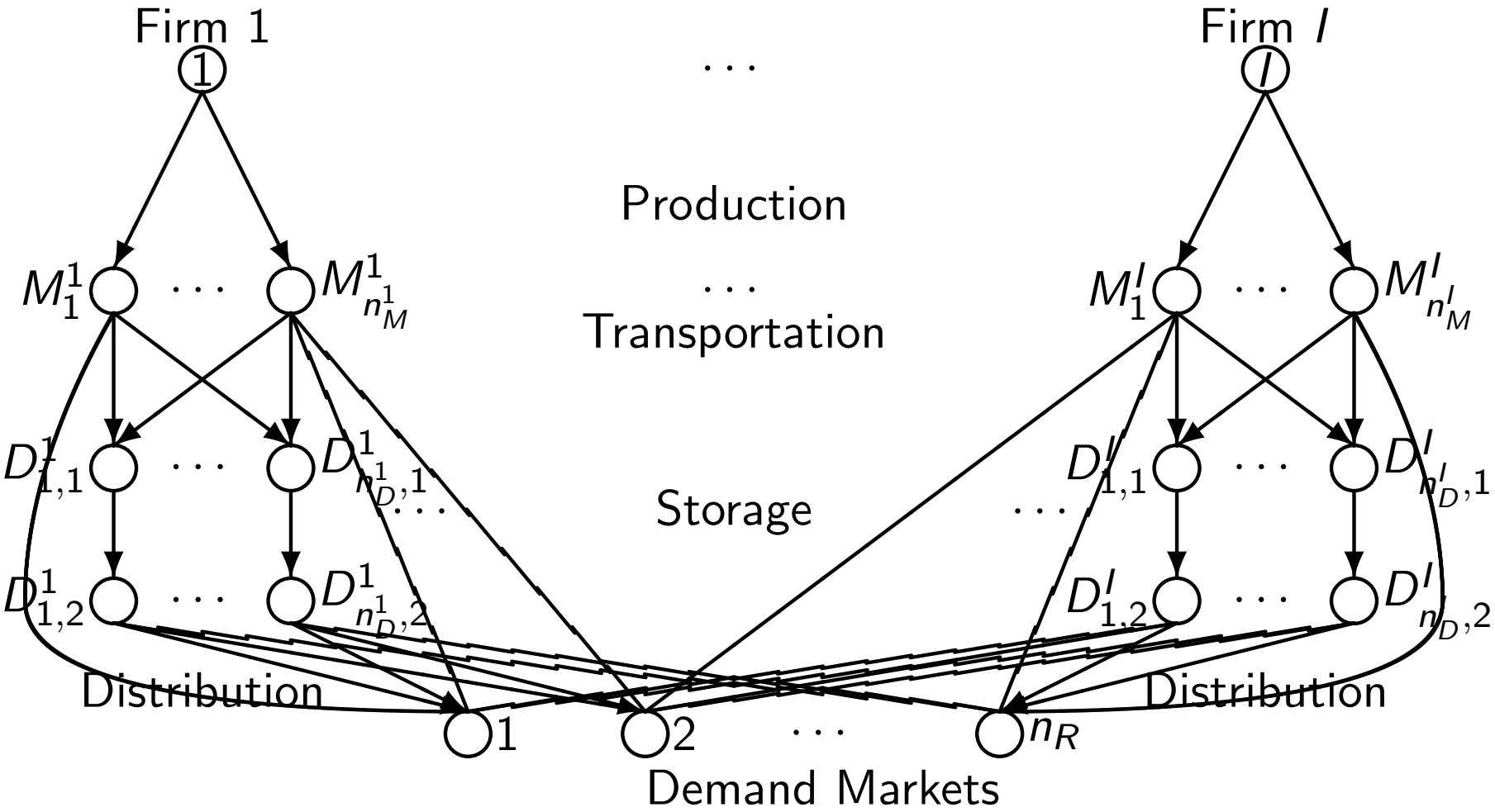


Figure: The Supply Chain Network Topology of the Game Theory Model with Labor

Game Theory Supply Chain Network Model with Labor

The model considers three sets of labor constraints, of increasing flexibility of movement.

1. **In the first set**, **each supply chain link has an upper bound of available labor.** Labor is is not free to move to other production sites, nor to other distribution centers, or assist in freight service provision.
2. **In the second set**, **labor is free to move across a supply chain set of network economic activities (such as production, or transportation, or storage, and, finally, distribution).** There is a capacity of labor associated with each such "tier" of supply chain links. Those who have skills in production, or in distribution, etc., may be reallocated. This has been happening in freight service provision, for example, during the Covid-19 pandemic.
3. **In the third set**, **labor is free to move across all the supply chain network economic activities, and there is a single capacity.** McKinsey & Company noted this is a means towards resilience and returning the supply chain to effectiveness while reenvisioning and reforming.

In the paper, we present a series of numerical examples documenting the potential impacts of labor disruptions under different scenarios.

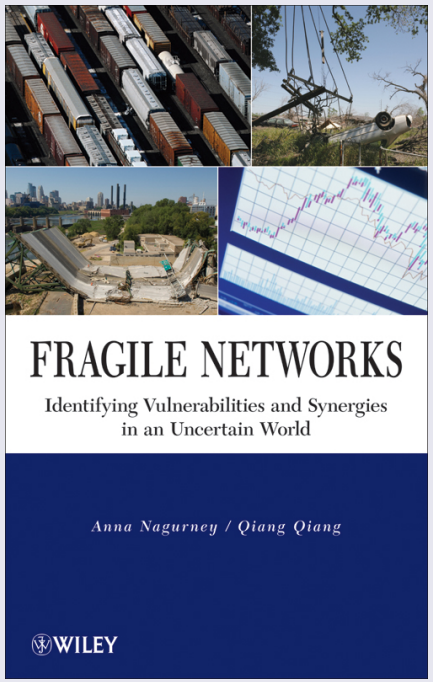
We include results for disruptions at manufacturing plants, storage facilities; the impacts of the addition of a competitor, changes in demand price functions, as well as decreases in available labor throughout the supply chain network economy.

The research adds to modeling methodology as well as applications since two of the scenarios are Generalized Nash Equilibrium problems.

Cybercrime

How I Became Interested in Cybersecurity

One of my books, written with a UMass Amherst PhD alum, now Professor Qiang, 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*.

How I Became Interested in Cybersecurity

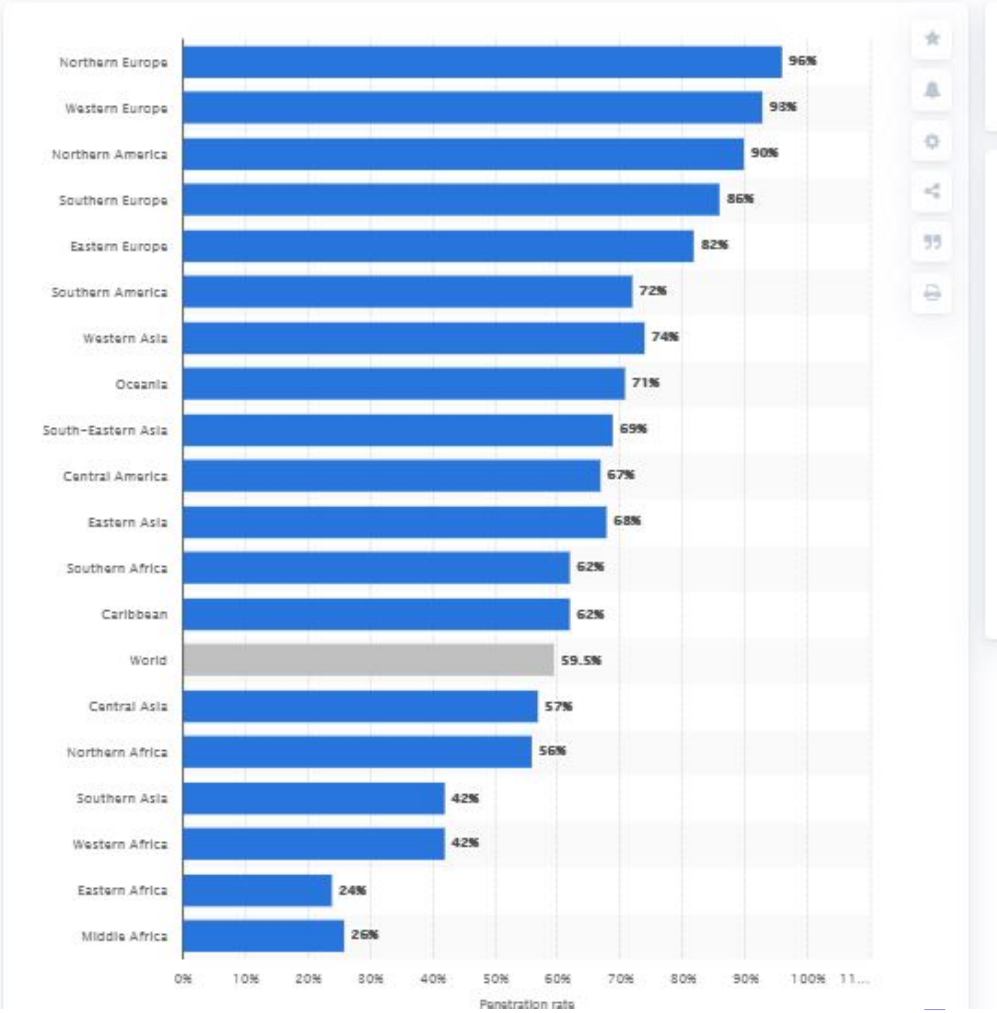
The publisher John Wiley & Sons was notified and lawyers got involved but how do you contact and then influence those responsible for postings on rather anonymous websites?

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.

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

In 2012, there were over 2.4 billion users. In 2020, there were 4.5 billion Internet users with 3.8 billion on social media. Table below thanks to Statista 2021.

Global internet penetration rate as of January 2021, by region



Some Recent Major Cyberattacks

The US Department of Justice declared 2020 as the "worst year ever" for extortion-related cyberattacks.

The Colonial Pipeline attack in April, 2021 resulted in payment of $4.4 million in ransom (The Washington Post (2021)).

JBS - the world's biggest meat producer was attacked in late May, 2021, with ransomware (The New York Times (2021)).

The New York MTA and the **ferry operator Steamship Authority** in eastern Massachusetts were recently hit by a ransomware attack (The Wall Street Journal (2021)).

City governments in the US as well as healthcare organizations have also been subject to cyberattacks with ransoms sought and, sometimes, paid.

Some Other Major Cyberattacks

• **Equifax**: In September, 2017, it was revealed that names, SSNs, birthdates, drivers' license information, and credit card numbers on about 143 million U.S. consumers was compromised in a cybersecurity breach that began in mid-May and was discovered only on July 29, 2017 (Bloomberg (2017)). In late February 2018, Equifax disclosed that it had discovered that an additional 2.4 million U.S. consumers were affected by the cyberattack (Reuters (2018)).

• **"WannaCry" ransomware**: Began in mid-May 2017. It crippled National Health Services (NHS) hospitals in the UK, hobbling emergency rooms, delaying vital medical procedures, etc. (WIRED (2017)).

Some Other Major Cyberattacks

• **Banks:** The Carbanak group, also known as Anunak, was exposed in 2015 after supposedly stealing upwards of $1 billion from more than 100 banks across 30 countries (The New York Times (2015)).

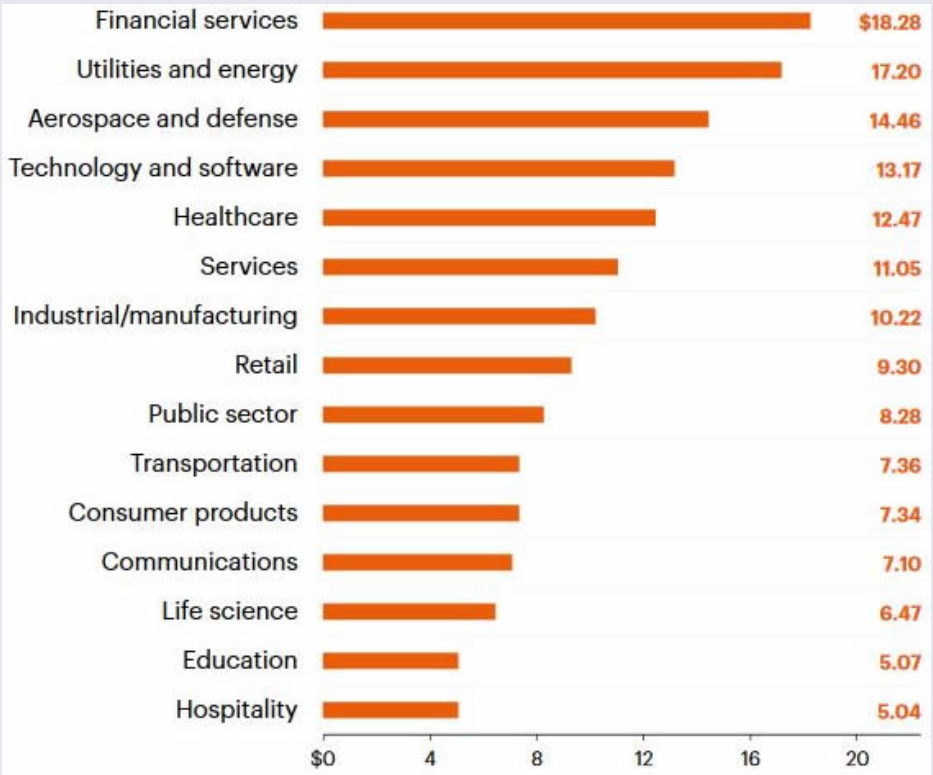
• **US Office of Personnel Management:** In June 2015, OPM discovered that sensitive information, including SSNs of 21.5 million federal employees was stolen (WIRED (2016)).

•**Sony Pictures Entertainment** The attack on Sony in 2014 destroyed data on more than 3,000 computers and disclosed prerelease films and embarrassing emails of executives (Fortune (2015)).

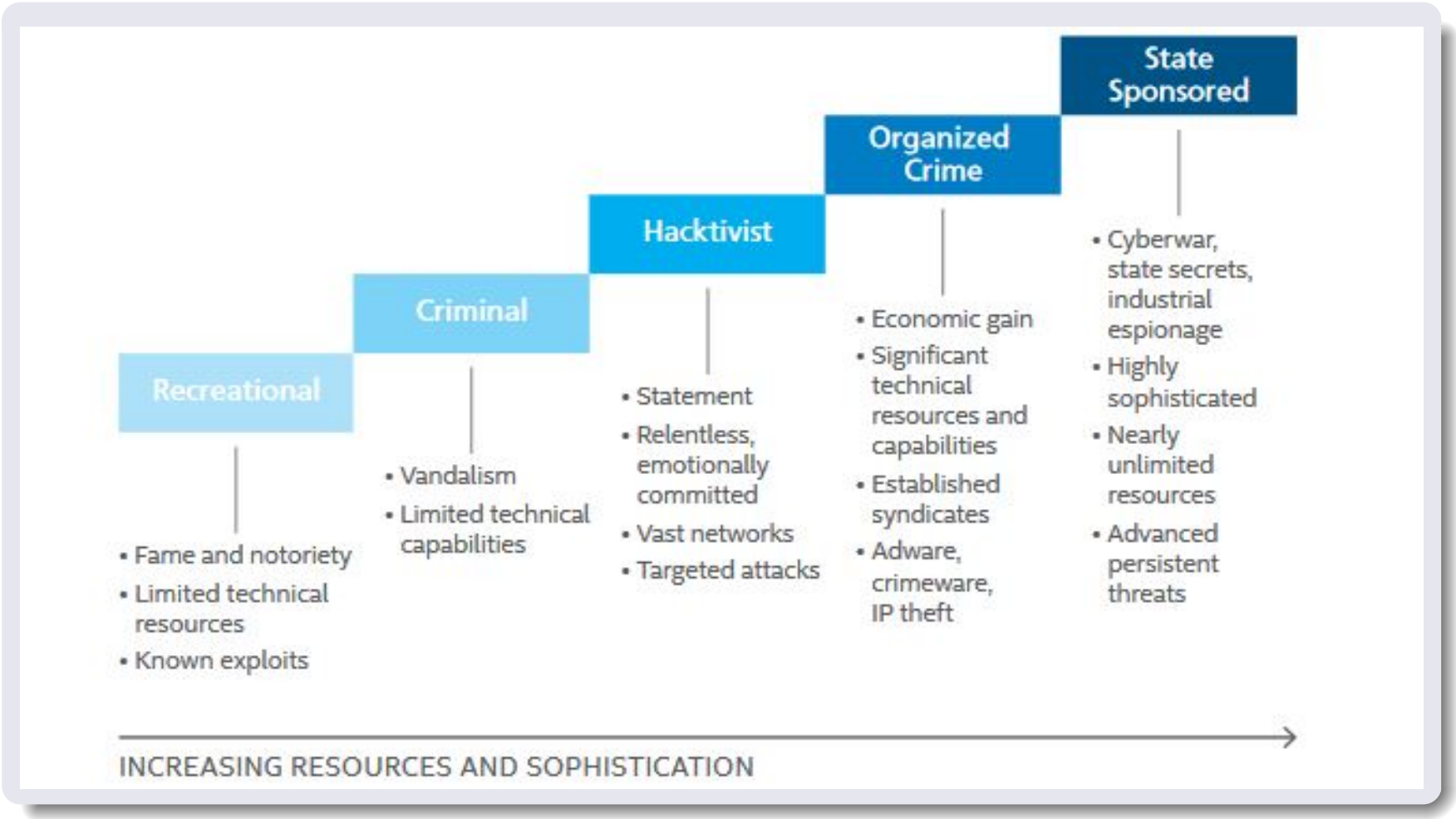
•**Target, Home Depot, Michaels Stores, Staples, and eBay:** These were breached in 2014 - card data and personal information of millions of customers were stolen (The New York Times (2015)).

Cost of Cybercrime

- **Cybercrimes are costly for organizations.** According to the FBI, the cost of cybercrime in the US was $3.5 billion in 2019. However, the actual toll could be much higher since oftentimes the exploits and intrusions go unnoticed.



Changing Attacker Profiles

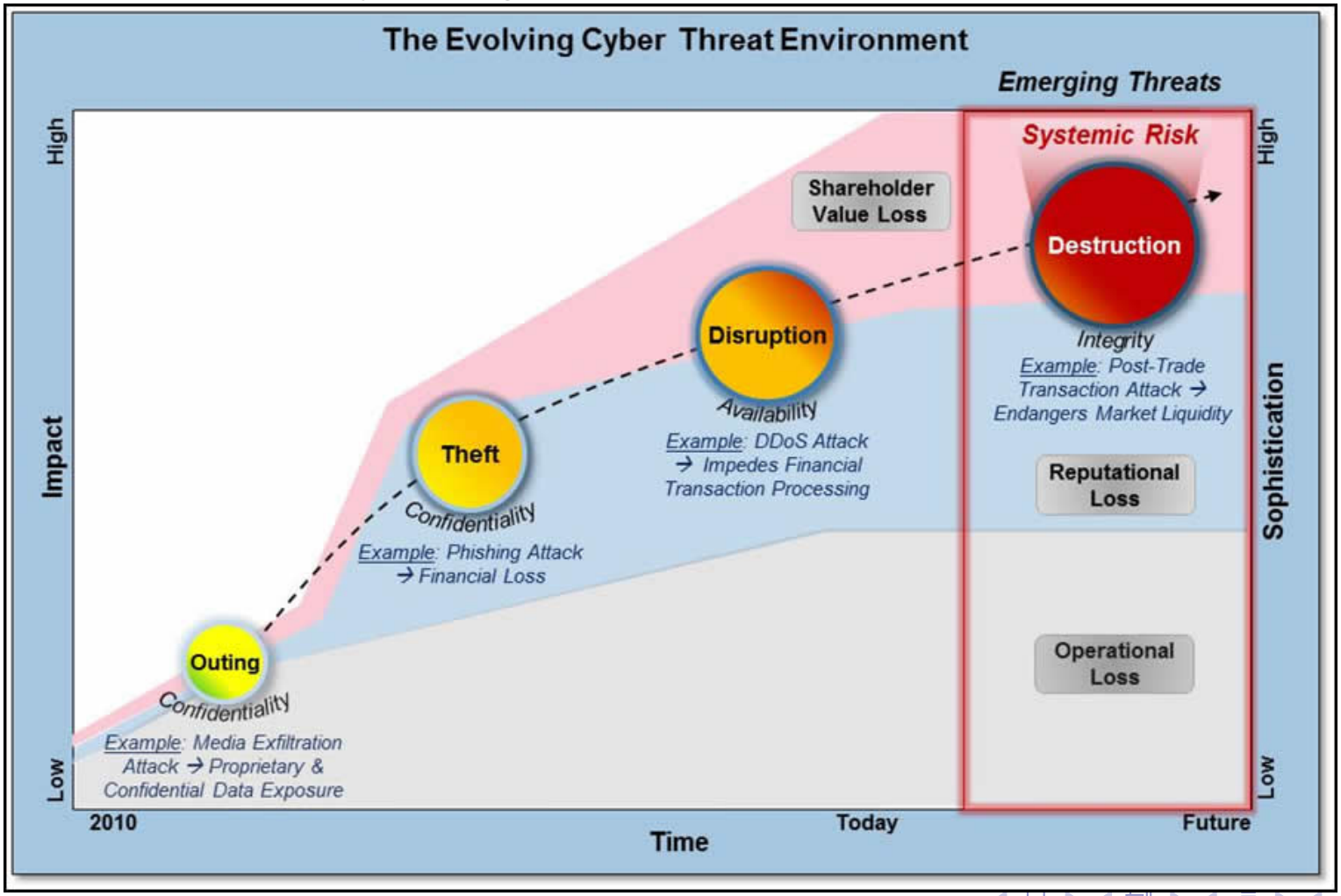


McAfee Labs Threats Report, August 2015

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. The number of ransomware claims and their average costs are also up substantially.

Mitigation may require enabling technologies, intrusion prevention systems, applications security testing solutions and enterprise solutions.

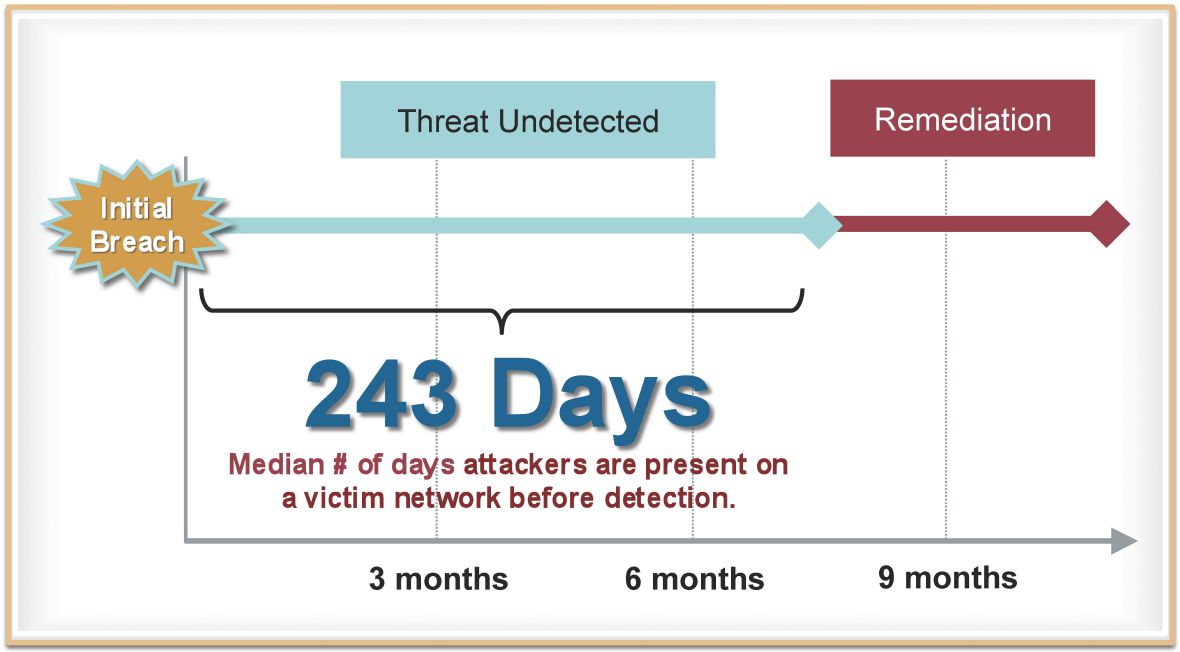


Putting Cybercrime in Context

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. By 2021, cybercrime is expected to cost the world $6 trillion yearly, making it more profitable than the global illegal drug trade, according to data provider Cybersecurity Ventures (2019).

Cyberattacks



Source: Mandiant M-Trends 2013

The median number of days that attackers were present on a victim's network before being discovered dropped to 146 days in 2015 from 205 days in 2014 – a trend that shows positive improvement since measuring 416 days back in 2012. In 2019 the dwell time was 177 days and in 2020 - 54 days. GDPR is getting credit for this. Breaches still often go undetected for years, according to Mandiant/FireEye.

Cybercrime and Financial Institutions

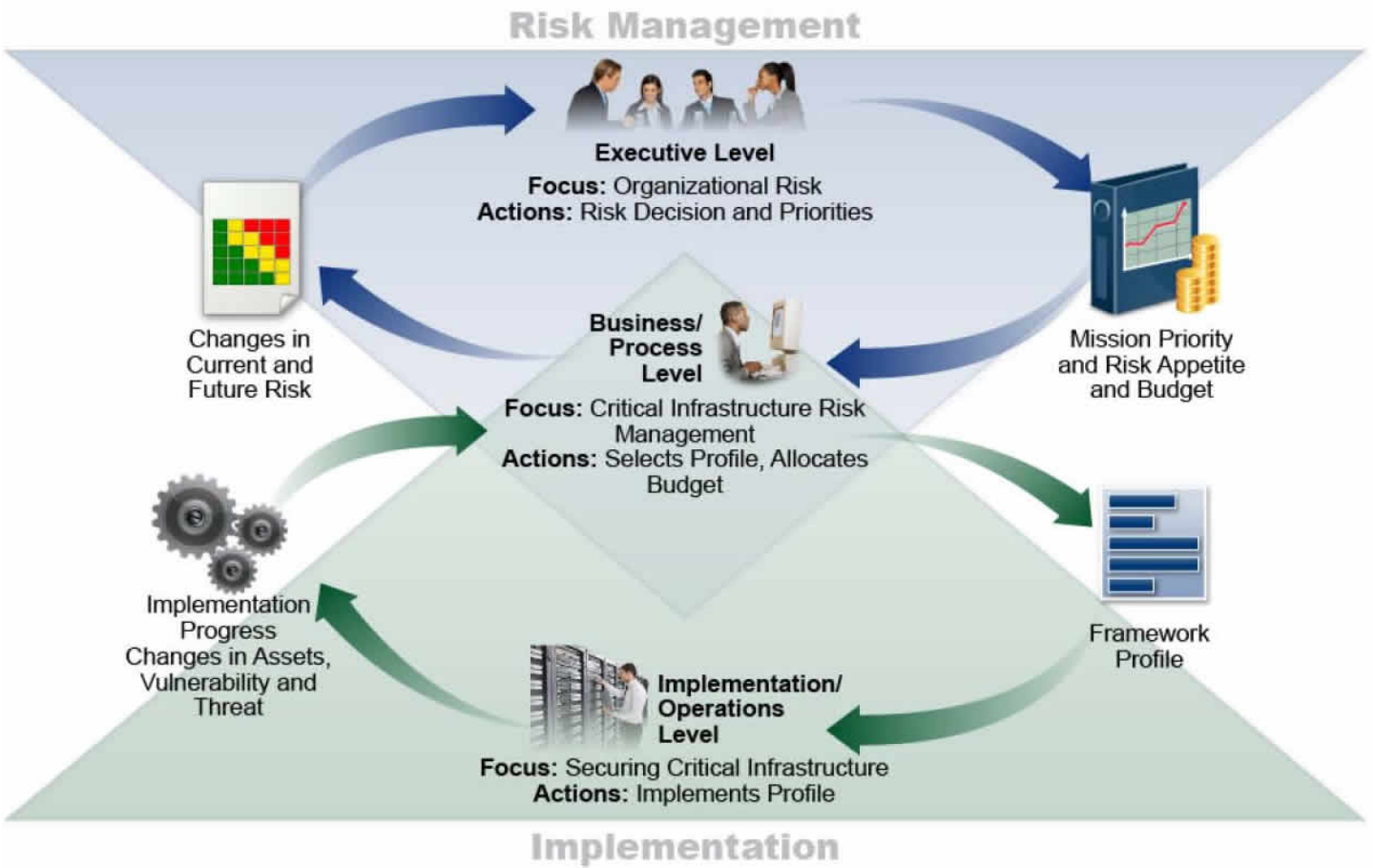
• According to a recent survey cybercrime is placing heavy strains on the global financial sector, with cybercrime now the second most commonly reported economic crime affecting financial services firms.

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

• An Accenture (2019) study found that the average annualized cost of cybercrime for financial services companies globally has increased to $18.5 million - the highest of all industries included in the study and more than 40% higher than the average cost of $13 million per firm across all industries.

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

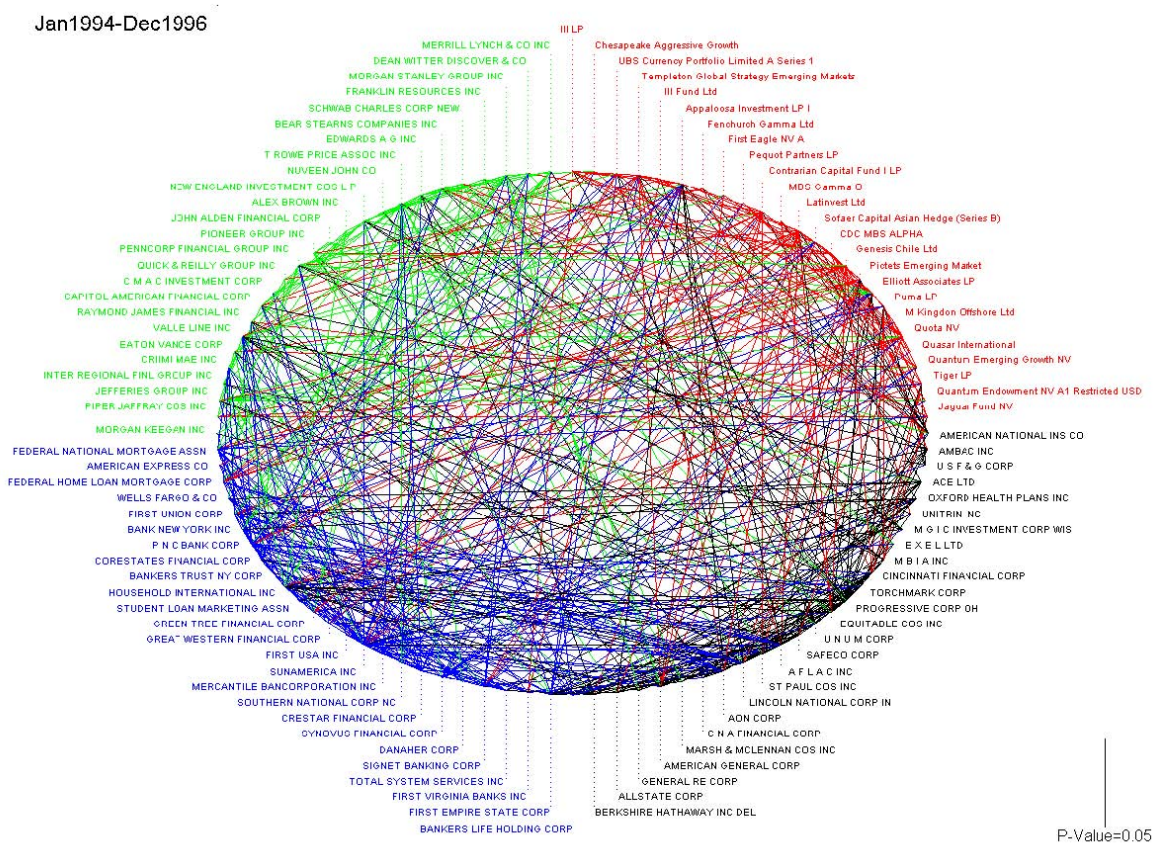
It's About Risk Management



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

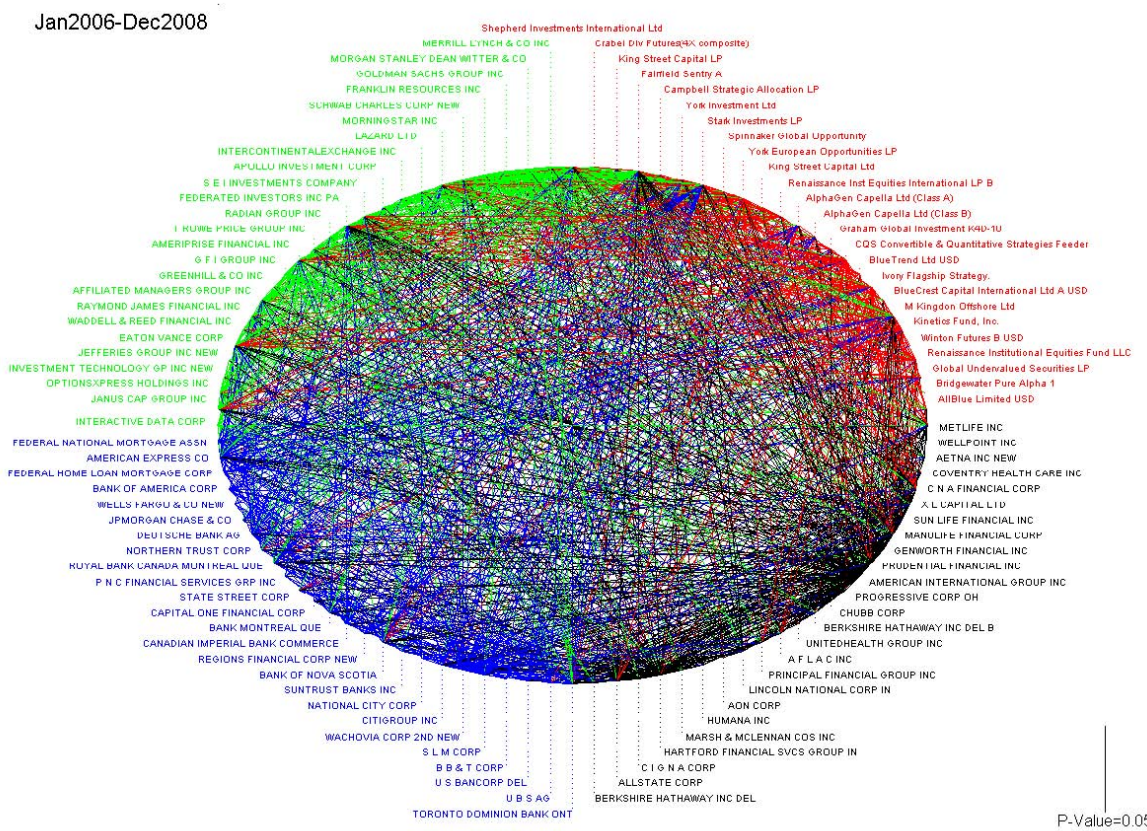
Which Nodes and Links Really Matter?

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)

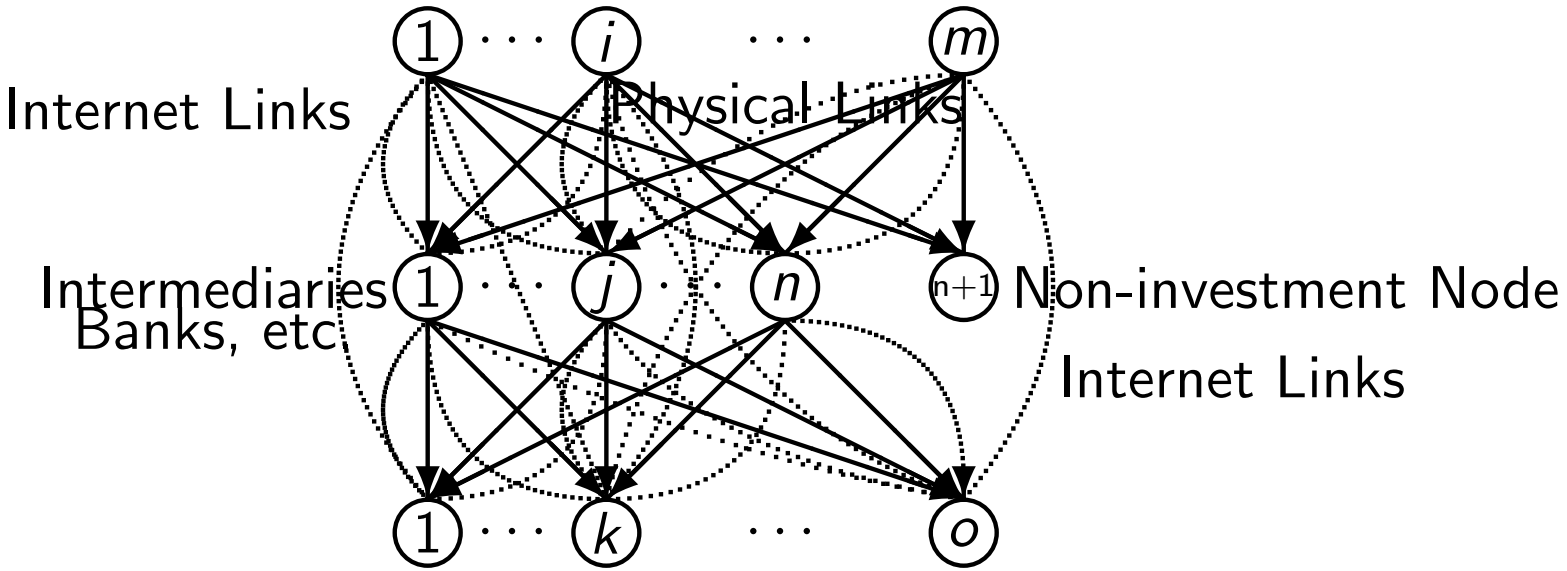
Empirical Evidence: Jan. 2006 - Dec. 2008 - Connectivity, Vulnerability



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

The Financial Network Model

Sources of Financial Funds: Businesses, Households, etc.



Demand Markets: Real Estate, Household, and Business Loans, etc.

Figure: The Structure of the Financial Network with Intermediation

A. Nagurney and K. Ke (2003), "Financial Networks with Electronic Transactions: Modeling, Analysis, and Computations," *Quantitative Finance* **3**, pp 71-87.

The Nagurney and Qiang (N-Q) 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.

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

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: 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

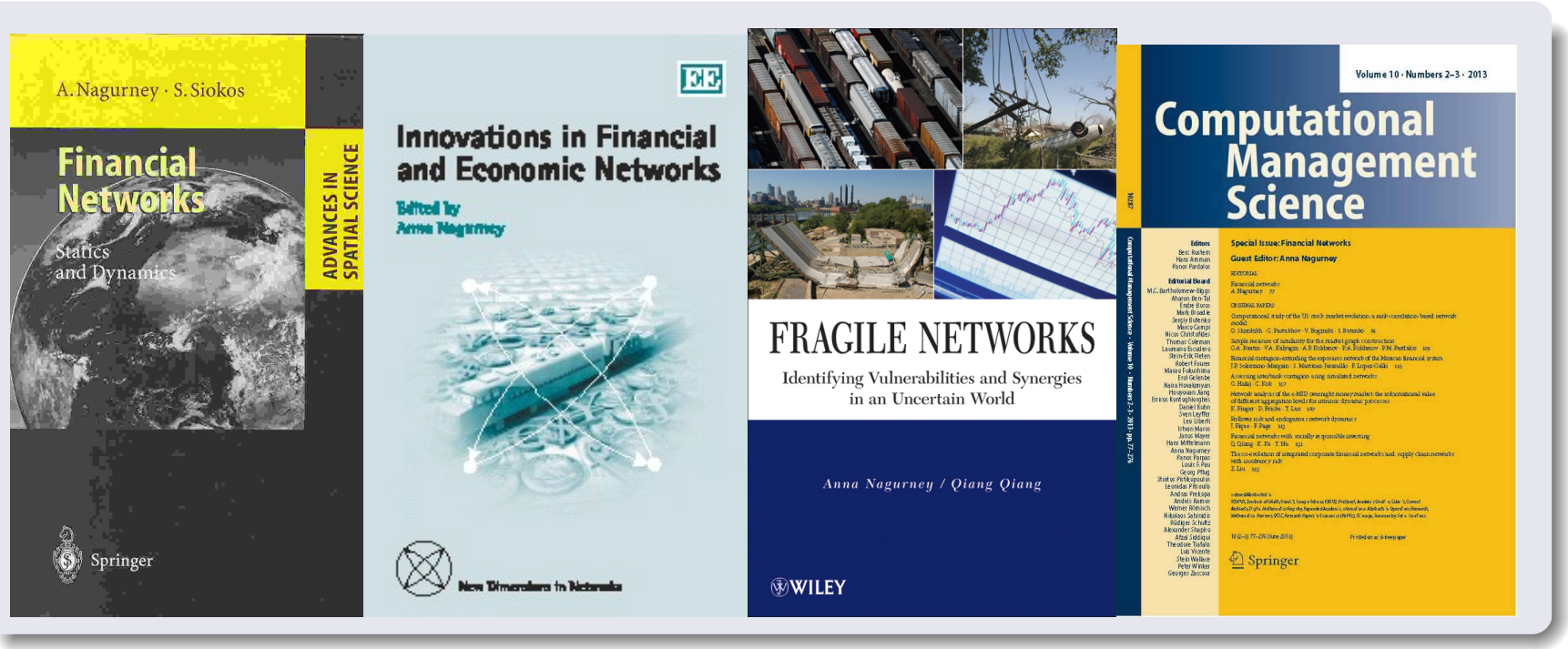
Table: Nodal Results for the Braess Network

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



A Predictive Network Economic Model of Cybercrime

Network Economics of Cybercrime

- We lay the foundation for the development of network economics based models for cyberccrime in financial services.
- **Financial services firms as well as hackers are economic agents.**
- **Our view is that financial firms produce/possess commodities (or products) that hackers (criminals) seek to obtain.**
- 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**.

Network Economics of Cybercrime

- 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.

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

• After the major 2013 Target breach, **some credit cards obtained thus initially sold for $135 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. **Target paid out $18.5M for the 2013 data breach that affected 41 million consumers.**

• Different "brands" of credit cards can be viewed as different products since they command different prices on the black market. 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 much more. **Hacked credit card numbers of European credit cards can command prices five times higher than U.S. cards** (Peterson (2013)).

Perishability and Cybercrime in Financial Products

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.

Perishability and Cybercrime in Financial Products

This part of the talk is based on the paper, "A Multiproduct Network Economic Model of Cybercrime in Financial Services," A. Nagurney, *Service Science* 7(1) (2015), pp 70-81.

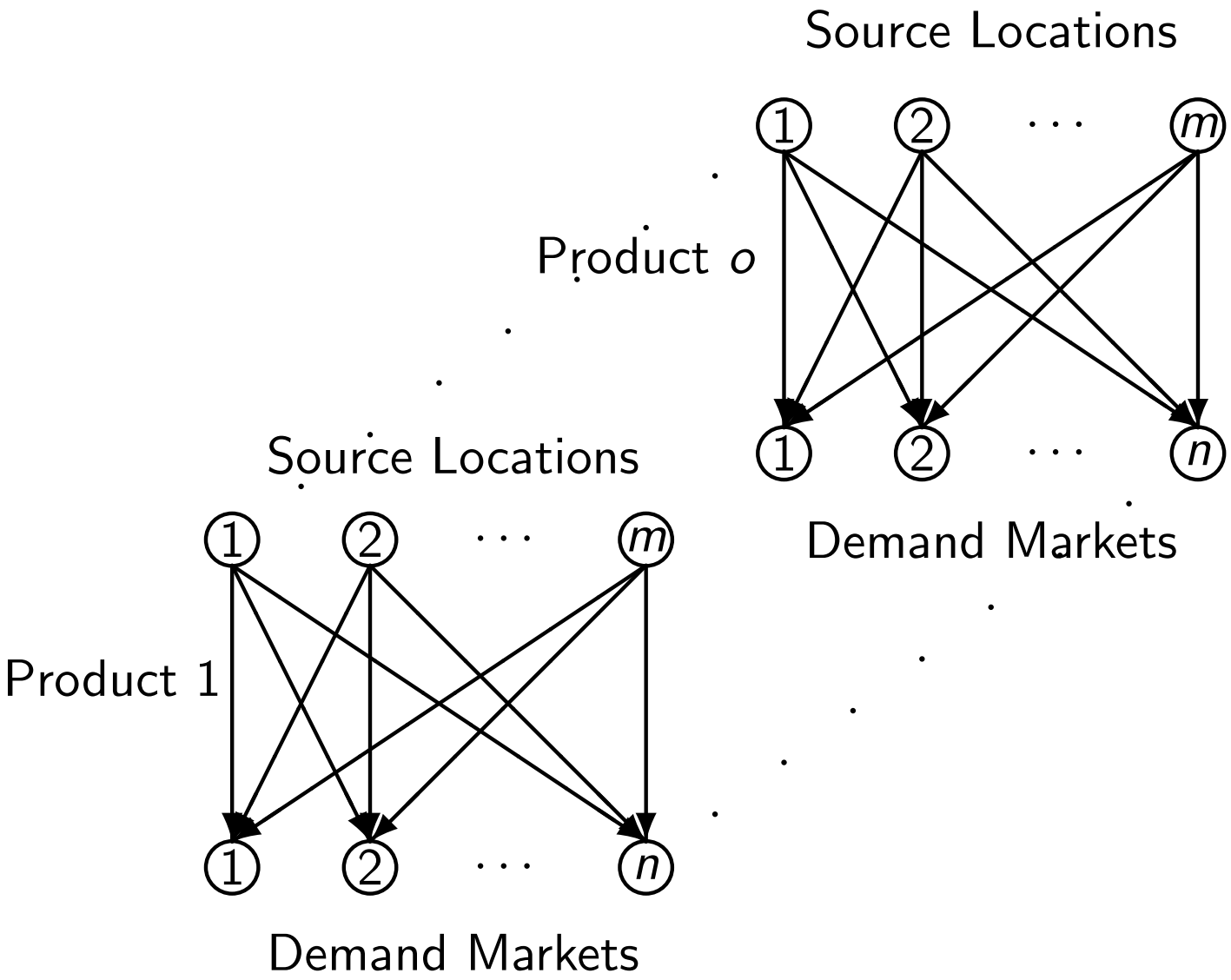


Figure: Structure of the Network Economic Problem

Some Notation - Variables

Variables

Let Q_{ij}^k denote the nonnegative amount of financial product k obtained from i and shipped to j. Q is the vector of Q_{ij}^ks.

Let s_i^k denote the nonnegative supply of financial product k at i and let d_j^k be the demand for k and j. s is the vector of s_i^ks and d is the vector of d_j^ks.

T_{ij}^k is the time between the acquisition of product k from source location i and its sale at j.

$T_{ave,j}^k$ is the average time for delivery of product k at demand market j, where $T_{ave,j}^k = \frac{\sum_{i=1}^m T_{ij}^k Q_{ij}^k}{d_j^k}$. T_{ave} is the vector of $T_{ave,j}^k$s.

Some Notation - Functions

Functions

Let $\pi_i^k(s)$ denote the price of acquiring product k at source location i.

Let $\rho_j^k(d, T_{ave})$ denote the demand price of financial product k at demand market j.

Let $\hat{c}_{ij}^k(Q)$ denote the unit transaction cost associated with transacting product k between i and j.

Conservation of Flow Equations

The conservation of flow equations are:

$$s_i^k = \sum_{j=1}^{n} Q_{ij}^k, \quad k = 1, \ldots, o; i = 1, \ldots, m,$$

$$d_j^k = \sum_{i=1}^{m} Q_{ij}^k, \quad k = 1, \ldots, o; i = 1, \ldots, n,$$

$$Q_{ij}^k \geq 0, \quad k = 1, \ldots, o; i = 1, \ldots, m; j = 1, \ldots, n.$$

In addition, we introduce the following expression, which captures time:

$$t_{ij}^k Q_{ij}^k + h_{ij}^k = T_{ij}^k, \quad k = 1, \ldots, o; i = 1, \ldots, m; j = 1, \ldots, n.$$

In view of the conservation of flow equations, we can define new demand price functions $\hat{\rho}_j^k$, $\forall k, \forall j$ as follows:

$$\hat{\rho}_j^k(Q) \equiv \rho_j^k(d, T_{ave}), \quad k = 1, \ldots, o; j = 1, \ldots, n.$$

If the demand at a demand market for a product is equal to zero, we remove that demand market from the network for that product since the corresponding time average would not be defined.

Also, we can define new supply price functions $\hat{\pi}_i^k$, $\forall k, \forall i$ as:

$$\hat{\pi}_i^k(Q) \equiv \pi_i^k(s), \quad k = 1, \ldots, o; j = 1, \ldots, n,$$

which allow us to construct a variational inequality formulation governing the equilibrium conditions below with nice features for computations. We assume that all the functions in the model are continuous.

The Network Economic Equilibrium Conditions

The network economic equilibrium conditions for cybercrime have been achieved if for all products k; $k = 1, \ldots, o$, and for all pairs of markets (i, j); $i = 1, \ldots, m$; $j = 1, \ldots, n$, the following conditions hold:

$$\hat{\pi}_i^k(Q^*) + c_{ij}^k(Q^*) \begin{cases} = \hat{\rho}_j^k(Q^*), & \text{if} \quad Q_{ij}^{k*} > 0 \\ \geq \rho_j^k(Q^*), & \text{if} \quad Q_{ij}^{k*} = 0, \end{cases}$$

where recall that $\hat{\pi}_i^k$ denotes the price of product k at source location i, c_{ij}^k denotes the unit transaction cost associated with k between (i, j), and $\hat{\rho}_j^k$ is the demand price of k at demand market j. Q_{ij}^{k*} is the equilibrium flow of product k between i and j with Q^* being the vector of all such flows.

We define the feasible set $K \equiv \{Q | Q \in R_+^{omn}\}$.

Theorem: Variational Inequality Formulation

A product flow pattern $Q^* \in K$ is a cybercrime network economic equilibrium if and only if it satisfies the variational inequality problem:

$$\sum_{k=1}^{o}\sum_{i=1}^{m}\sum_{j=1}^{n}\left[\hat{\pi}_i^k(Q^*) + c_{ij}^k(Q^*) - \hat{\rho}_j^k(Q^*)\right] \times (Q_{ij}^k - Q_{ij}^{k*}) \geq 0,$$

$$\forall Q \in K.$$

The above VI can be put into standard form (see Nagurney (1999)): determine $X^* \in \mathcal{K}$, such that

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

if we define $\mathcal{K} \equiv K$, $X \equiv Q$, and $F(X) \equiv (F_{kij}(X))$; $k = 1, \ldots, o$; $i = 1, \ldots, m$; $j = 1, \ldots, n$, where $F_{kij} = \hat{\pi}_i^k(Q) + c_{ij}^k(Q) - \hat{\rho}_j^k(Q)$.

The Algorithm

The Euler Method

At each iteration τ one solves the following problem:

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

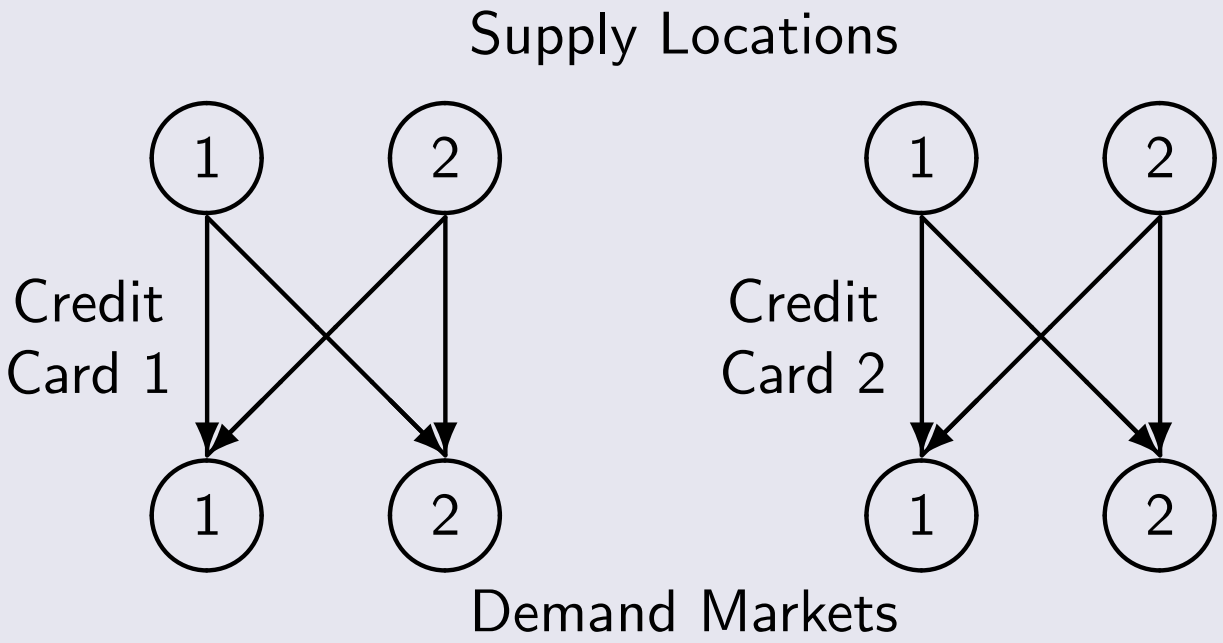
where $P_{\mathcal{K}}$ is the projection operator, and where $\{a_{\tau}\}$ must satisfy: $\sum_{\tau=0}^{\infty} a_{\tau} = \infty$, $a_{\tau} > 0$, $a_{\tau} \rightarrow 0$, as $\tau \rightarrow \infty$.

Explicit Formulae

We have the following closed form expression for the product flows $k = 1, \ldots, m$; $i = 1, \ldots, m$; $j = 1, \ldots, n$:

$$Q_{ij}^{k\,\tau+1} = \max\{0, Q_{ij}^{k\,\tau} + a_{\tau}(\hat{\rho}_j^k(Q^{\tau}) - c_{ij}^k(Q^{\tau}) - \hat{\pi}_i^k(Q^{\tau})\}.$$

The Network Topology of the Examples



Example 1

The supply price functions are:

$$\pi_1^1(s) = 5s_1^1 + s_2^1 + 2, \quad \pi_2^1(s) = 2s_2^1 + s_1^1 + 1,$$

$$\pi_1^2(s) = 2s_1^2 + s_1^1 + 1, \quad \pi_2^2(s) = s_2^2 + .5s_2^1 + 1.$$

The unit transaction cost functions are:

$$c_{11}^1(Q) = .03{Q_{11}^1}^2 + 3Q_{11}^1 + 1, \quad c_{21}^1(Q) = .02{Q_{21}^1}^2 + 2Q_{21}^1 + 2,$$

$$c_{11}^2(Q) = .01{Q_{11}^2}^2 + Q_{11}^2 + 1, \quad c_{21}^2(Q) = .001{Q_{21}^2}^2 + .1Q_{21}^2 + 1,$$

$$c_{12}^1(Q) = .01{Q_{12}^1}^2 + Q_{12}^1 + 1, \quad c_{22}^1(Q) = .01{Q_{22}^1}^2 + Q_{22}^1 + 1,$$

$$c_{12}^2(Q) = .01{Q_{12}^2}^2 + Q_{12}^2 + 1, \quad c_{22}^2(Q) = .02{Q_{22}^2}^2 + 2Q_{22}^2 + 2.$$

Example 1

The demand price functions are:

$$\rho_1^1(d, T_{ave}) = -2d_1^1 - d_1^2 - .5T_{ave,1}^1 + 500,$$

$$\rho_1^2(d) = -3d_1^2 - d_1^1 - .1T_{ave,1}^2 + 300,$$

$$\rho_2^1(d, T_{ave}) = -d_2^1 - .5d_2^2 - .2T_{ave,2}^1 + 200,$$

$$\rho_2^2(d, T_{ave}) = -2d_2^2 - d_2^1 - .1T_{ave,2}^2 + 100.$$

Example 1

The time expressions are:

$$T_{11}^1 = .1Q_{11}^1 + 10, \quad T_{21}^1 = .5Q_{21}^1 + 5,$$

$$T_{11}^2 = .1Q_{11}^2 + 20, \quad T_{21}^2 = .5Q_{21}^2 + 15,$$

$$T_{12}^1 = .1Q_{12}^1 + 10, \quad T_{22}^1 = .1Q_{22}^1 + 10,$$

$$T_{12}^2 = .5Q_{12}^2 + 5, \quad T_{22}^2 = .5Q_{22}^2 + 10,$$

so that

$$T_{ave,1}^1 = \frac{T_{11}^1 Q_{11}^1 + T_{21}^1 Q_{21}^1}{d_1^1}, \quad T_{ave,1}^2 = \frac{T_{11}^2 Q_{11}^2 + T_{21}^2 Q_{21}^2}{d_1^2}.$$

$$T_{ave,2}^1 = \frac{T_{12}^1 Q_{12}^1 + T_{22}^1 Q_{22}^1}{d_2^1}, \quad T_{ave,2}^2 = \frac{T_{12}^2 Q_{12}^2 + T_{22}^2 Q_{22}^2}{d_2^2}.$$

Example 2

Example 2 has the same data as Example 1 except that now we have a modification in the demand price function associated with the second product at Demand Market 2 so that:

$$\rho_2^2(d, T_{ave}) = -2d_2^2 - d_2^1 - .1T_{ave,2}^2 + 200.$$

Such a change might represent that the value of this financial product has increased at that demand market.

Example 3

Example 3 was constructed from Example 2 and had the same data except that we increased the fixed terms in all the transaction cost functions so that:

$$c_1^1(Q) = .03{Q_{11}^1}^2 + 3Q_{11}^1 + 10, \quad c_{21}^1(Q) = .02{Q_{21}^1}^2 + 2Q_{21}^1 + 20,$$

$$c_{11}^2(Q) = .01{Q_{11}^2}^2 + Q_{11}^2 + 10, \quad c_{21}^1(Q) = .001{Q_{21}^2}^2 + .1Q_{21}^2 + 10,$$

$$c_{12}^1(Q) = .01{Q_{12}^1}^2 + Q_{12}^1 + 10, \quad c_{22}^1(Q) = .01{Q_{22}^1}^2 + Q_{22}^1 + 10,$$

$$c_{12}^2(Q) = .01{Q_{12}^2}^2 + Q_{12}^2 + 10, \quad c_{22}^2(Q) = .02{Q_{22}^2}^2 + 2Q_{22}^2 + 20.$$

This could represent the situation that the cybercriminals have a harder time fencing all the products at all the demand markets.

Results

Table: Equilibrium Solutions for the Examples

Financial Flows	**Example 1**	**Example 2**	**Example 3**
$Q_{11}^{1}{}^{*}$	25.93	26.31	26.21
$Q_{12}^{1}{}^{*}$	0.00	0.00	0.00
$Q_{21}^{1}{}^{*}$	46.73	48.28	46.45
$Q_{22}^{1}{}^{*}$	16.77	12.50	11.61
$Q_{11}^{2}{}^{*}$	11.69	4.81	3.47
$Q_{12}^{2}{}^{*}$	6.09	23.46	23.59
$Q_{21}^{2}{}^{*}$	37.56	39.27	39.57
$Q_{22}^{2}{}^{*}$	0.00	12.67	9.69

Results

Table: Incurred Equilibrium Prices and Average Times

Prices	**Example 1**	**Example 2**	**Example 3**
$\rho_1^1(d^*, T_{ave}^*)$	294.07	295.07	300.35
$\rho_1^2(d^*, T_{ave}^*)$	76.52	89.85	94.87
$\rho_2^1(d^*, T_{ave}^*)$	175.51	164.94	167.28
$\rho_2^2(d^*, T_{ave}^*)$	69.98	113.86	120.52
Average Times	**Example 1**	**Example 2**	**Example 3**
$T_{ave,1}^1$	22.74	23.32	22.59
$T_{ave,1}^2$	30.78	33.09	33.62
$T_{ave,2}^1$	23.35	22.50	22.32
$T_{ave,2}^2$	10.61	13.75	13.08

Managerial Insights

• The above numerical examples, although stylized, provide important managerial insights that cybersecurity professionals may take advantage of in securing their data.

• The examples show the quantified impacts of changes in the data on the equilibrium financial product flows, and on the incurred demand prices and average times for product delivery.

• The results are consistent with existing data on hacked credit cards. **For example, Goncharov (2012) reports that the cost, that is, the supply price, of hacking into various accounts can range anywhere from $16 to over $325. Also, as reported in Ablon, Libicki, and Golay (2014), following an initial breach, the markets may get flooded with cybercrime products leading to a decrease in prices, which the structure of our demand price functions capture**.

Managerial Insights

• Credit cards acquired in the Target breach **initially fetched from $20 to $135 depending on the type of card, expiration date as well as limit (cf. Ablon, Libicki, and Golay (2014))**. Although our numerical study did not focus on a specific historical data breach, the results are not inconsistent with results obtained in practice.

• Finally, the model captures the crucial time element in the demand market pricing of products obtained through cybercrime with a focus on financial services.

Cybersecurity Investments

Multifirm Models of Cybersecurity Investment

This part of the presentation is based on the paper, **"Multifirm Models of Cybersecurity Investment Competition vs. Cooperation and Network Vulnerability," A. Nagurney and S. Shukla,** *European Journal of Operational Research* **260(2) (2017), pp 588-600**, where many references and additional theoretical and numerical results can be found.

Investing in Cybersecurity

There is a growing interest in developing rigorous frameworks for cybersecurity investments.

JPMorgan increased its cybersecurity spending to over $600 million in 2019 (The New York Times).

It is clear that making the best cybersecurity investments is a very timely problem and issue.

Common Features of the Models

We describe three different models of multifirm cybersecurity investments.

The first model is a Nash Equilibrium (NE) one capturing noncooperative behavior; the second and third are cooperative models, using Nash Bargaining (NB) and System-Optimization (S-O) concepts, respectively.

Common Features of the Models

There are m firms in the "network." These firms can be financial service firms, energy firms, manufacturing firms, or even retailers.

Each firm i; $i = 1, \ldots, m$, 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, wlog, by s_i; $i = 1 \ldots, m$.

Common Features of the Models

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

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

where $u_{s_i} < 1$, and is also greater than zero, is the upper bound on the security level for firm i.

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. We group the security levels of all firms into the m-dimensional vector s.

Common Features of the Models

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.

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 we use in this paper is

$$h_i(s_i) = \alpha_i\left(\frac{1}{\sqrt{(1 - s_i)}} - 1\right)$$

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 (2015).

Common Features of the Models

Network Security Level of a Firm and the Network Vulnerability

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

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

The vulnerability of firm i, $v_i = (1 - s_i)$, and the network vulnerability, $\bar{v} = (1 - \bar{s})$.

Common Features of the Models

Following Shetty (2010), the probability p_i of a successful attack on firm i; $i = 1, \ldots, m$ is

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

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.

Common Features of the Models

Each firm i; $i = 1, \ldots, m$ 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 we use is $\sqrt{W_i}$ (see Shetty et al. (2009)).

Also, a firm i is faced with damage D_i if there is a successful cyberattack on it.

Common Features of the Models

Expected Utility of a Firm

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

$$E(U_i) = (1 - p_i) f_i(W_i) + p_i(f_i(W_i - D_i)) - h_i(s_i).$$

We may write $E(U_i) = E(U_i(s)), \forall i$. Each $E(U_i(s))$ is strictly concave with respect to s_i under the assumed functional forms above since we also know that each $h_i(s_i)$; $i = 1, \ldots, m$ is strictly convex.

The Nash Equilibrium Model of Cybersecurity Investments

We 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. 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.

Definition: 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 $i; i = 1, \ldots, m$:

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

where

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

VI Formulation of the NE Model

Theorem: VI Formulation of Nash Equilibrium

Since for each firm i; $i = 1, \ldots, m$ the expected profit function $E(U_i(s))$ is concave with respect to the variable s_i, and is continuously differentiable, and the feasible set K^1 is convex, we know that $s^* \in K^1$ is a Nash equilibrium in cybersecurity levels according to the Definition if and only if it satisfies the VI

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

or, if and only if it satisfies the VI

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

$$\times (s_i - s_i^*) \geq 0, \ \forall s \in K^1.$$

Algorithm for the Solution of the NE Model

We can apply the Euler method, presented earlier to solve this model.

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:

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

$$\max\{0, \min\{u_{s_i}, s_i^\tau + a_\tau(-\frac{\partial h_i(s_i^\tau)}{\partial s_i^\tau} - (f_i(W_i) - f_i(W_i - D_i))$$

$$\left[\frac{1}{m}\sum_{j=1}^{m} s_j^\tau - 1 - \frac{1}{m} + \frac{s_i^\tau}{m}\right]\}\}.$$

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). An excellent overview can be found in Binmore, Rubinstein, and Wolinsky (1989) and in the book by Muthoo (1999).

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

The Nash Bargaining Model of Cybersecurity Investments

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

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

The optimization problem to be solved is then:

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

subject to:

$$E(U_j(s)) \geq E(U_j^{NE}), \quad j = 1, \ldots, m, \quad s \in K^1.$$

We define the feasible set K^2 consisting of the above constraints, which we know is convex.

The S-O Model of Cybersecurity Investments

Under system-optimization, the objective function becomes:

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

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:

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

subject to:

$$s \in K^1.$$

A Retail Case Study

A Retail Case Study

A Retail Case Study

Solutions of the Nash Equilibrium model were computed by applying the Euler method, with the Euler method implemented in Matlab on a Lenovo G410 laptop with an Intel Core i5 processor and 8GB RAM.

The convergence tolerance was 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 $\{a_\tau\}$ was set to: $.1\{1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, ...\}$.

We initialized the Euler method by setting the security levels at their lower bounds. The upper bounds on the security levels $u_{s_i} = 0.99, \forall i$.

A Retail Case Study

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.

A Retail Case Study

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.

We 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 Newsweek (2014).

A Retail Case Study

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 (Newsweek (2014)).

Firm 1 (Target) suffered \$148 million in damages, according to the Consumer Bankers Association and the Credit Union National Association (Newsweek (2014)). Firm 2 (Home Depot) incurred a \$62 million in legal fees and staff overtime to deal with their cyberattack in 2014. Additionally, it paid \$90 million to banks for re-issuing debit and credit cards to users who were compromised (Newsweek (2014)).

A Retail Case Study

We 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): $D_1 = 148$; $D_2 = 152$.

The wealth functions are of the 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

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

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

Results

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 FBI (RILA (2014)).

Even Home Depot has expressed openness towards the sharing threat information.

Sensitivity Analysis

The network vulnerability is consistently the lowest under the NB solution concept, demonstrating the benefit of bargaining for cooperation in cybersecurity.

Additional Sensitivity Analysis

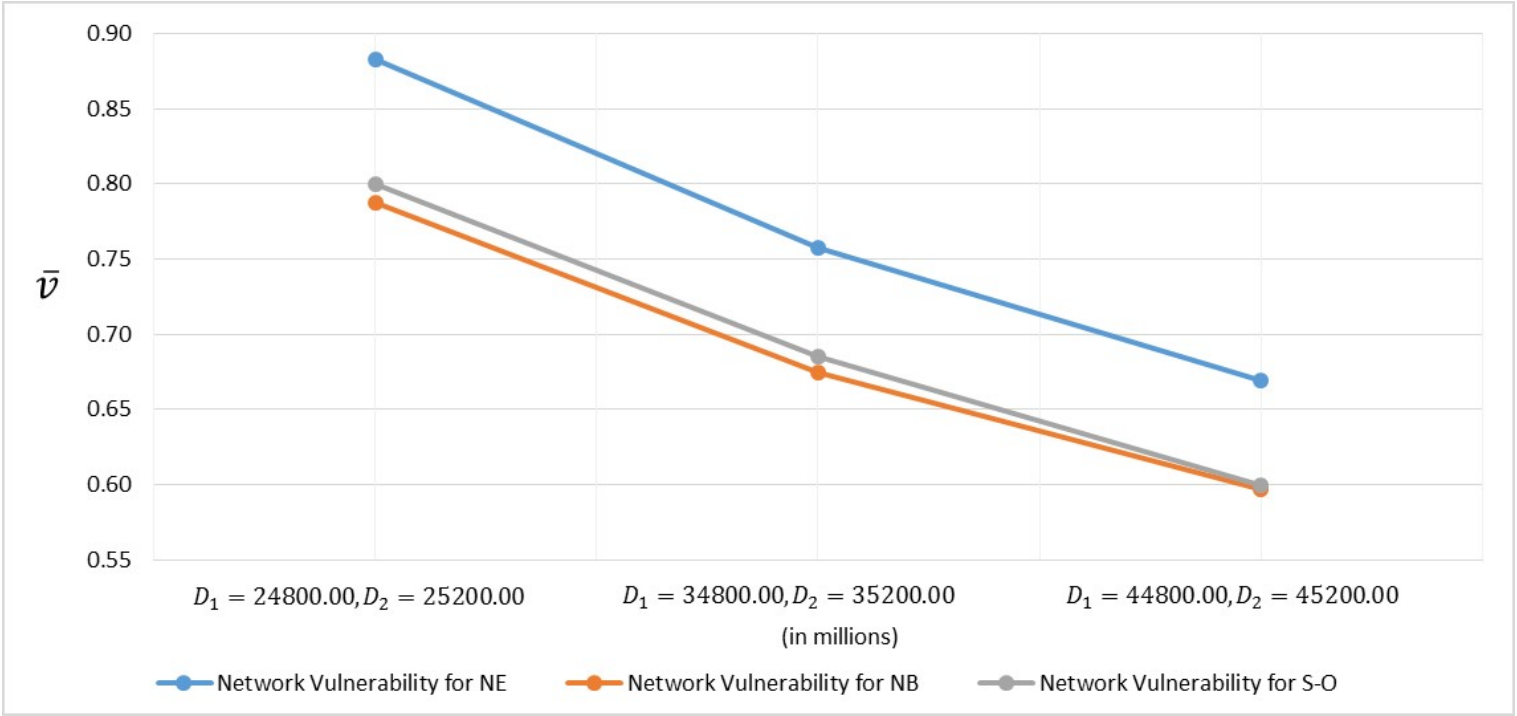


Figure: Representation of Table Showing Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O with Varying D_i Parameters $\alpha_1 = 100.00$ and $\alpha_2 = 120.00$

The network vulnerability is consistently the lowest for the NB solution, signifying the benefits of cooperation for cybersecurity.

Sharing of cyber information among these companies could be tricky, yet, nevertheless, essential.

LOGIIC, Linking the Oil and Gas Industry to Improve Cybersecurity, was established for collaboration among companies in this sector and the US Department of Homeland Security. BP, Chevron, Shell, Total and others possessing global energy infrastructure are members of the program (Automation Federation (2013)).

Based on our case studies, which describe results for different industrial sectors, 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.

Cybersecurity and Supply Chains

Figure: Supply chains are also vulnerable to cyberattacks and can serve as entre points

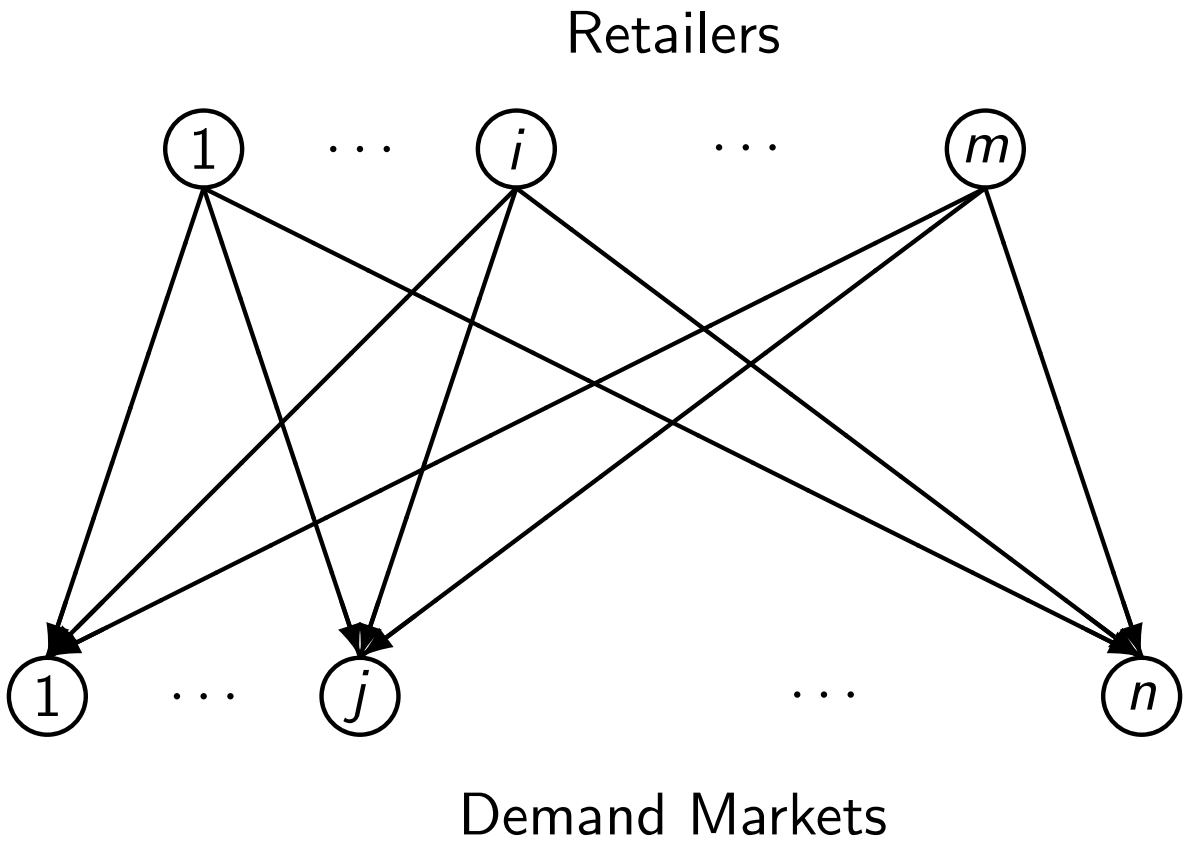


Figure: The Structure of the Supply Chain Network Game Theory Model

Some Other Examples of Our Cybersecurity Work

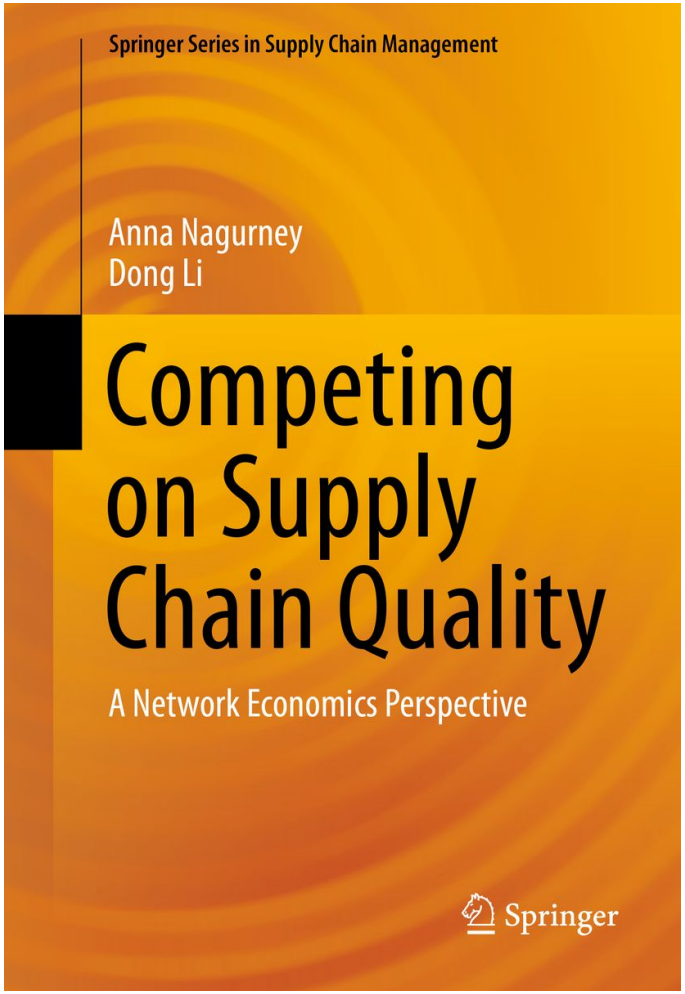
"Cybersecurity Investments with Nonlinear Budget Constraints and Conservation Laws: Variational Equilibrium, Marginal Expected Utilities, and Lagrange Multipliers," G. Colajanni, P. Daniele, S. Giuffre, and A. Nagurney, *International Transactions in Operational Research* **25(5)** (2018), pp 1443-1464.

"A Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints," A. Nagurney, P. Daniele, and S. Shukla, *Annals of Operations Research* **248(1)** (2017), pp 405-427.

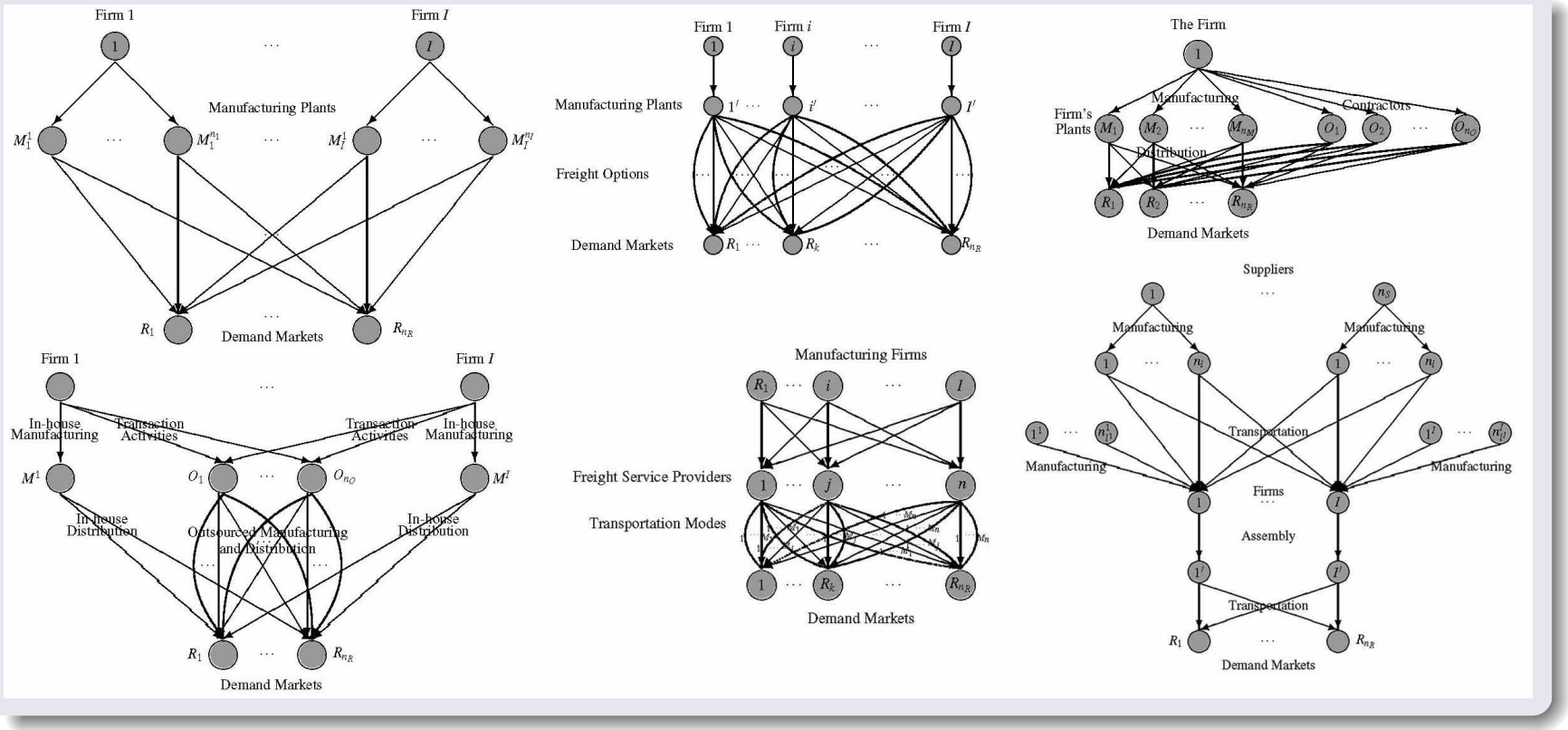
"Cybersecurity Investments with Nonlinear Budget Constraints: Analysis of the Marginal Expected Utilities," P. Daniele, A. Maugeri, and A. Nagurney, in: *Operations Research, Engineering, and Cyber Security*, Th.M. Rassias and N.J. Daras (Eds.), Springer International Publishing Switzerland (2017), pp 117-134.

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

Our Latest Supply Chain Book



In the book, we present supply chain network models and tools to investigate: information asymmetry, impacts of outsourcing on quality, minimum quality standards, applications to industries such as pharma and high tech, freight services and quality, and the identification of which suppliers matter the most.



Envisioning a New Kind of Internet ChoiceNet

Envisioning a New Kind of Internet – ChoiceNet

We were one of five teams funded by the US National Science Foundation as part of the Future Internet Architecture (FIA) project. Our project: *Network Innovation Through Choice* envisions a new Internet architecture *ChoiceNet*.

Team:

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

Some Weaknesses of Current Internet

- **The Internet architecture lacks 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**.

- **Routing of messages may be inefficient** and **the capacity is not well-utilized in the network**.

ChoiceNet Foci: *Choices* and *Network Economics*

Choice criteria can include:

- **privacy**
- **minimization of risk**
- even **reducing environmental impact**.

Transparency is associated with ChoiceNet and having more refined routing options **can also assist in cybersecurity**.

ChoiceNet Principles

Competition Drives Innovation!

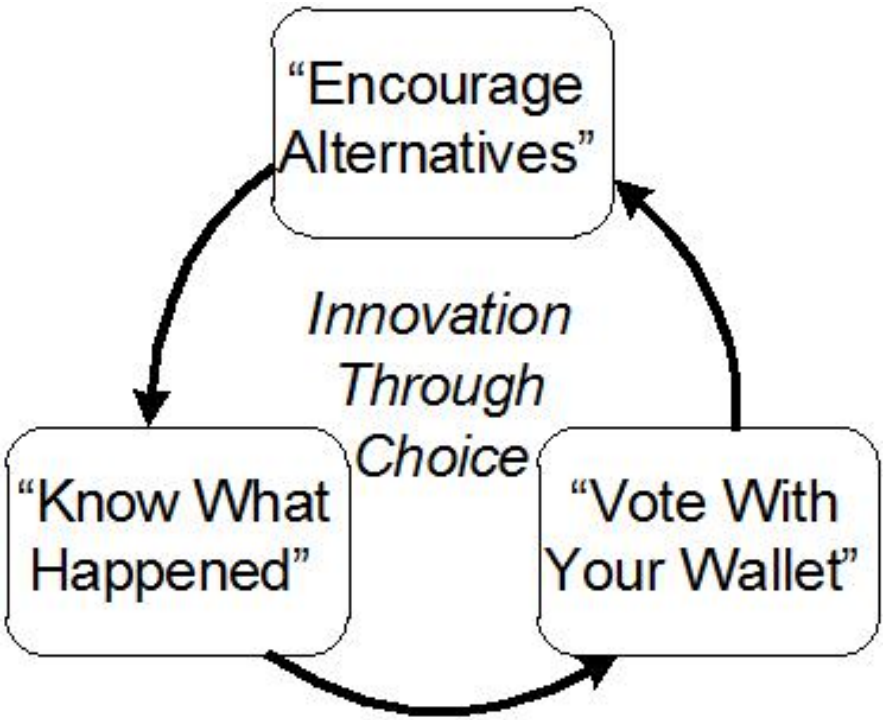
Services are at core of ChoiceNet
("everything is a service")

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 / economy plane enables new business models in the Internet**

– Very dynamic economic relationships are possible

– All entities get rewarded.

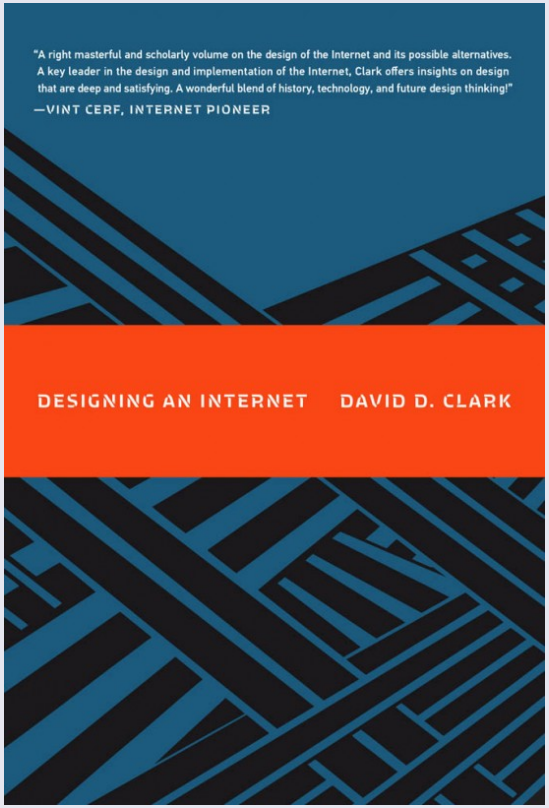
• **Examples**

– Movie streaming

– Reading a newspaper online in a coffee shop (short-term and long-term contracts)

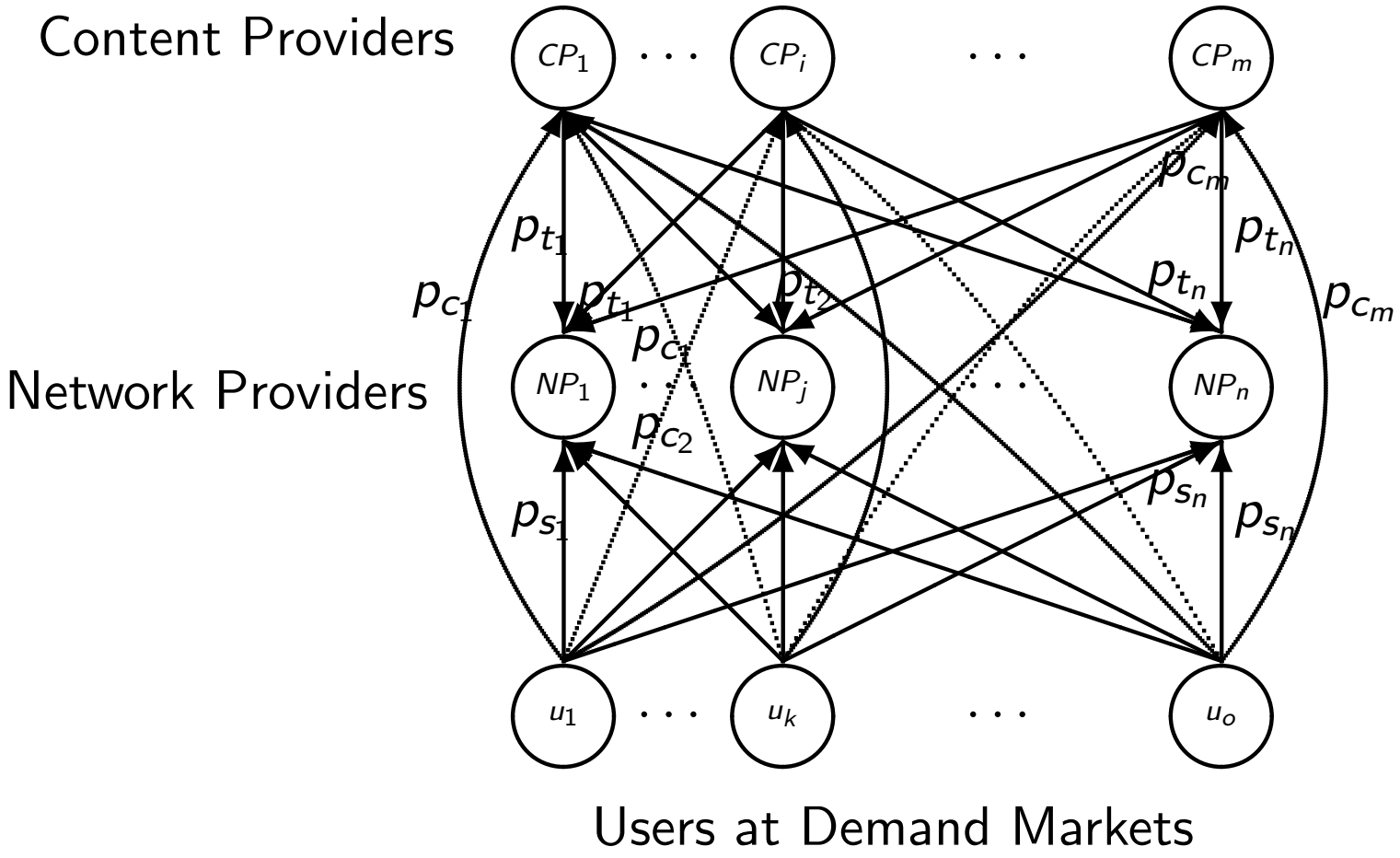
–Customers as providers.

Designing an Internet



The book by David Clark, a developer of the Internet, cites our paper: "ChoiceNet: Toward an Economy Plane for the Internet," Wolf, Griffioen, Calvert, Dutta, Rouskas, Baldin, and Nagurney, *ACM SIGCOMM Computer Communication Review* **44(3)** (2018), pp 58-65.

Game Theory Models - Flow of Content and Payments



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

Summary

Summary and Conclusions

- We have shown, beginning with transportation networks, the importance of capturing behavior of users of critical infrastructure networks.
- We highlighted the Braess Paradox, in its classical setting and with increasing demand.
- We overviewed some fundamentals of variational inequality theory and then shown how it can be used to formulate Nash Equilibria.
- A spectrum of supply chain network applications from food to healthcare were highlighted, along with recent work inspired by the COVID-19 pandemic.
- We then turned to cybercrime and cybersecurity and present a model of perishable products in finance and also different behavioral concepts associated with decision-making regarding cyver security investments.
- Discussed a new way of envisioning the Internet - ChoiceNet.

THANK YOU!

For more information, see:
http://supernet.isenberg.umass.edu