Threat Networks and Threatened Networks:
Social Network Analysis for Counter-Terrorism

Q1: What are the problems?

- Extending basic research in the science of network analysis to improve military and intelligence approaches to attacking and defending warfighting networks
- Development of improved tools for conducting basic research in the analysis of critical warfighting networks and for the disruption of opposing networks

Q2: Why care?

- Scientific: New Laws
- Practical: Intentional attack vs. Random attack, Immunization (ex: SARS)

Q3: What do we do?

Collaborators: S. Havlin / L. Braunstein / S.V. Buldyrev / R. Cohen / G. Paul / S. Sreenivasan

* * *

THREE TAKE HOME MSGS:

Msg #1: 6 degrees of separation

versus

100 degrees of separation

Msg #2: Efficient immunization strategies

Random or Targeted (How?)

versus

“Acquaintance immunization" (No prior knowledge needed)

Msg #3: On the threshold of uncovering new principles and applications of networks.

Financial support: Office of Naval Research

Examples of Real World Problems

- **In terror or intelligence networks:**

efficiency
versus
secrecy

- **In vaccination strategy:**

risks of vaccination
versus
safety

- **In information warfare contexts:**

cost of spreading information
versus
need to make sure the right people get the messages

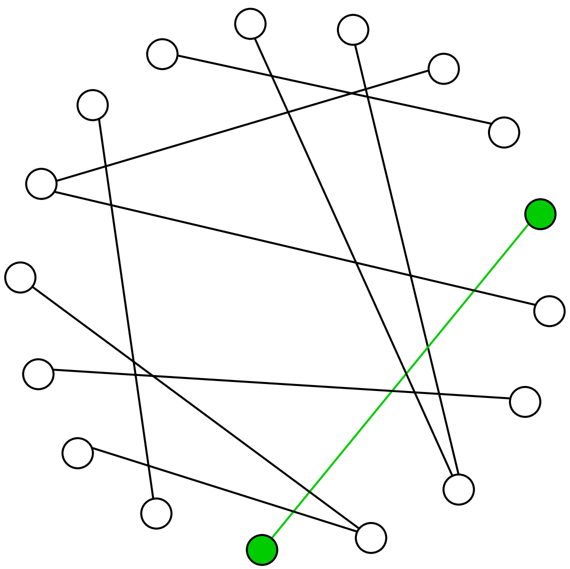
- **In command and control contexts:**

creating “all channel networks”
(linking everyone to all information and enabling everyone to communicate)
versus
information overload and “babble” as well as problems of information control

3 kinds of networks

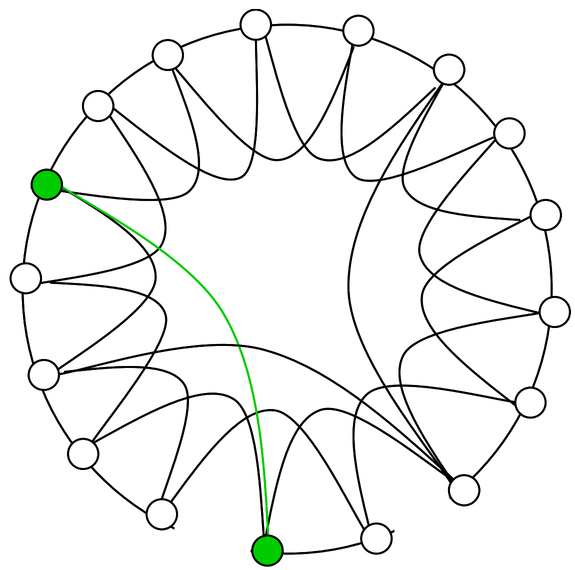
Classic

Erdős-Rényi

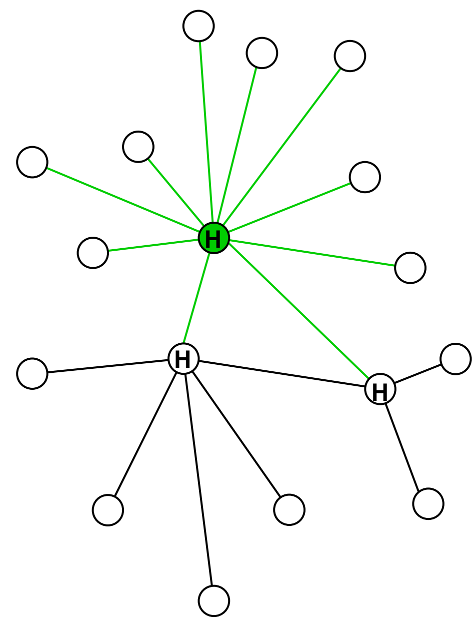


Modern

Small world:
Watts-Strogatz



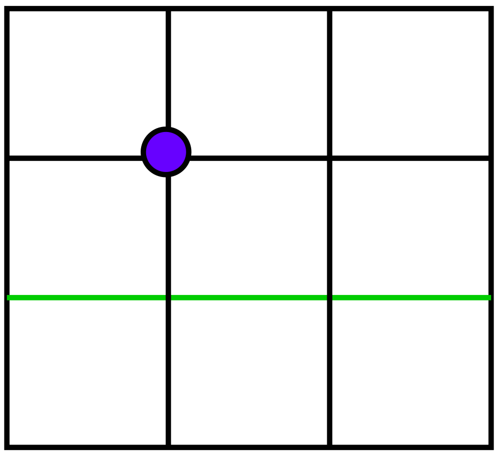
Scale free:
Barabási-Albert



Real world example of scale free network: Airline route map

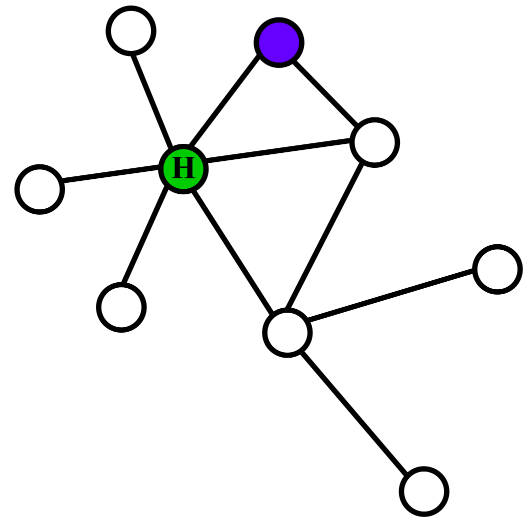
Resilience to attack

"Old"



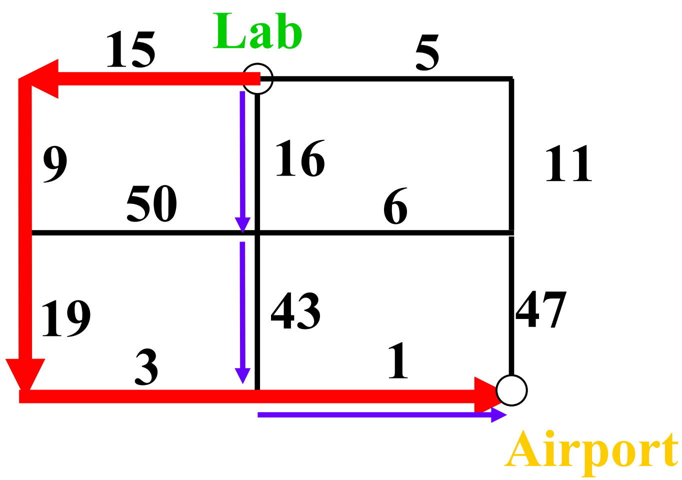
- Random attack:
  must remove 50% to destroy
- Intentional attack:
  must remove 1% to destroy

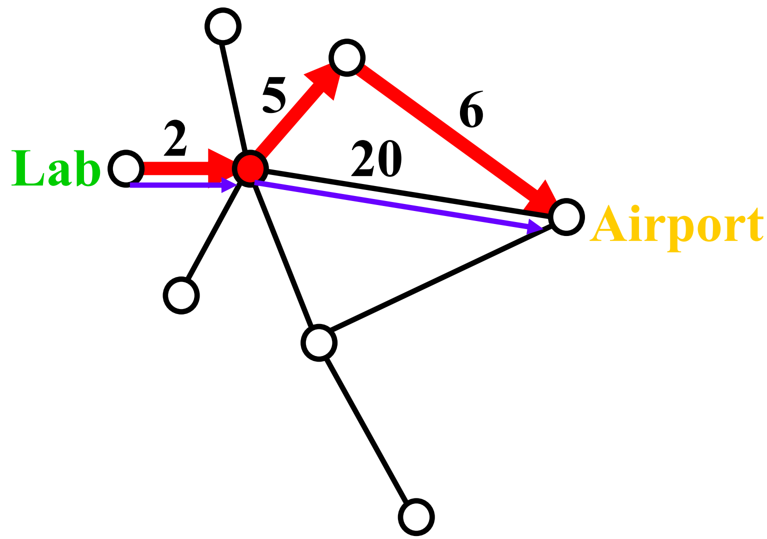
"New"



- Random attack:
  must remove 99% to destroy
- Intentional attack:
  must remove 1% to destroy

Optimal Path: Minimize total "cost"





For this example:

Shortest path: 3 (cost = 60)

Optimal path: 5 (cost = 47)

Shortest path: 2 (cost = 22)

Optimal path: 3 (cost = 13)

Generally:

Shortest path = $N^{0.50}$

Optimal path = $N^{0.61}$

$N^{0.50} < N^{0.61}$

ex: $(10^6)^{0.50} < (10^6)^{0.61}$

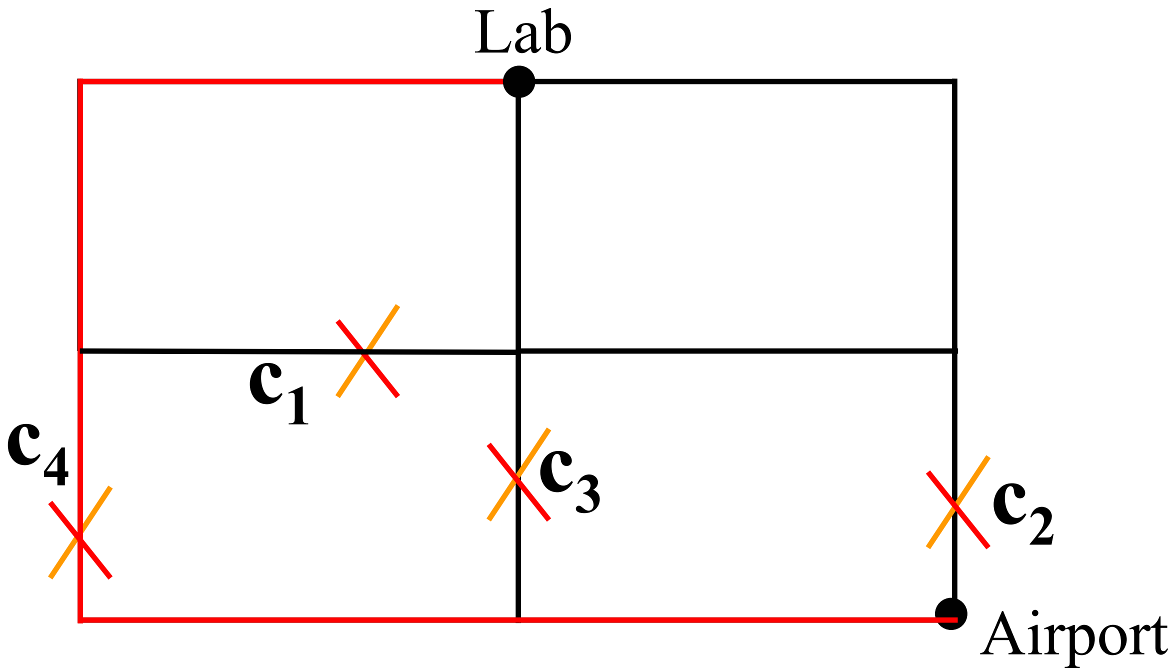
Shortest path = Log N

Optimal path = $N^{1/3}$

Log N << $N^{1/3}$

ex: $N=10^6$, $\log 10^6 \ll (10^6)^{1/3}$

Bombing algorithm



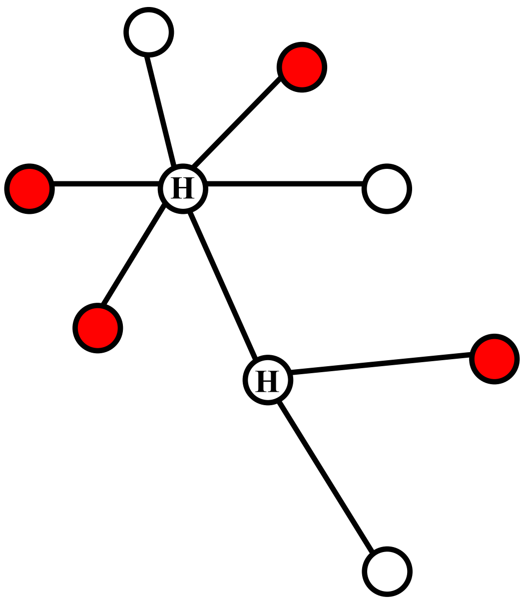
Brute Force: Calculate cost for each path

Classic: If $c_1 > c_2 > c_3 > \cdots$, remove c_1, then c_2, …

Modern: "bomb" randomly chosen links.

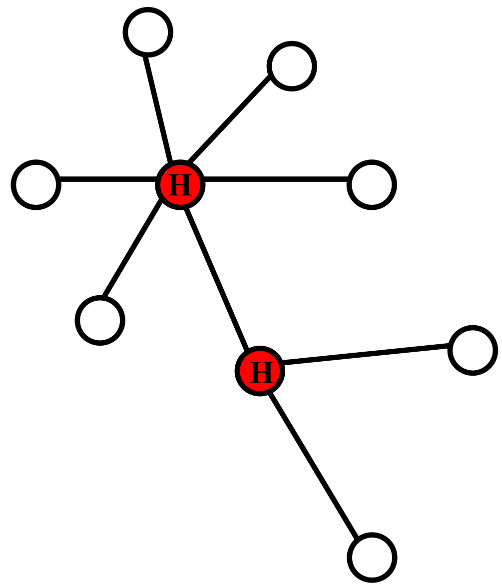
An efficient immunization strategy

Immunize at random:



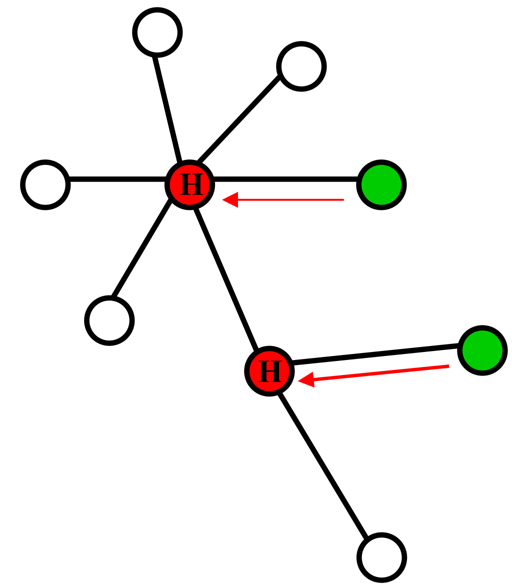
Need very high fraction

Target the hubs:



Very low fraction
But need to know the hubs

Choose at random
Immunize the neighbor



Very low fraction
Advantage: No prior information needed

The future projects

Quantifying and modeling properties found in real networks

#1. Clustering of nodes

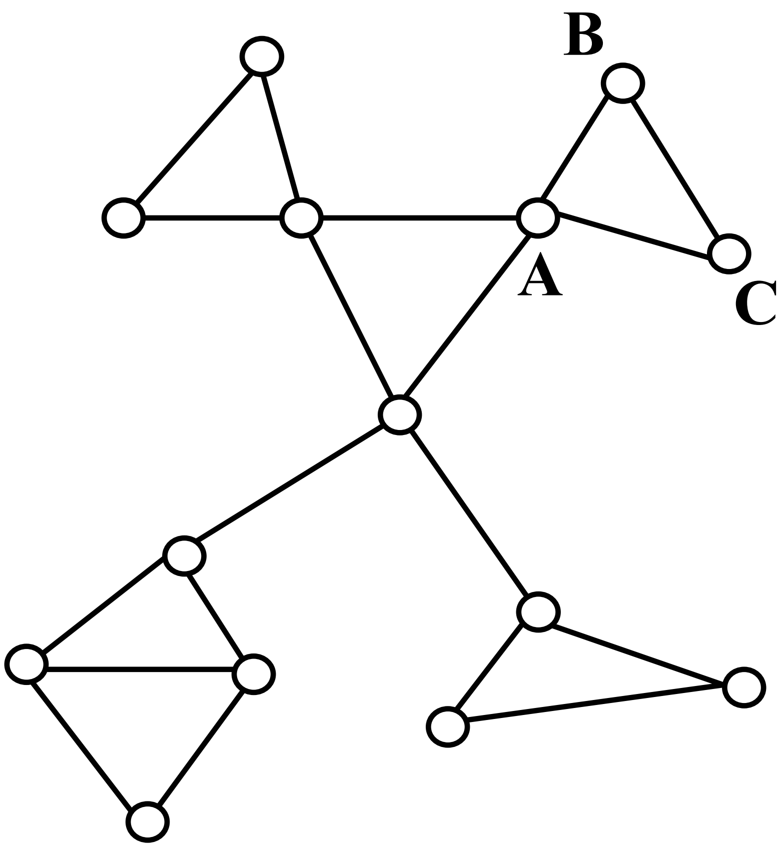
#2. Correlations of high degree nodes

#3. Nodes have different infection probabilities

How these properties affect immunization strategies and resilience?

Future project #1: Clustering of nodes

"My friend's friends are also my friends"



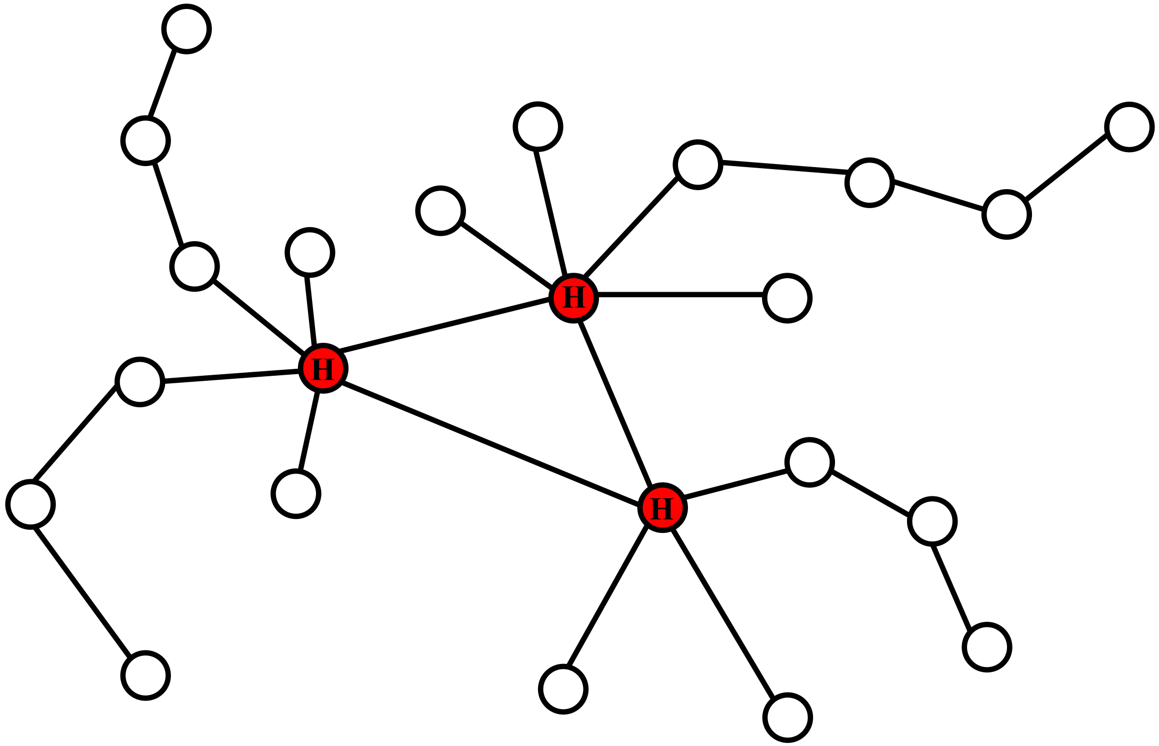
- ✓ **Known for real networks – particularly social networks**
- ? **How clustering affects resilience and immunization strategy?**

Future project #2: Correlations of high degree nodes

"If I have many friends then my friends have many friends"

Hubs hang out with other hubs ("Rich intermarry")

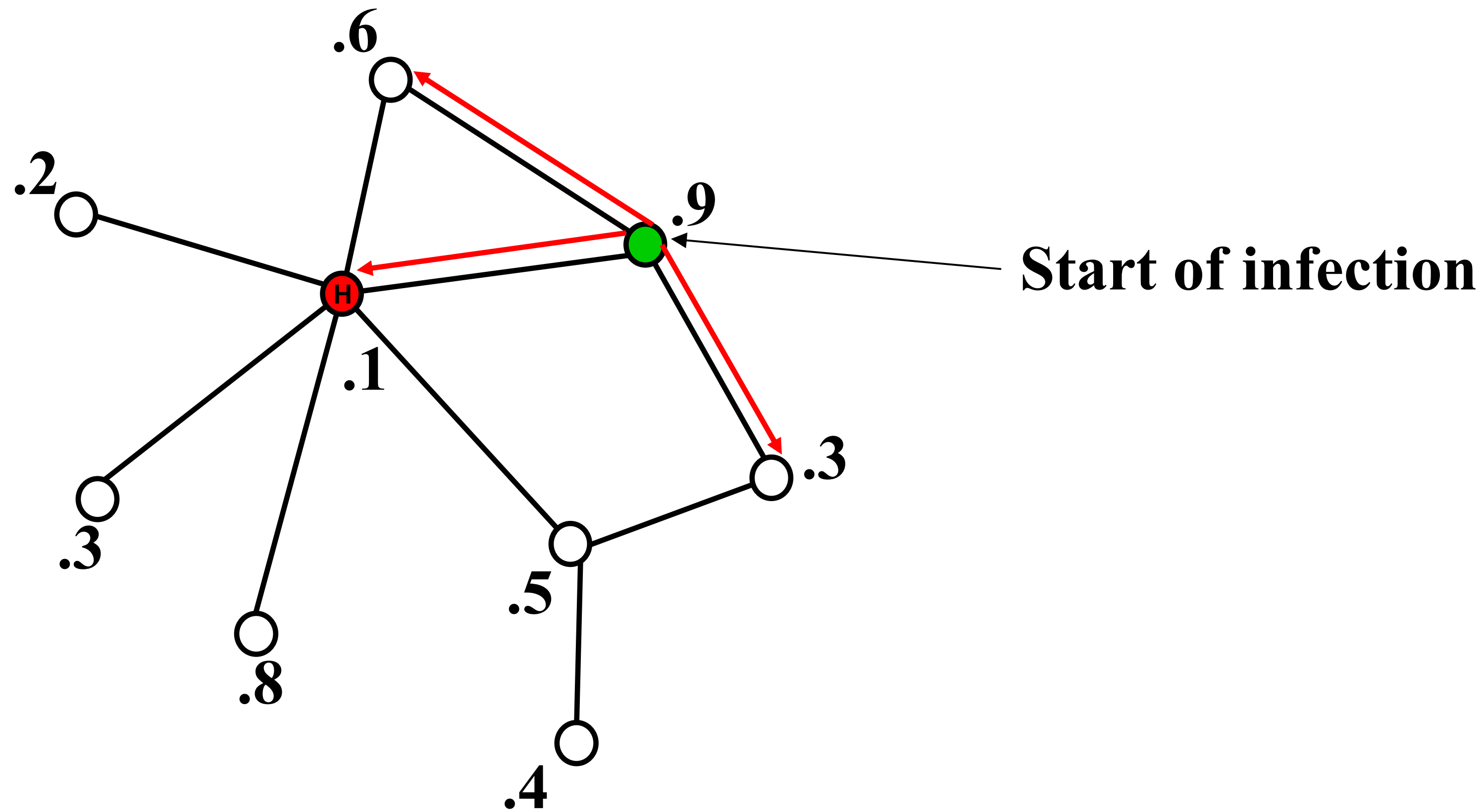
Non-hubs hang out with other non-hubs ("Poor intermarry")



✓ **Known for real network e.g. computer networks, social networks.**

? **How degree correlations affect resilience and immunization strategy?**

Future project #3: Nodes have different infection probabilities



✓ex: SARS (some people are super-infectious sources, some people are not)

? Effect on immunization strategies?

Threat Networks and Threatened Networks:
Social Network Analysis for Counter-Terrorism

Q1: What are the problems?

– Extending basic research in the science of network analysis to improve military and intelligence approaches to attacking and defending warfighting networks
– Development of improved tools for conducting basic research in the analysis of critical warfighting networks and for the disruption of opposing networks

Q2: Why care?

– Scientific: New Laws
– Practical: Intentional attack vs. Random attack, Immunization (ex: SARS)

Q3: What do we do?

Collaborators: S. Havlin / L. Braunstein / S.V. Buldyrev / R. Cohen / G. Paul / S. Sreenivasan

* * *

THREE TAKE HOME MSGS:

Msg #1: 6 degrees of separation
versus
100 degrees of separation

Msg #2: Efficient immunization strategies
Random or Targeted (How?)
versus
"Acquaintance immunization" (No prior knowledge needed)

Msg #3: On the threshold of uncovering new principles and applications of networks.

Financial support: Office of Naval Research