Network Resilience

Sanjeev Goyal

Christ’s College
University of Cambridge

Latsis Symposium 2012
Zurich
Frank’s `RESEARCH QUESTION’

Can economics as a scientific discipline that must extricate itself from its current conceptual crisis, benefit from concepts, methods and insights developed in other disciplines, notably the natural sciences?

**View:** Economists have been successful at developing concepts for the study of interaction in small groups (game theory) and interaction among large groups (competitive markets and general equilibrium).

Networks contain large numbers of actors, interaction is local, personalized and overlapping.

Questions of great practical relevance – systemic risk, contagion, peer effects, social norms and values, political participation, social movements – are network phenomena.
Research Question

-- Analysis of many actors located within large networks strains the plausibility of delicate chains of reasoning in game theory.
-- ‘Local' interaction’ makes anonymous competitive analysis implausible.

Tension between large and small key to understanding behaviour at intersection of markets and networks.

Networks is an ambitious inter-disciplinary endeavour:

**Economics** (incentives and mechanism design),
**Sociology** (core ideas in social networks)
**Statistical physics** (approximations in large systems)
**Computer science** (computational complexity, algorithms)
**Mathematics**: probability theory, graph theory, linear algebra.
1. Introduction

Connections between individuals facilitate exchange of goods, services and information but are costly to set up and may expose nodes to threats faced by others.

Examples:

Transportation: node/link failure blocks flows.
Crime: capture of node triggers others…
Computer networks: viral attacks/botnet herders.
Finance: links smooth shocks, systemic risks.
Epidemiology: vaccination and interaction
Research Questions

1. Optimal attack strategy: who to target.
2. Network design to minimize damage.
3. Random versus strategic attack.
4. Optimal defense & network design.
5. Centralized vs. decentralized decisions: trade-offs and role of policy intervention.
Modelling Issues

Three dimensions

- Nature of shocks: *strategic vs. random*
- Nature of attack: *contagion vs. static*
- Decisions: *centralized vs. decentralized*

Capture different applications… and trace out an ensemble of models.
Examples

<table>
<thead>
<tr>
<th>Planner/Designer</th>
<th>Random attacks</th>
<th>Intelligent Adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decentralized choices</td>
<td>Infrastructure vs. nature</td>
<td>Criminal gangs vs. police Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Vaccination vs. virus</td>
<td>Airports vs. terrorists</td>
</tr>
<tr>
<td></td>
<td>Inter-bank networks</td>
<td>Computers vs. hackers</td>
</tr>
</tbody>
</table>
Framework

- **Two/many players**: network designer $D$ and adversary $A$.
- **Designer(s) choose(s)** network and defence on nodes.
- **Attack**: Adversary allocates resources/random attack.
- **Technology of shocks**: shock affects a node and spread via connections

Strategic adversary: study equilibrium of game of conflict
Random attack: study optimal networks and defence.
2. Contagion and Resilience
Goyal and Vigier 2010

*Single Designer* chooses network/allocates D defence. *Adversary* allocates resources across nodes of network.

**Two key features:**

1. Contests: Attack/defence probability of elimination
2. Contagion: attack spreads through links in network
Consider a Peer-to-Peer network: BitTorrent, Kazaa or eMule. The returns from network are increasing in the number of users.

Online criminals, such as hackers and `botnet' herders take the topology and security of a P2P network as given when they attack hosts taking part in the network.

One of the most dangerous threats are self propagating malicious software called contagious (or stealth) worms. Worms are deployed by an external attack with viruses/malware.

Deployed worms propagate by taking control of neighbouring hosts in the network. The worm attaches itself to packages of data sent between connected hosts.
Payoffs from network

Assumption 1

The payoffs from a network are given by

$$\sum_{C_i \in C(g)} f(|C_i|)$$

where $f(.)$ is increasing and convex.

E.g. $f_n(x) = \frac{x^2}{n^2}$
Contagion and Resilience

Contests

A canonical model of contests due to Tullock (1980):

Assumption A.2
Probability of successful attack on node is increasing in attack and falling in defense allocation. Marginal returns from defense and attack are falling and symmetric.
Spread of attacks

Assumption A.3:
*Attack spreads across nodes that are poorly defended.*

- E.g. threshold model: a path between two nodes $i$ and $j$ is *weak* if every node $k$ on path has defense less than some threshold.
Payoff: $4 f(1)$
Payoff: \( f(8) \)
Contagion and Resilience Payoffs

Given a network $g$, defence $d$ and attack strategy $a$, A.2 and A.3 yield a probability distribution on networks:

$$P(g'| g, d, a)$$

The expected rewards to designer are:

$$\sum_{g'} P(g'| g, d, a) \sum_{C_k \in C(g')} f(| C_k(g') |)$$

We study zero sum games.
Pure Design Problem

**Theorem 1**

Assume zero defense budget. In equilibrium

-- adversary targets at most one node in each component
-- Designer chooses network with equal size components
-- # components grows (and size falls) in adversary budget.

**Remark:** If attack is random, optimal network consists of fewer and unequal components.
Effects: adversary budget

\( \alpha = 2 \) \( a = 2 \) \( k = 4 \)

\( \alpha = 2 \) \( a = 4 \) \( k = 8 \)
Effects of Convexity

$n=24 \ \alpha=2 \ \alpha=2: \ \ k=4$

$n=24 \ \alpha=3 \ \alpha=2: \ \ k=3$
Contagion and resilience
Random vs. strategic attack

**Example:** Fix $a=1$. Random attack $q=a/n$. Independent and identical across nodes.

As $n$ gets large, optimal network is connected. Payoff to designer is

$$[1 - 1/n]^n = 0.38$$

Under intelligent attack resilient network contains two equal components and payoff is 0.25, irresp. of number of nodes.

Thus # components differ: 1 vs. 2. Mistaking intelligent adversary for random attack leads to zero payoff!
Design and defence

Theorem 2

Consider connected network. Suppose budgets of defense and attack are small relative to number of nodes. Then it is optimal to have a star network and assign all defense to hub node. The optimal attack strategy is to target the hub with all resources.
Attack tolerance in networks?

Empirical work on networks has highlighted the salience of hub-spoke structures.

Albert, Jeong and Barabasi (2000, Nature): hub-spoke networks are robust to random attacks but vulnerable to strategic attacks.

Our work draws attention to value of hub-spoke architectures: in a world with limited defence and contagion. Successful defence of a few hub nodes contains the spread of attacks through the network.

Our work complements the work in physics: provides an efficiency based foundation for the salience of hubs in real world networks which face adversaries.
Proof: General Ideas

1. In hub-spoke network, optimal to protect/attack hub: convex f(.) and large n.

2. Payoff in hub-spoke network is bounded below by

\[ \chi = \frac{d}{d + (a-x)} f(n-x) \]

3. Single hub better than many hubs: many hubs allows adversary to mimic conflict in star.
   Key: in hub-spoke network survival network is bang-bang. In multiple hubs distribution is smoother. But f(.) is convex, so payoff higher in single hub.

4. K core-periphery network better than other networks with K protected nodes: minimizes attack contagion
What happens with large resources?

• In the result above, a key assumption is that resources are scarce relative to nodes. If attack resources are large relative to nodes then protecting the hub would be to no avail, if all spokes are eliminated.

• Indeed, with large resources, dense networks and diffused defence may be optimal.
HIGH DEFENCE BUDGET: $n=4$, $d=4$, $a=1$

DISPERSED DEFENCE

Prob. 1

Prob. 1/2

Prob. 1/2
HIGH DEFENCE BUDGET: n=4, d=4, a=1
DENSE NETWORKS
4. Concluding Remarks

Connections facilitate the exchange of goods, resources and information but links are costly and they also expose an individual node to threats faced by other nodes.

We studied research questions:

1. Optimal attack strategy: who to target
2. Network design to minimize damage.
3. Random versus strategic attack.
4. Optimally combine defense & network design
5. On-going work

1. Competing for security: Higher security diverts attack to other nodes… and so individuals invest too much in security and exhaust all surplus.

Open problem: how does network location affect security choice? How does optimal centralized design compare to optimal design when security is decentralized?
5. On-going work

2. Decentralized security and linking: In many applications, agents form links and also choose security. E.g., Banks, social interaction, travel and vaccination.

Open problem: what is the emerging network and how secure are they? What is the role of public policy?
References

S. Goyal and A. Vigier (2010), Robust networks.
M. Dziubinski and S. Goyal (2012), Network defence and design.
Y. Bacharach, M. Draeif and S. Goyal (2011), Competing for security
S. Goyal and J. Kovarik (2012), Network resilience: an empirical study
D. Kovenock and B. Roberson (2011), Conflicts with Multiple Battlefields.
Milind Tambe (2010), *Security and Game theory.*