Static and Dynamic Robustness in Emergency-Phase Communication Networks

Sean M. Fitzhugh[1] and Carter T. Butts[1,2]
[1]Department of Sociology
[2]Institute of Mathematical Behavioral Sciences
University of California, Irvine

MURI AHM
May 25th, 2010

This material is based on research supported by the Office of Naval Research under award N00014-08-1-1015 as well as NSF award CMS-0624257

Outline

1. Introduction: Network robustness and disaster response
2. Methodology: How to measure network robustness
3. Results and analysis: static case
4. Dynamic robustness: Methods and results
5. Concluding remarks

Network Robustness and Disaster Response

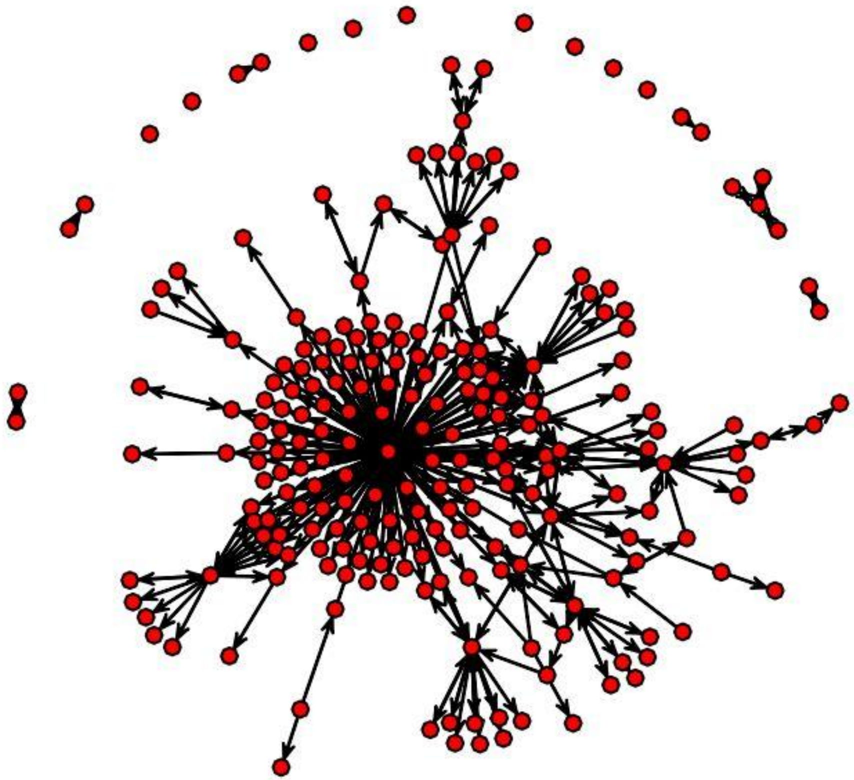
- Disaster response teams carry out complex tasks which require extensive training and planning
  - Typically operate in a volatile, chaotic environment
- Perform tasks that require substantial coordination
  - Medical response/triage
  - Resource allocation
  - Search and rescue
  - Evacuation

Network Robustness and Disaster Response

- Certain types of network structure are conducive to performing activities related to disaster response
- Locally centralized patterns of communication help large groups of individuals carry out complex tasks (Bavelas 1973)
  - To enhance efficiency, certain actors can function as “information hubs”: may serve to coordinate actions of others

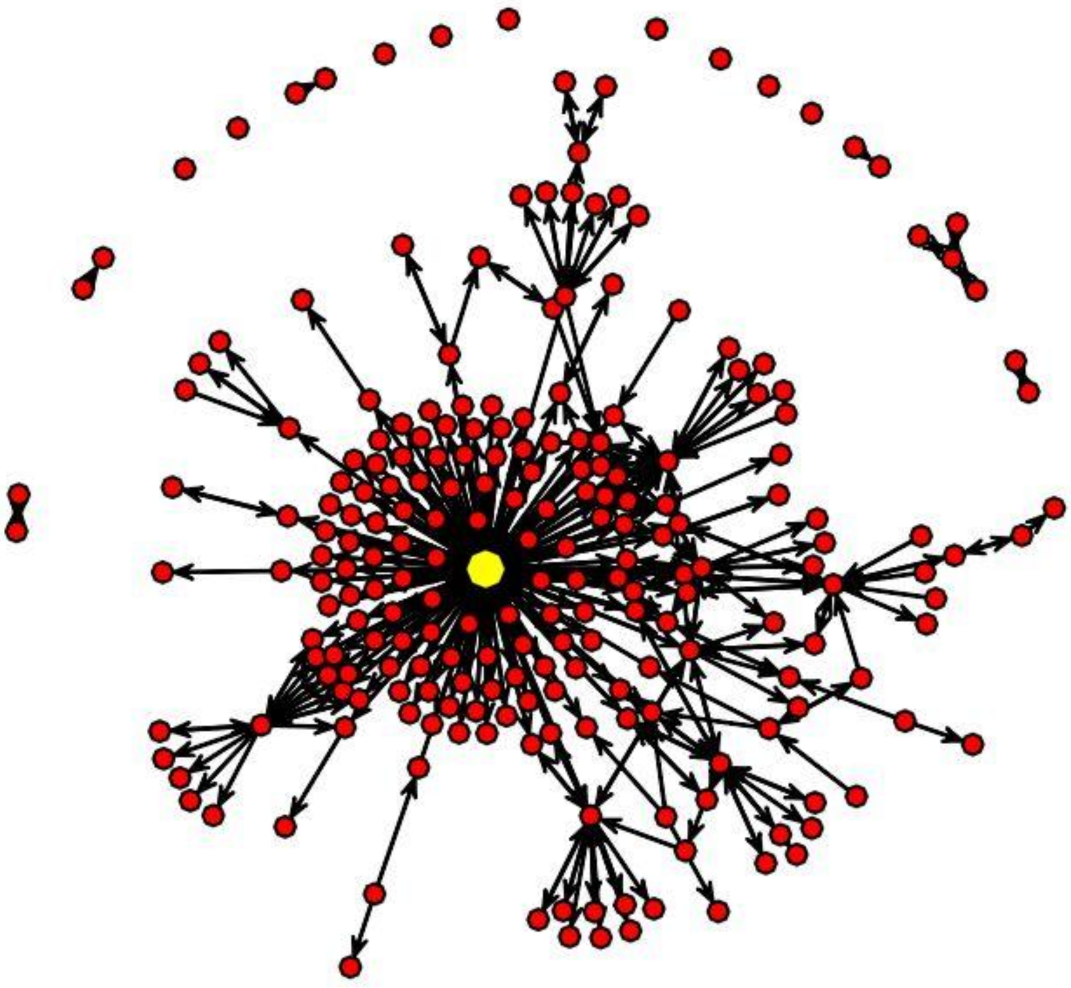
Network Robustness and Disaster Response

- Hub-dominated structure of observed WTC Radio networks is potentially efficient, but this structure creates vulnerabilities

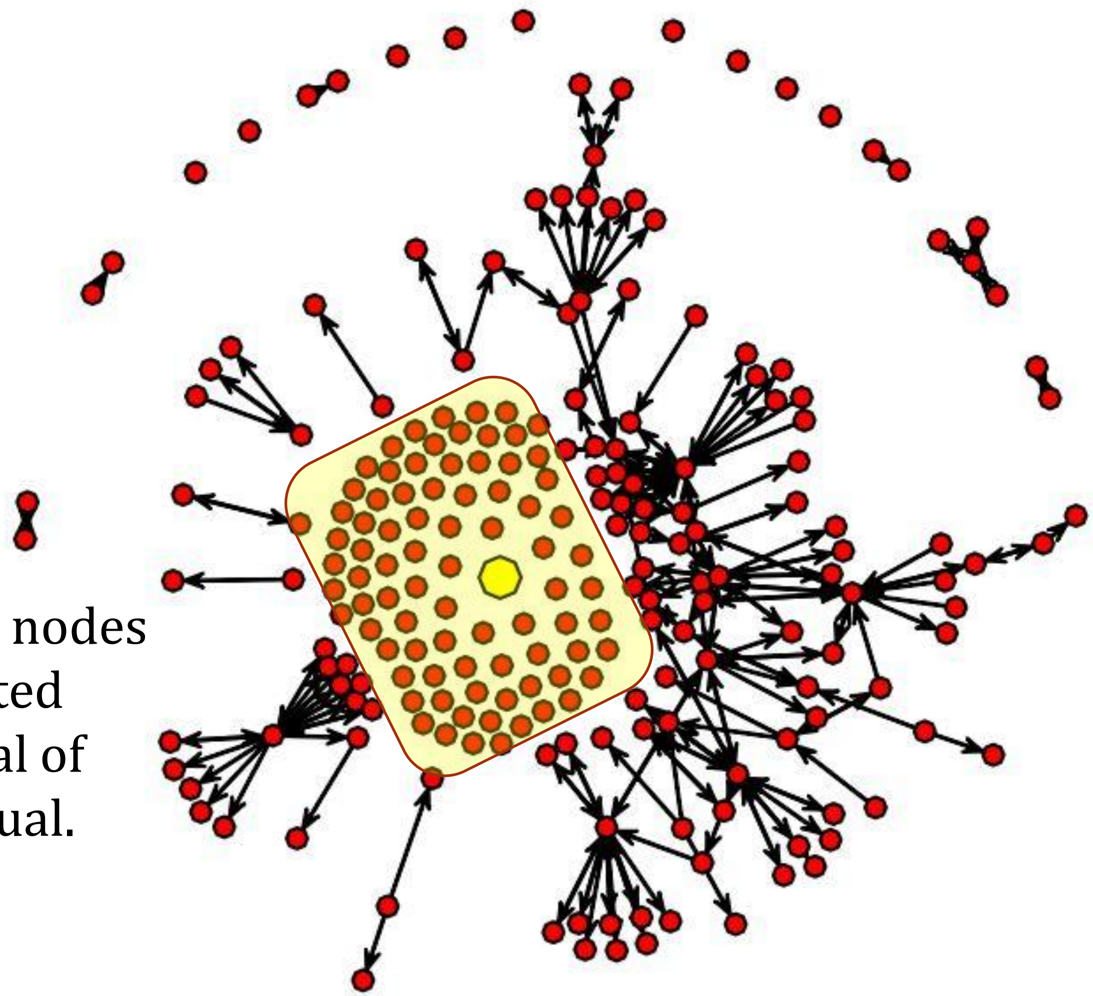


Network Robustness and Disaster Response

What happens if we eliminate the yellow node's ties?

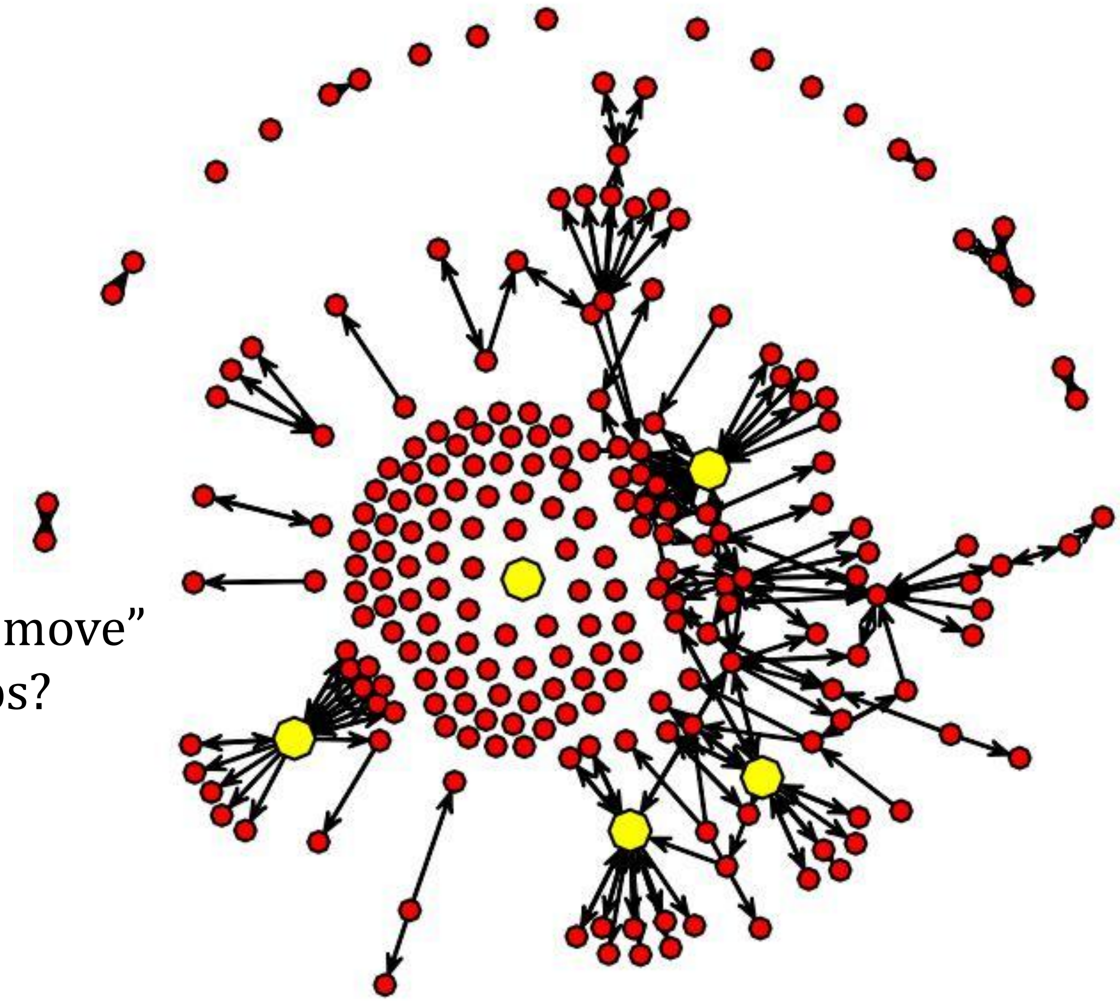


Network Robustness and Disaster Response



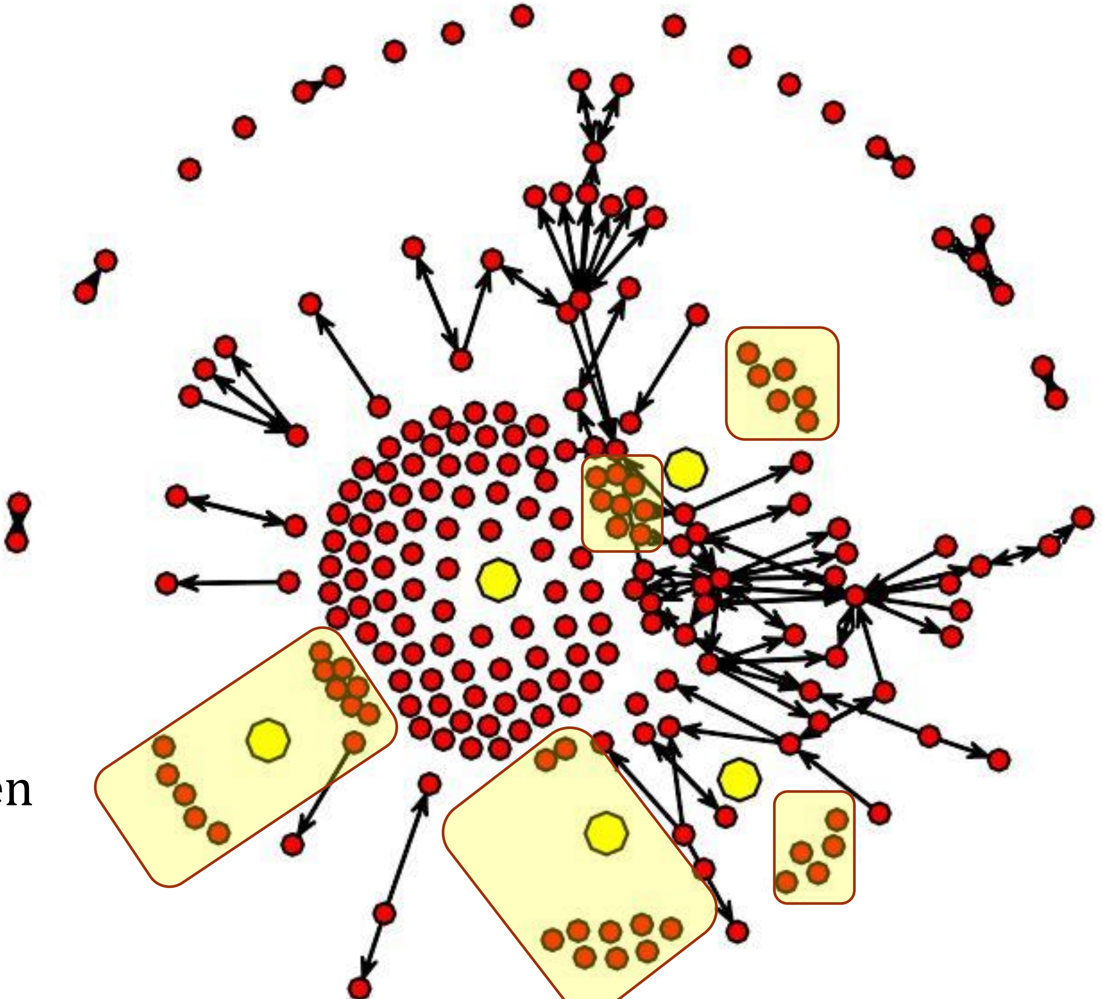
Note how many nodes have been isolated with the removal of just one individual.

Network Robustness and Disaster Response



What if we “remove” four more hubs?

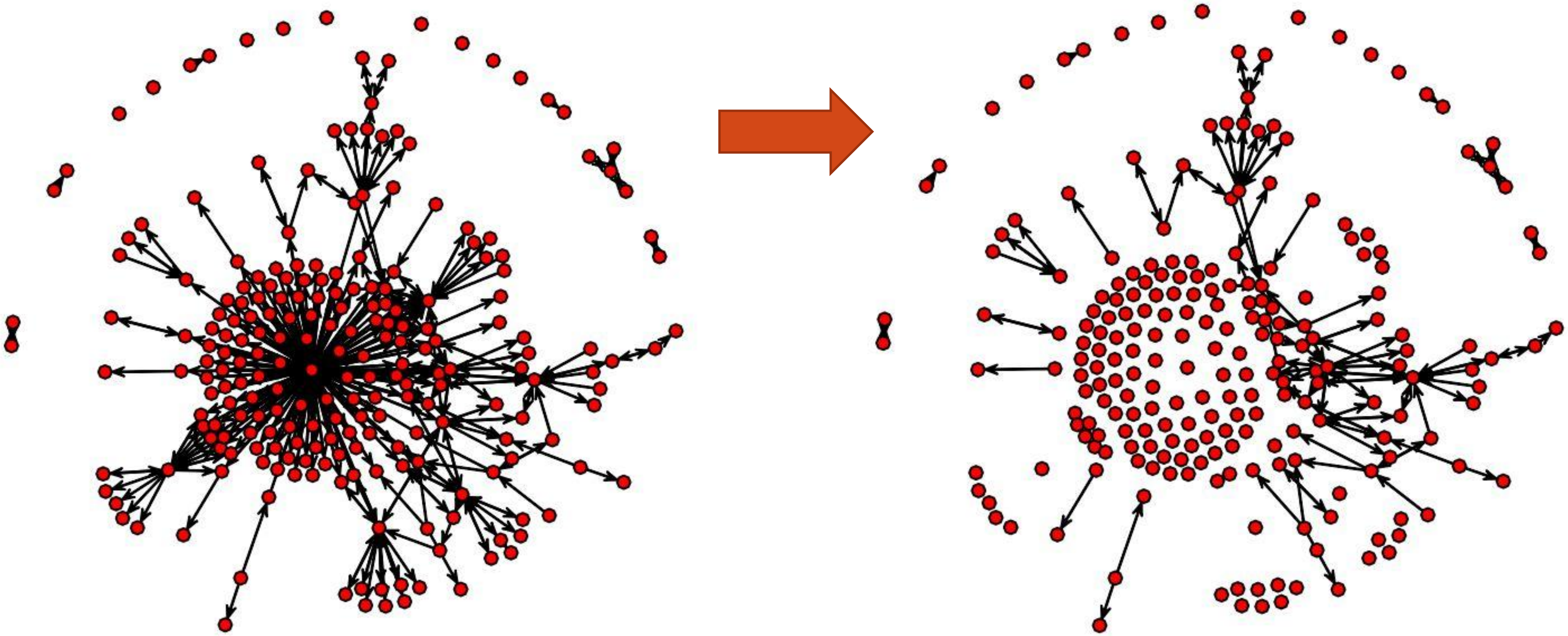
Network Robustness and Disaster Response



Dozens more nodes have been isolated.

Network Robustness and Disaster Response

- This network's information hubs are weak points



Network Robustness and Disaster Response

- Why is vulnerability problematic for these networks?
- Without effective information transmission, tasks may be carried out in an unstructured, counterproductive, or inefficient manner (Auf Der Heide 1989)
  - Worse, some tasks may be overlooked altogether

- Studying robustness patterns of communication networks allows us to see who is important in holding the network together
  - Actors with predetermined coordinative roles or emergent coordinators?

Data: World Trade Center Radio

- Seventeen radio communications networks from the World Trade Center disaster (Butts and Petrescu-Prahova, 2005)
  - Fixed-channel radio communication: groups are independent (no cross-channel radio communication), so we can think of them as separate organizations
  - Networks reconstructed from transcripts
    - Transmission from actor i to actor j is coded as an (i,j) edge
    - Actors generally treat communication as dyadic
      - Individual conversations dominate communication

Data: World Trade Center Radio

- Specialist networks: daily occupational routine involves emergency response
  - Lincoln Tunnel Police, Newark command, Newark Police, Newark CPD, New Jersey Statewide Police Emergency Network (NJ SPEN1), NJ SPEN2, WTC Police, Port Authority Trans-Hudson (PATH) Police
- Non-specialist networks: lack daily involvement in emergency response, but were in some way involved with WTC response
  - PATH radio communications, Newark operations terminals, Newark maintenance, PATH control desk, WTC operations, WTC vertical transportation, Newark facility management, WTC maintenance electric

Data: World Trade Center Radio

- Each network has a number of actors in institutionalized coordinative roles (ICR)
  - Their formal role is to coordinate the actions of others in the network
  - Transcribed labels such as “command”, “desk”, “operator”, “dispatch(er)”, “manager”, “control”, “base”
  - Manage a variety of roles in these networks: assisting searches for personnel, advising units on traffic/closures, coordinating equipment/EMT/personnel distribution, forwarding information

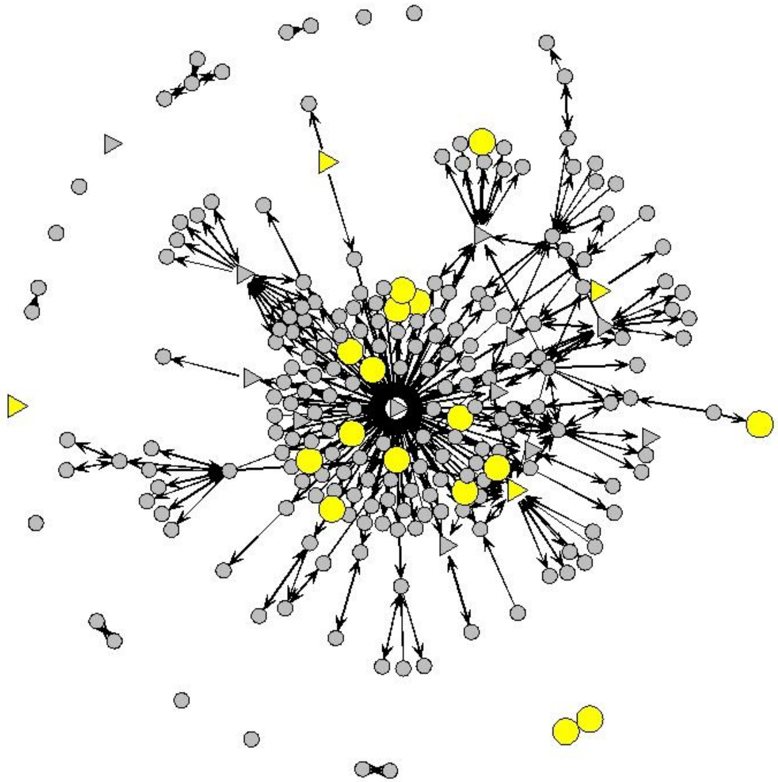
- Will ICRs operate in their formal, institutionalized roles or will others adopt those roles?

How to Measure Network Robustness

- Test the robustness of a network by subjecting it to various “attacks” (not literal attacks)
  - Remove nodes from the network and see how well it holds up
- Two basic sequences of node failure: random and degree-targeted
  - I also selectively target ICRs to assess their role in holding the network together (leads me to use four total variations of sequential node failure)
  - Remove nodes until none remain in the network

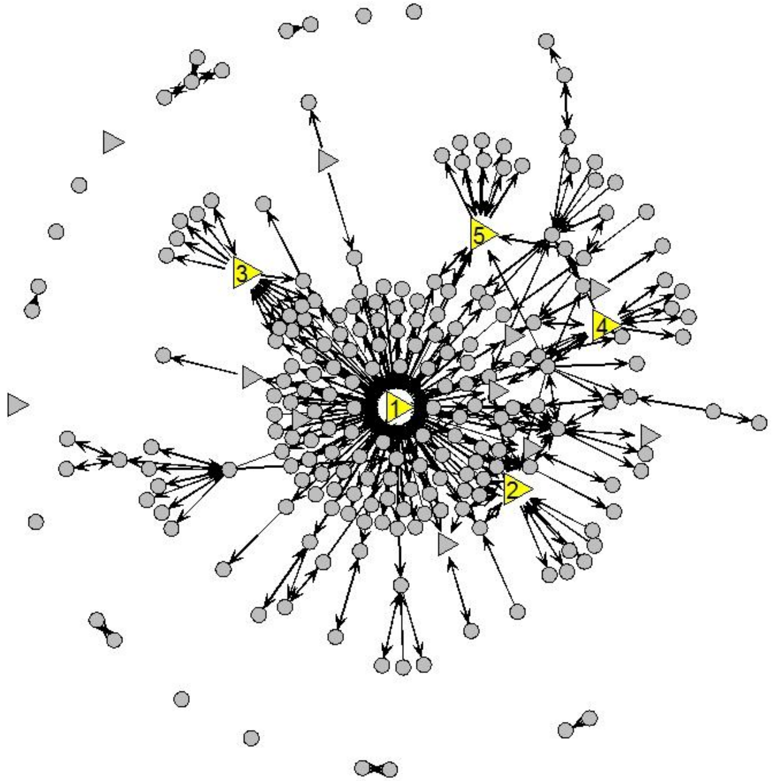
How to Measure Network Robustness

- Random failure: remove nodes at random



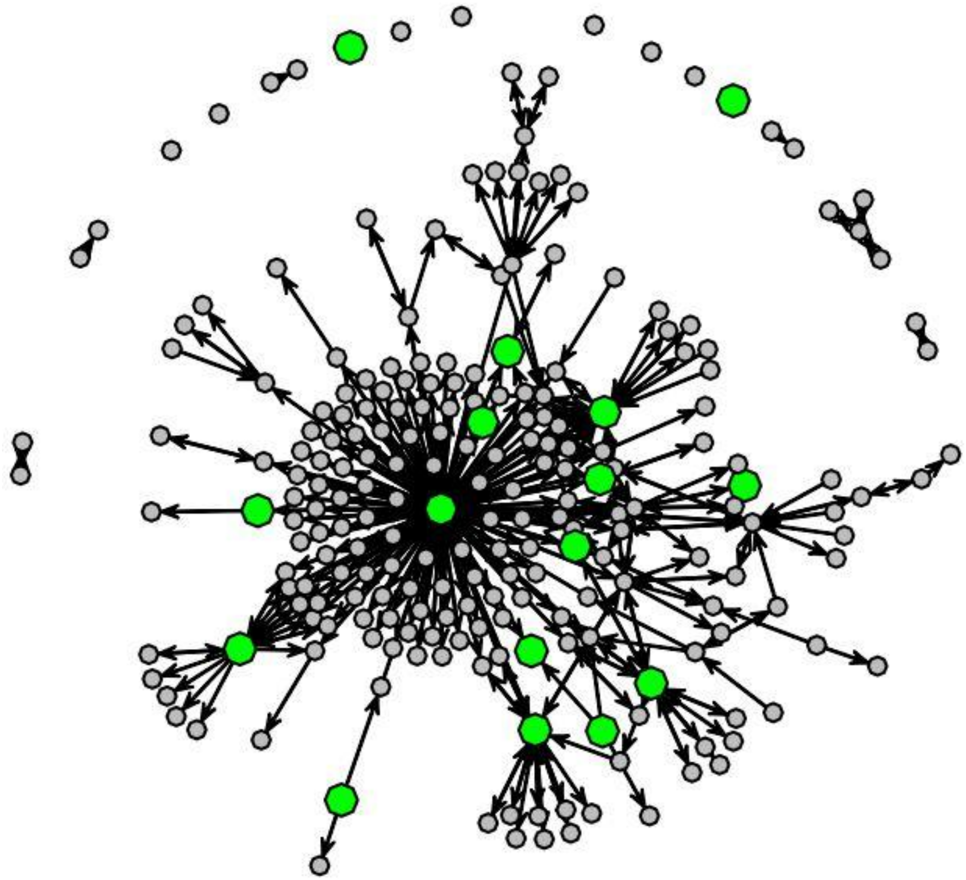
How to Measure Network Robustness

- Degree-targeted failure: remove nodes in sequential order according to degree



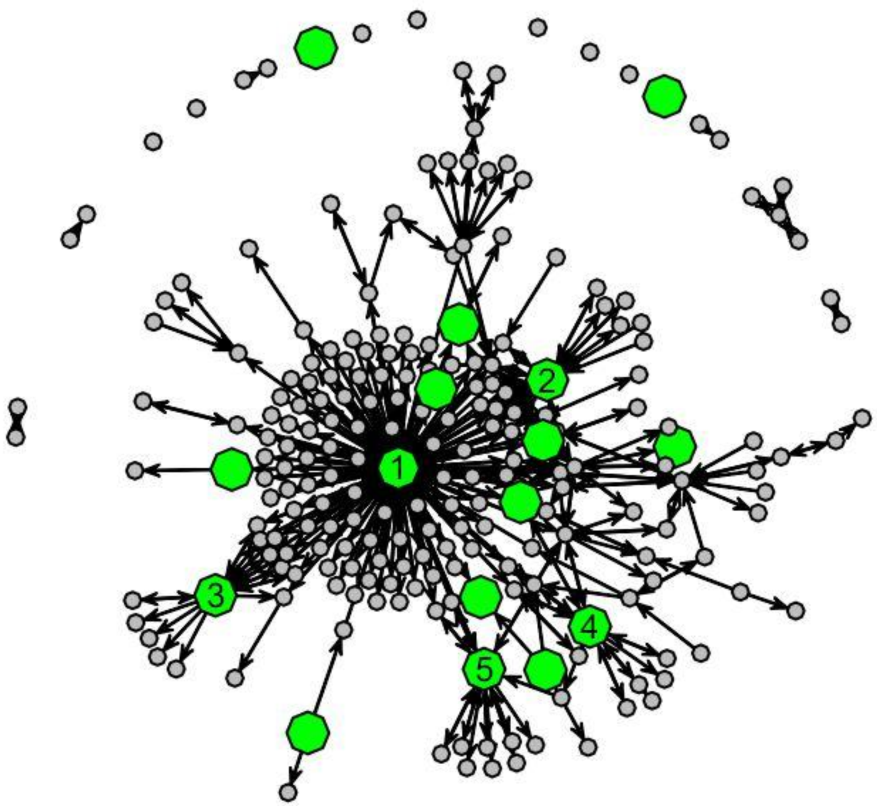
How to Measure Network Robustness

- Random failure targeting ICRs: remove ICRs at random, followed by random removal of remaining nodes

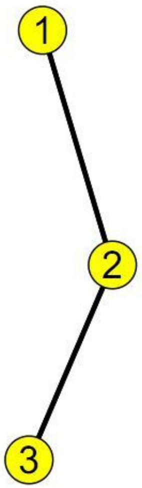


How to Measure Network Robustness

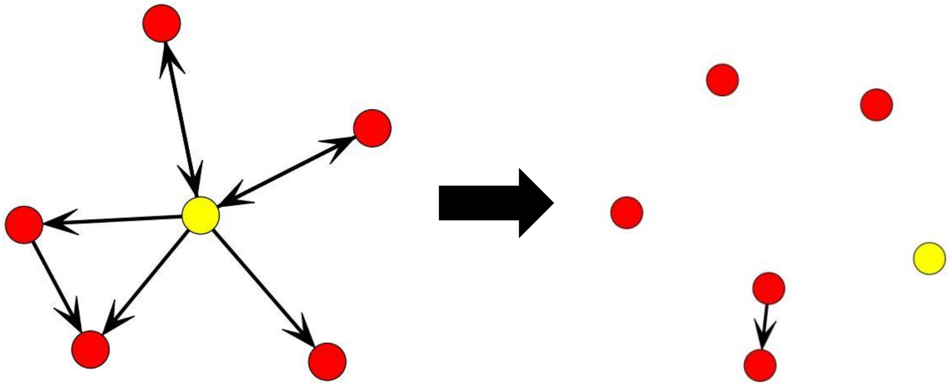
- Degree-targeted failure targeting ICRs: remove ICRs in sequential order according to degree, followed by sequential removal of remaining nodes



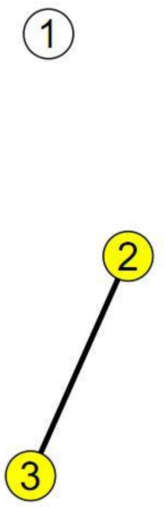
How to Measure Network Robustness



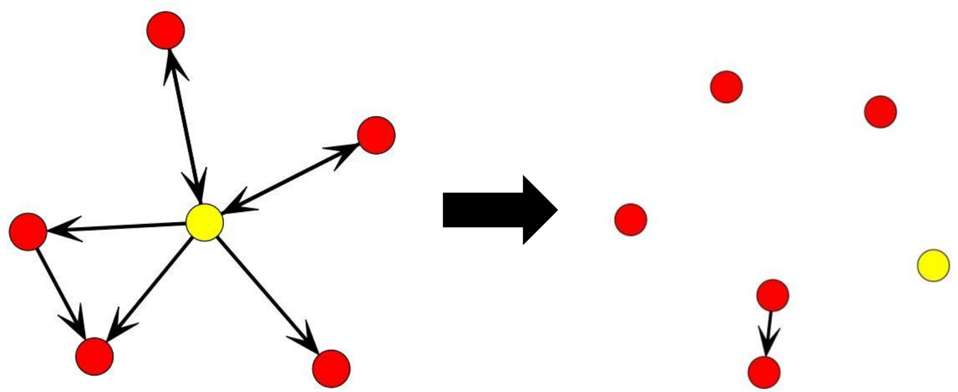
- Connectivity:
  - Who can reach whom?
- Isolate formation:
  - Whose removal isolates others?



How to Measure Network Robustness

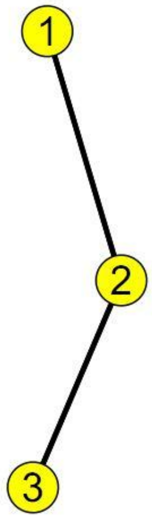


- Connectivity:
  - Who can reach whom?
- Isolate formation:
  - Whose removal isolates others?

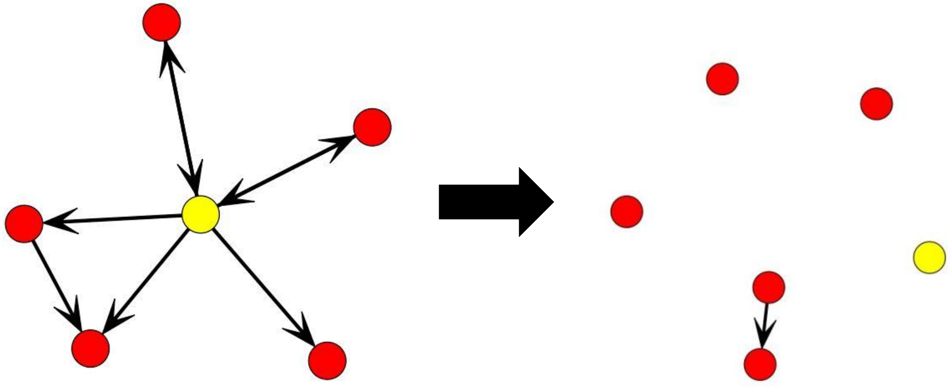


How to Measure Network Robustness

- Connectivity:
  - Who can reach whom?



- Isolate formation:
  - Whose removal isolates others?



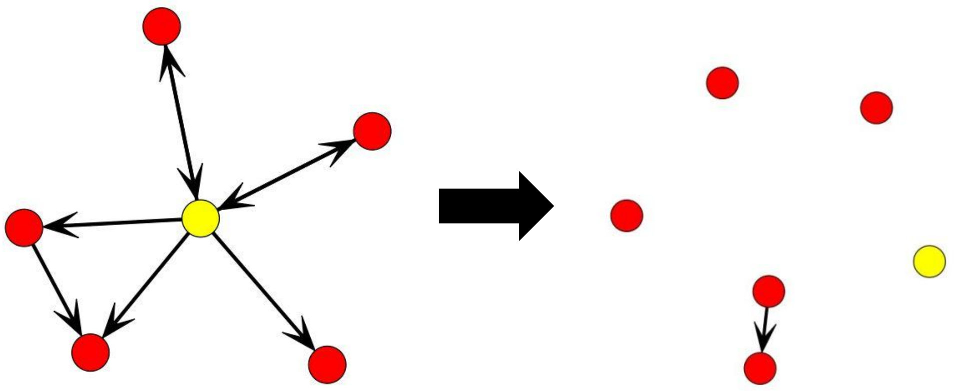
How to Measure Network Robustness

1

- Connectivity:
  2
  - Who can reach whom?

3

- Isolate formation:
  - Whose removal isolates others?



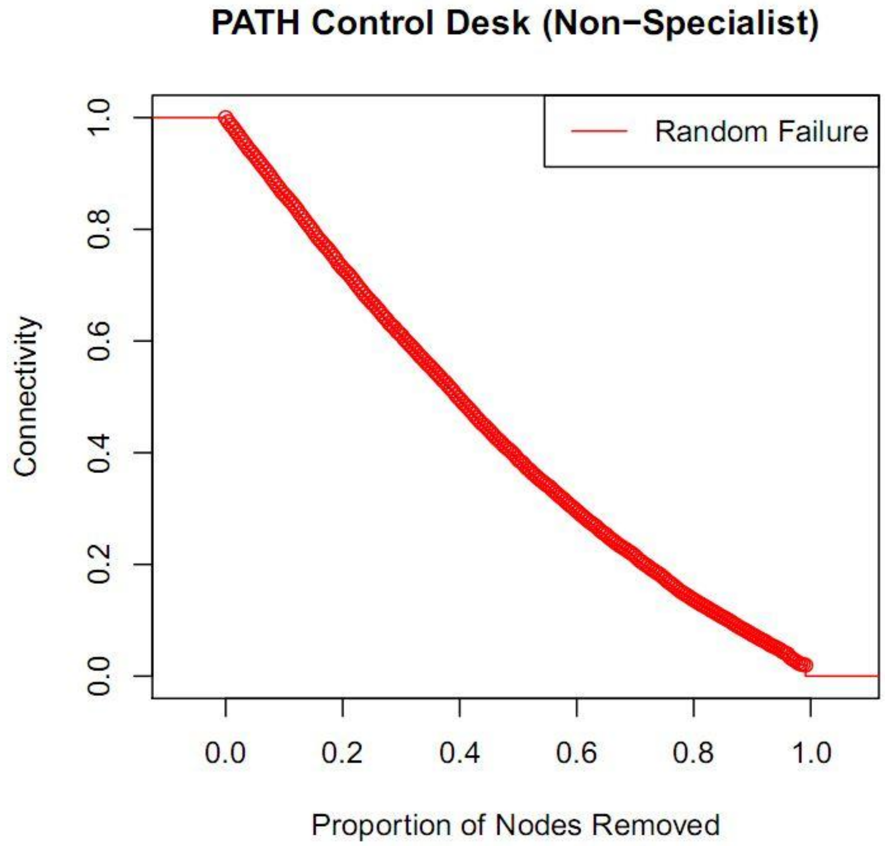
Building Robustness Profiles

- We need a way to measure connectivity as a network progressively degrades
  - Robustness scores: measure of a network's declining connectivity as more and more of its nodes are removed
- Use simulation of node failure to obtain robustness scores
  - After up many iterations, simulation yields expected mean connectivity as nodes are removed

- Let's look at some examples for clarification…

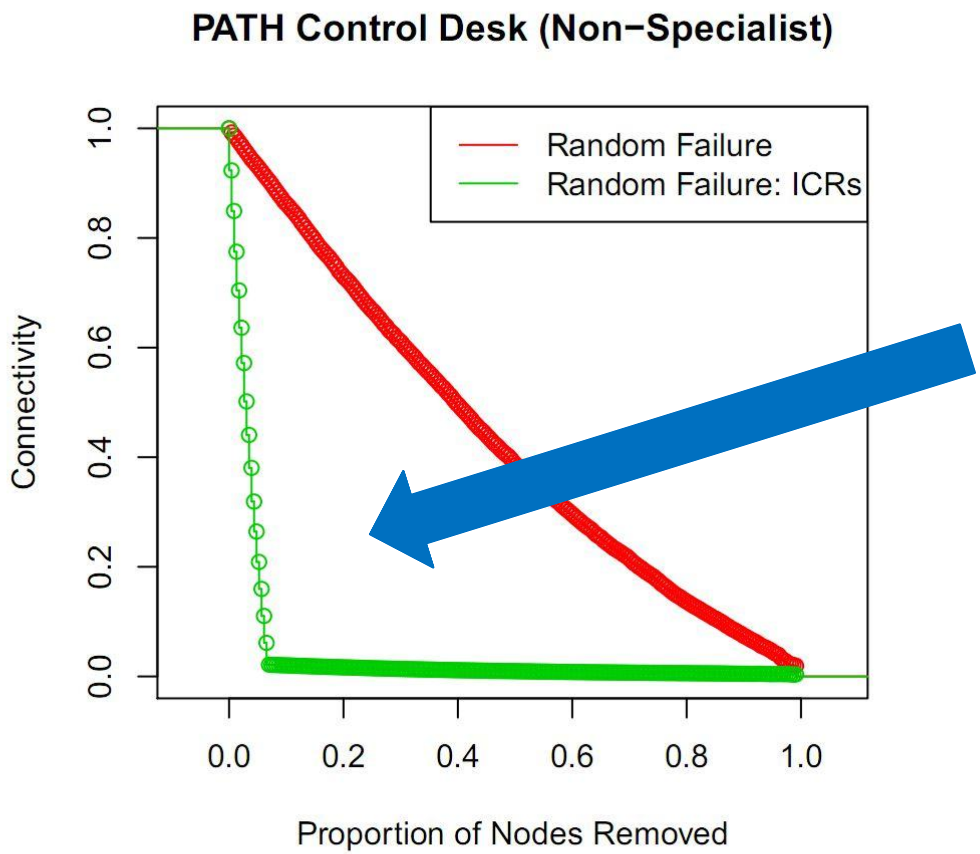
Building Robustness Profiles

- Using either of the previous measures, plot the robustness curve to monitor network connectivity as more nodes fail



Building Robustness Profiles

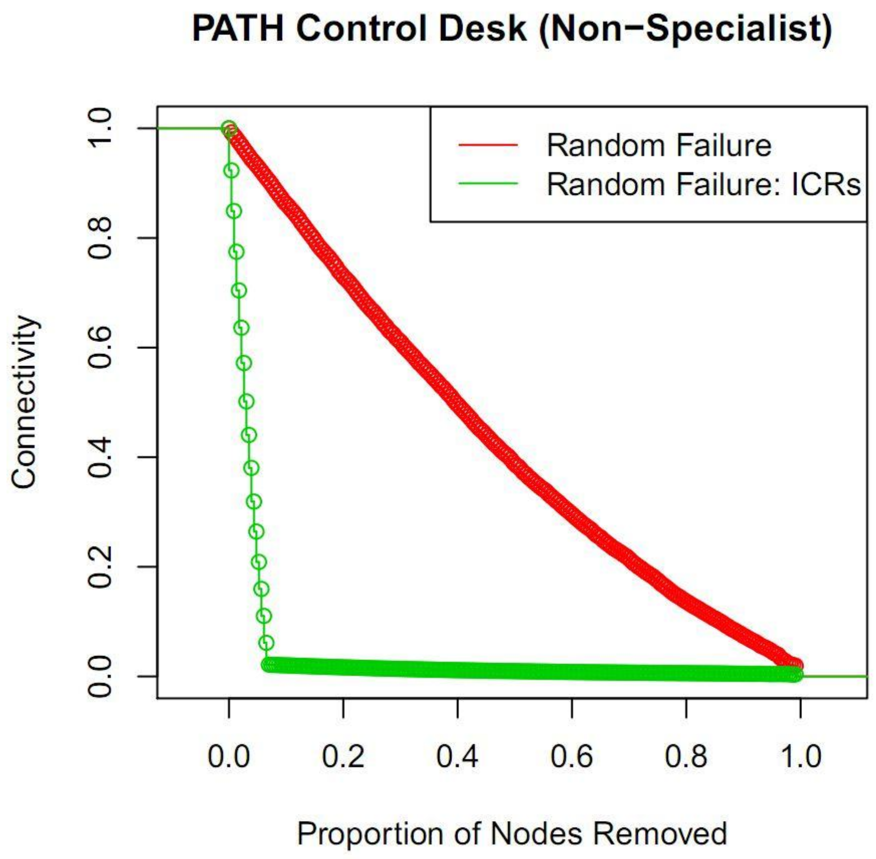
- Use multiple plots to compare robustness of different series of node failures



The area between curves tells us how network robustness differs across attacks

Building Robustness Profiles

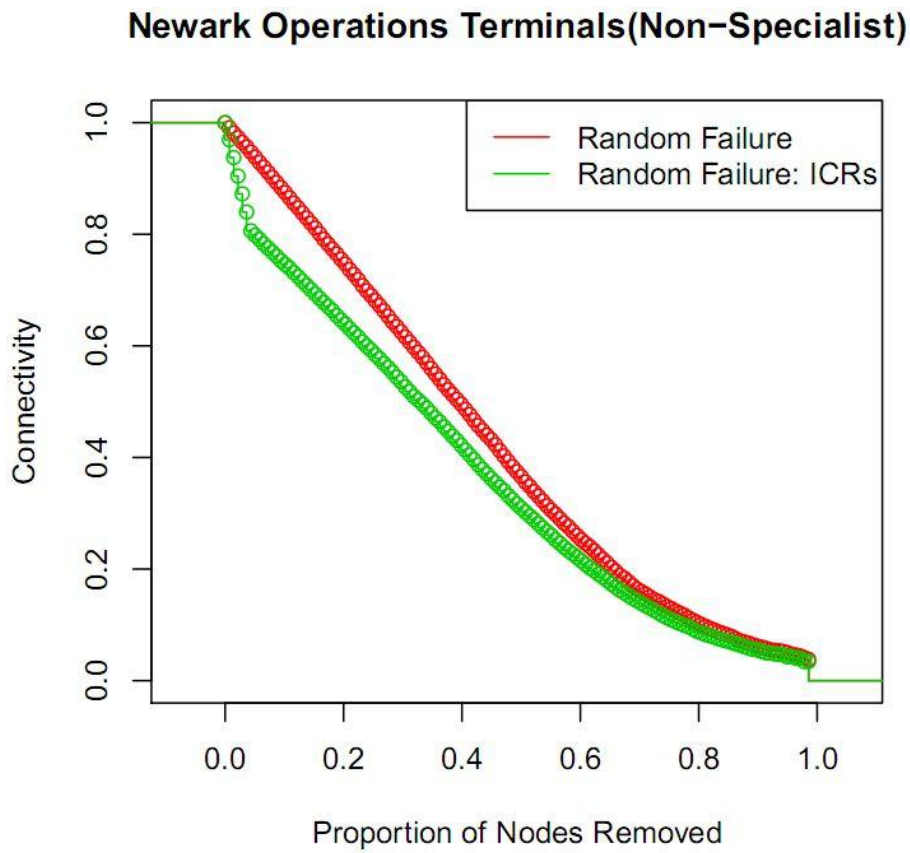
- Take the integral of the curve to obtain a robustness score



<u>Connectivity</u>
Random failure:
0.4287
Random failure of ICRs:
0.0397

Building Robustness Profiles

- Robust example:



<u>Connectivity</u>
Random failure:
0.4159
Random failure of ICRs:
0.3579

Hypotheses

- With an understanding of how to measure network robustness, we can test some hypotheses
  - **Hypothesis 1:** Specialist and non-specialist networks will be more robust to random failure than to random failure of ICRs
- Those with institutionalized roles will maintain those roles during the disaster response
  - **Hypothesis 2:** Specialist networks will be less robust to loss of ICRs than non-specialist networks
- Trained for these types of tasks, specialists can consolidate their coordination needs onto a smaller number of people

Hypotheses

- **Hypothesis 3:** Degree targeted failure and degree-targeted failure of ICRs will produce similar robustness scores among specialist and non-specialist networks

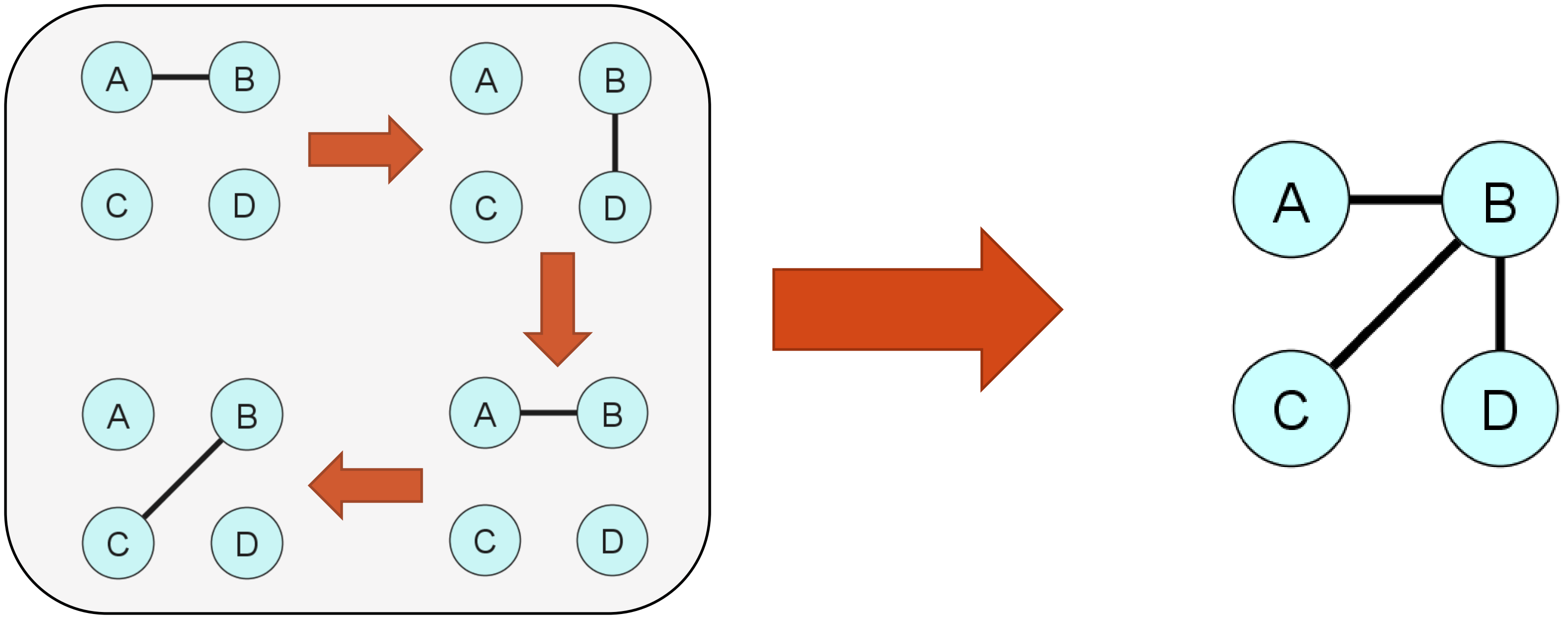
- If ICRs occupy positions with the most ties, there should be no difference between the two attacks

Comparing Robustness Profiles

- Calculate robustness scores for all varieties of attacks (random, degree-targeted, and ICR-targeted) across measures of connectivity and isolate formation
- Use t-tests to compare scores across different dimensions (ICR vs. non-ICR failures, specialist vs non-specialist networks)

Static Robustness: Results

- Static robustness examines the time-aggregated networks
  - Series of time-ordered communication events collapsed into a single network



Static Robustness: Results

- **Hypothesis 1:** Specialist and non-specialist networks will be more robust to random failure than to random failure of ICRs
- **Hypothesis 2:** Specialist networks will be less robust to loss of ICRs than non-specialist networks
- Specialist networks are significantly more robust to random failure than to random failure of ICRs
  - $t=4.2877$, $p=.0026$
- Among non-specialist networks, ICRs prove less crucial to preserving connectivity
  - $t=1.9004$, $p=.0991$

Static Robustness: Results

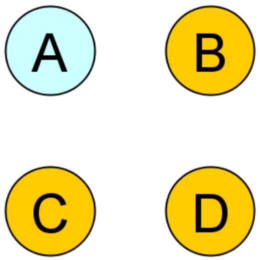
- **Hypothesis 3:** Degree targeted failure and degree-targeted failure targeting ICRs will produce similar robustness scores among specialist and non-specialist networks
- Degree-targeted failure is significantly more damaging than degree-targeted failure of ICRs in specialist networks
  - t=-2.4815, p=.0380
- The difference between the two attacks is significant in non-specialist networks
  - t=-4.0548, p=.0048

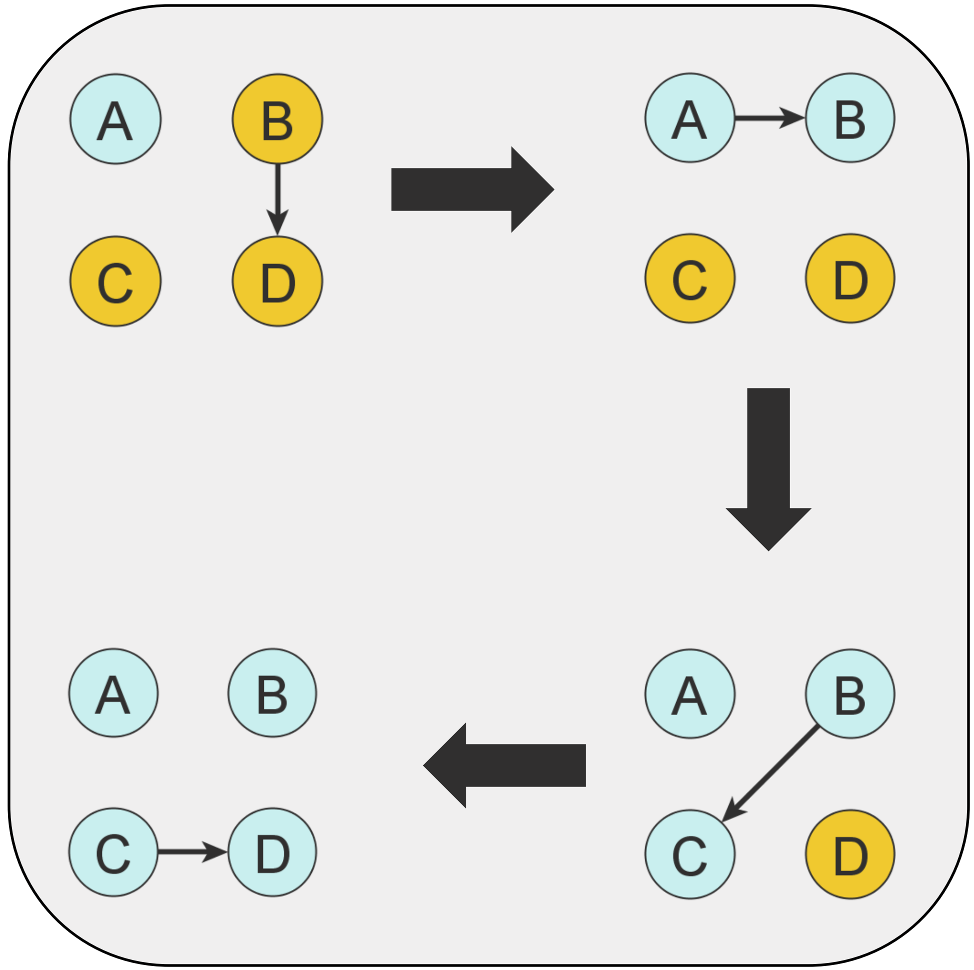
Dynamic Robustness: Methodology

- Ordinal nature of transcripts allows us to explore dynamic robustness
- Using the time-ordered sequence of communication to measure forward connectedness
  - How would network unfold if certain actors *were never present* in the network?

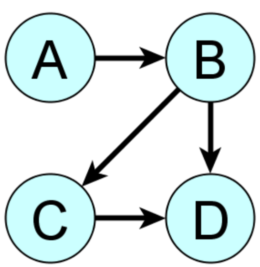
Dynamic Robustness: Methodology

Can a message from A reach D?



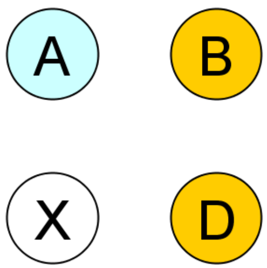


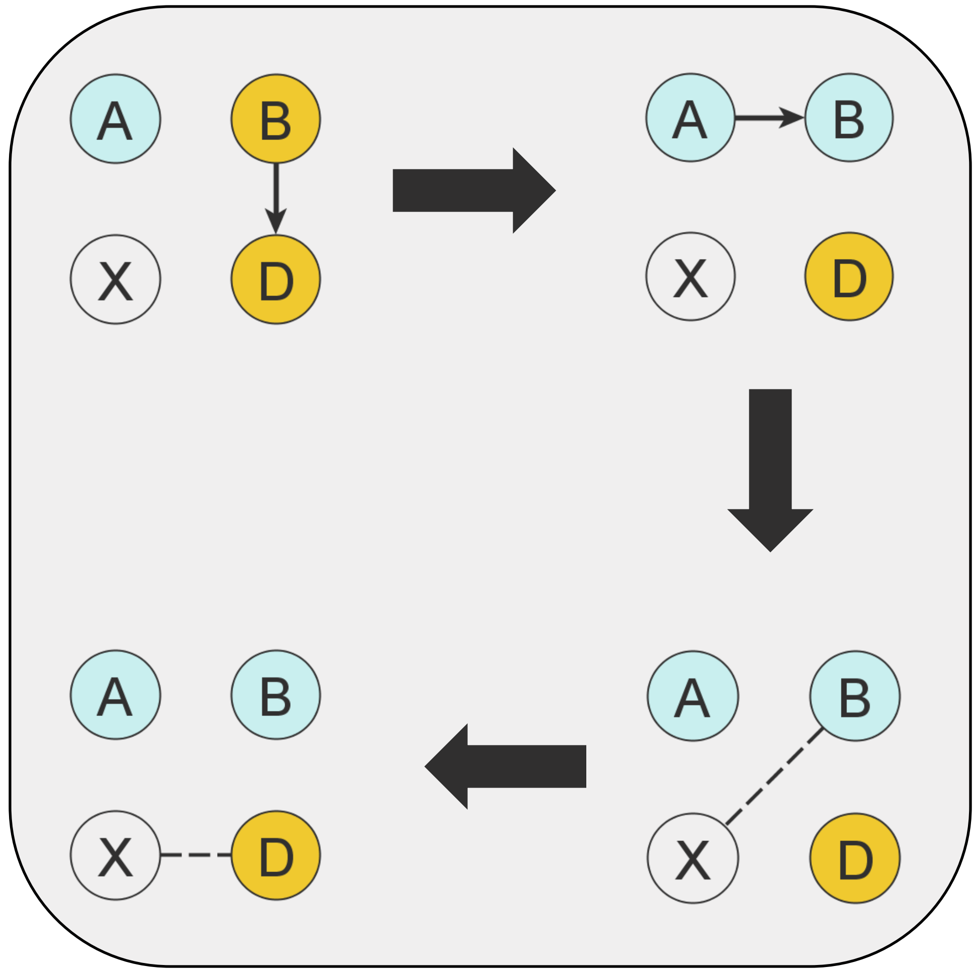
Time-aggregated network:



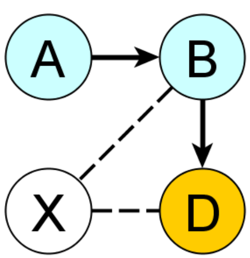
Dynamic Robustness: Methodology

Can a message from A reach D in the absence of C?





<u>Dynamic network</u>:



Dynamic Robustness: Results

- **Hypothesis 1:** Specialist and non-specialist networks will be more robust to random failure than to random failure of ICRs
- **Hypothesis 2:** Specialist networks will be less robust to loss of ICRs than non-specialist networks
- Difference between robustness scores of random failure and random failure of ICRs remains significant for specialist networks
  - $t=3.5697$, $p=0.0073$
- Random failure of ICRs remains not significantly more damaging than random failure for non-specialists
  - $t=1.7971$, $p=0.1154$

Dynamic Robustness: Results

- **Hypothesis 3:** Degree targeted failure and degree-targeted failure targeting ICRs will produce similar robustness scores among specialist and non-specialist networks
- Degree-targeted failure remains more damaging than degree-targeted failure targeting ICRs
  - $t=-3.231$, $p=0.005$
- Insignificant difference between specialist and non-specialist robustness to degree-targeted failure
  - $t=0.778$, $p=0.450$

Results and Analysis: Recap

- What do these results tell us?
  - Hypothesis 1: Rejected
    - ICR failure is not significantly more damaging than random failure in non-specialist networks (but ICRs still play an important role in specialist networks)
  - Hypothesis 2: Supported
    - ICRs play a more important role in coordinating specialist networks than they do in non-specialist networks
  - Hypothesis 3: Rejected
    - Degree-targeted attack is more damaging than degree-targeted attack on ICRs: it takes more than ICRs alone to hold together the network…

Isolate Formation: Results

- What can isolate formation tell us that connectivity cannot?
  - Measuring isolate formation tells us more about *how* these attacks pull apart the networks
- Degree-targeted failure produces significantly more isolates in specialist networks than it does in non-specialist networks
  - $t=-2.6515$, $p=.0237$
- DT-ICR produces significantly more isolates in specialist networks than it does in non-specialist networks
  - $t=-2.2608$, $p=.0441$

Isolate Formation: Results

- What does this tell us that previous findings did not tell us?
  - When specialist networks lose their high-degree actors (usually ICRs), many remaining actors become isolated
    - Low degree actors tend to be tied exclusively to a single ICR
  - Non-specialist networks have a higher level of negotiation (more ties among those with relatively low numbers of ties)

Conclusions: What Have We Learned?

- Specialist networks are especially vulnerable to loss of ICRs and subsequent node isolation
  - Reliant on institutional features to build network structure

- Non-specialist networks remain moderately more connected following ICR loss
  - Not as reliant on institutional roles to guide network structure
  - Relative lack of isolation suggests increased negotiation among non-coordinators; likely have a more difficult time delegating emergency coordination tasks (have to figure out what to do and how to do it); confirmed in actual transcripts

Conclusions: Take-Home Points

- Organizational roles are key to predicting network structure among specialists
- Non-specialists are less reliant on organizational institutions to build their communication network

Future Directions

- ✓ Static, time-aggregated robustness
- ✓ Dynamic robustness

- What's next?
  - Resilience: How can the network *actively respond to damage* and rebuild itself following personnel loss?

Thank you!

- Questions, comments, thoughts?

Dynamic Robustness: Methodology

- If dynamic gives a more precise result, why bother with time-aggregated network?
  - More precise *for this exact ordering* of ties
    - Would network unfold exactly like this again? Can't be sure
  - Ties indicate open channel of communication regardless of ordering of messages
    - Illustrate opportunity structure for communication