



the topology of covert conflict

Shishir Nagaraja
and Ross Anderson

Security Group

Computer Laboratory



What are complex networks?

- WWW, Internet, adhoc networks, network of email users
- networks of airports, networks of rebel groups, networks of activists.
- An enormous intricate network resulting from a self-organized growing process following local dynamical rules without a global blueprint.

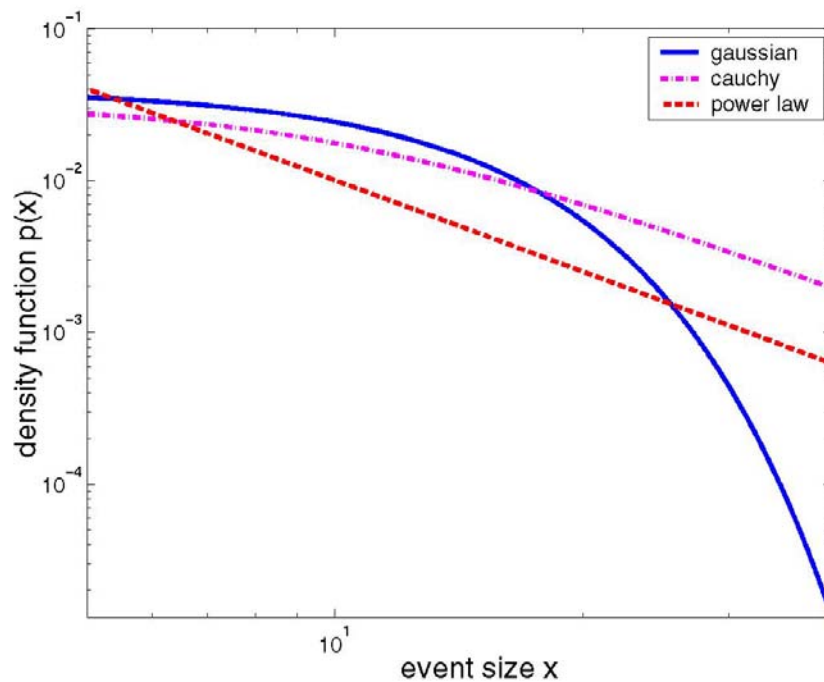
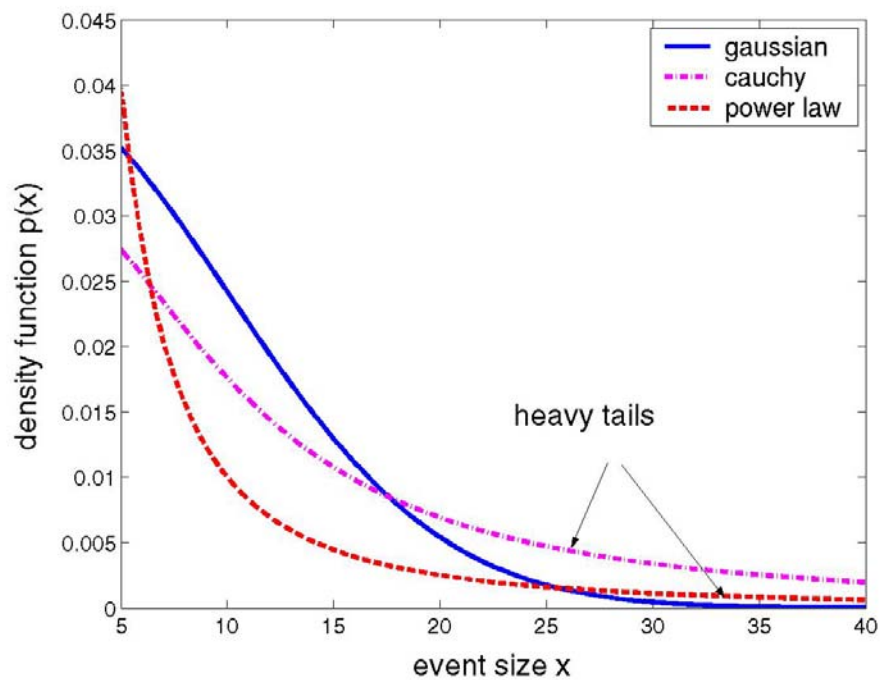


Is a complex network not merely a complicated network?

- A working definition of complexity
 - Heterogeneity – not just complex rules but heterogeneity on every scale.
 - Emergence – characteristic features are a result of the spontaneous interactions between the many constituent units in the system.
- As a result average and typical behaviour are very different.

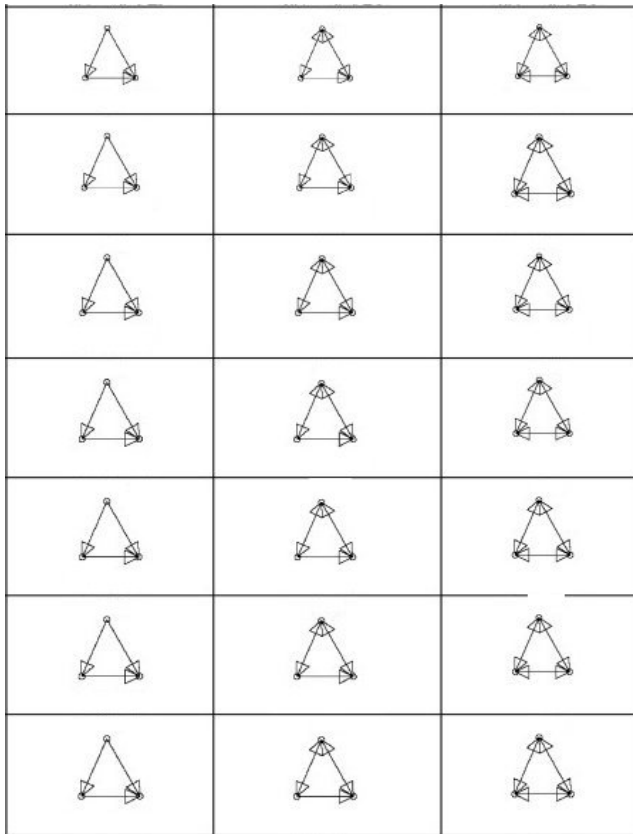
complex network characteristics

Heavy tailed degree distributions

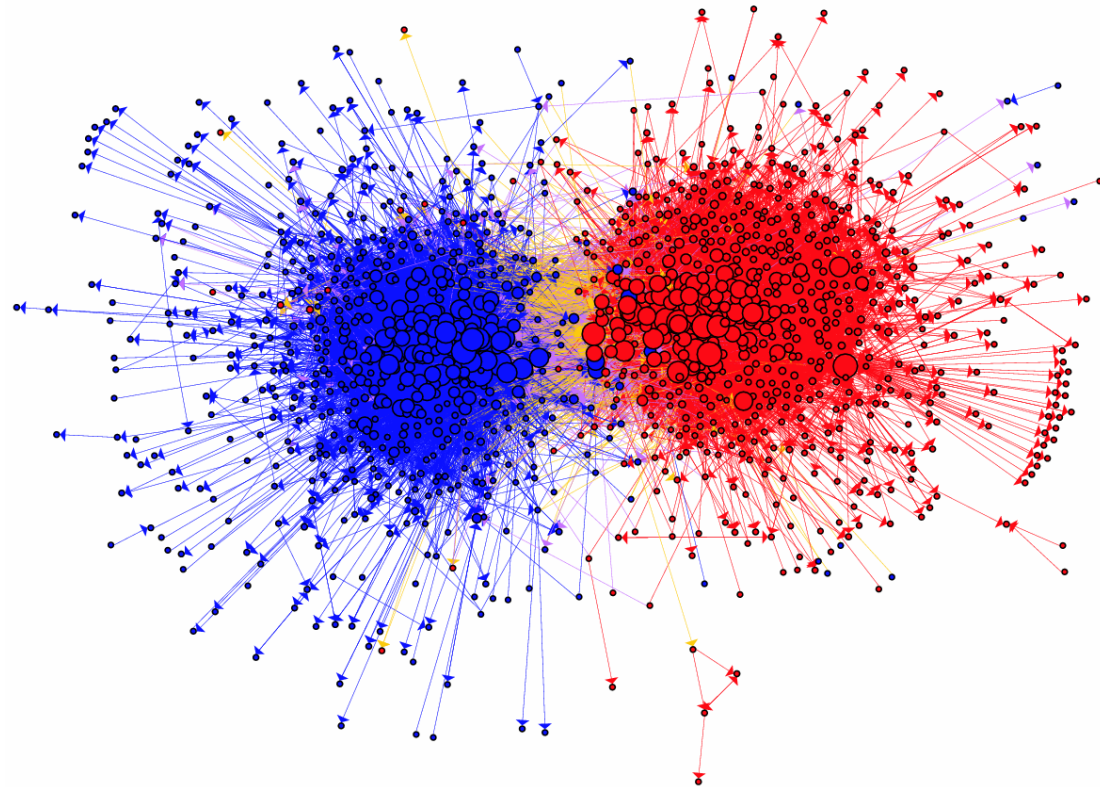


complex network characteristics

Motifs and Community structure



Motifs in metabolic networks



Community structure of political blogs
2004 US Elections
(...Adamic and Glance 2005)



conflict and communication

- Conflicts turn on connectivity
 - Historical examples
 - Contemporary – Traffic Analysis
 - Military – Electronic warfare.
 - The MIT media reality mining project.
 - Email surveillance - WEIS 2006 Danezis et.al. result.
- Albert and Barabási result.
- Holme et al. result.



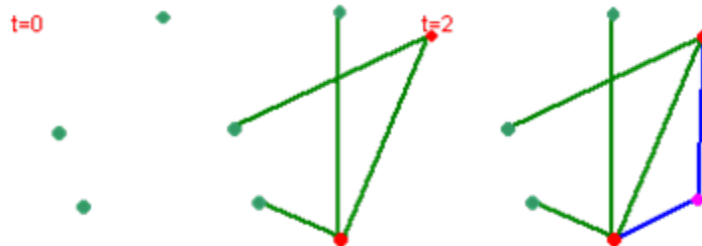
Tactical and Strategic Options

- Efficiency vs. resilience.
- Local rules only.

Network model

- Undirected BA-Scale free network.
- Start out with m_0 disconnected nodes.
- At each step add one node with m links with a probability distribution.

$$P(\text{linking to node } i) \sim \frac{k_i}{\sum_j k_j}$$





Game Model

- Multi-round game of three phases
 - Attack
 - Resource addition
 - Recovery
- Attacker's motive
 - Causing the largest connected component to disappear.
 - Exponential increase in the average geodesic length.
- Defenders motive
 - Keeping the largest connected component and average geodesic length a constant.



Game rules

- Nodes can observe and conscript fresh recruits into any topological arrangements they wish.
- Local organization(only single hop communication is allowed): Nodes can ask their neighbours to modify topology but centralised coordination is not allowed.
- A node is in complete control of its local edge resources.
- Edge sharing: since we are considering undirected graphs. Edges can be under the control of either but not both ends.



Attack Mechanisms

- Remove nodes with high vertex order nodes.
- Remove nodes with high (freeman) betweenness centrality.

$$C_B(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}}$$



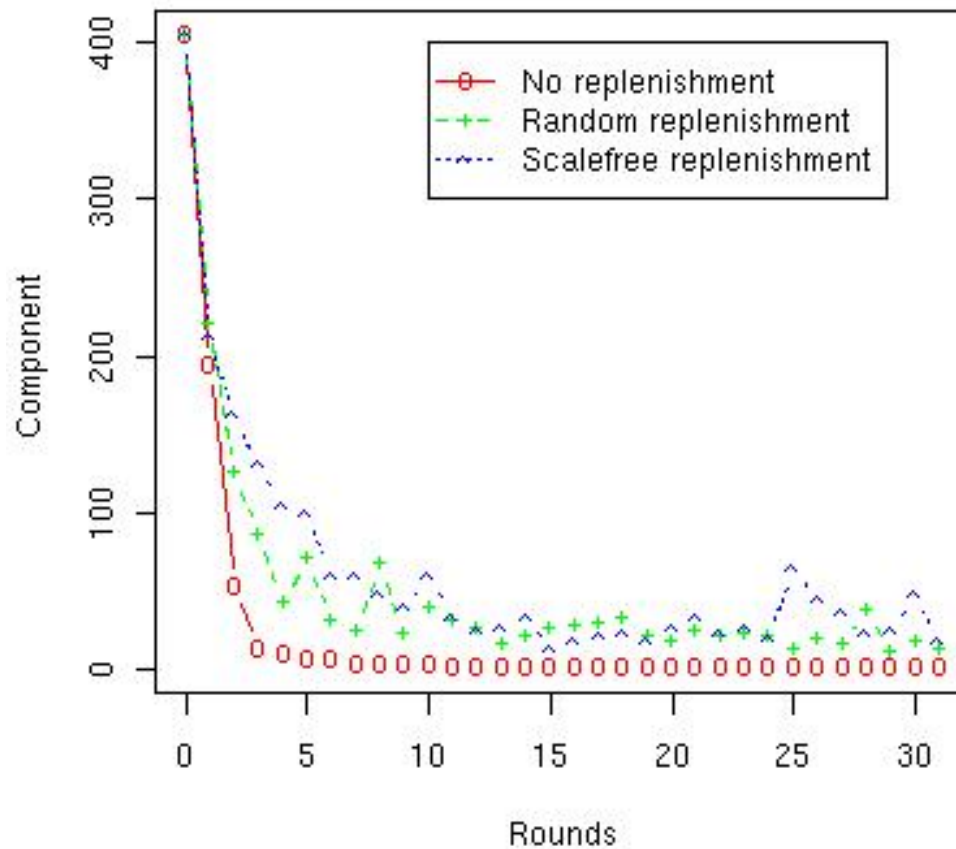
Defence Mechanisms

- Naive Replenishment - No motif creation
- Rings
- Cliques
- Delegation

Creation of rings and cliques are subject to the game rules of the previous slide.

Naive Replenishment

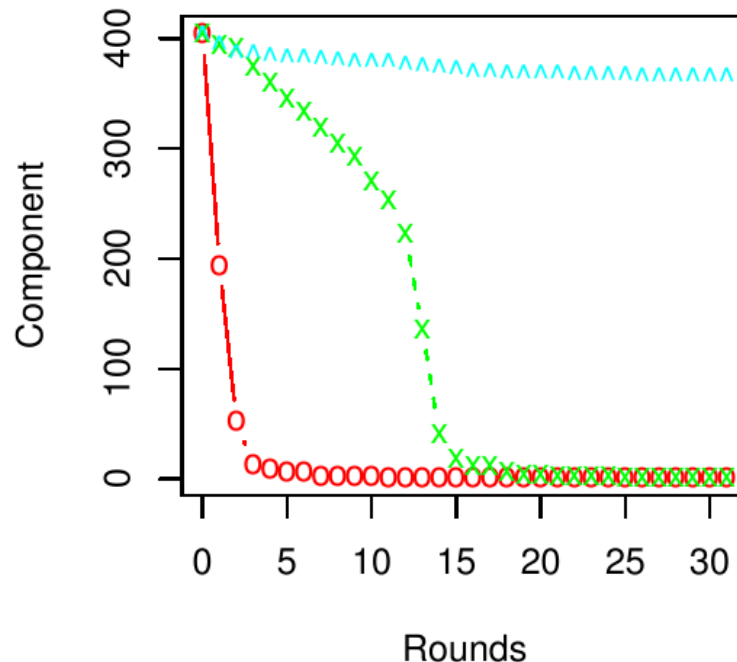
Vertex-order attack
with naive replenishment



Attack - Vertex order

Defences - Rings and Cliques

Vertex-order attack
with Rings and Cliques

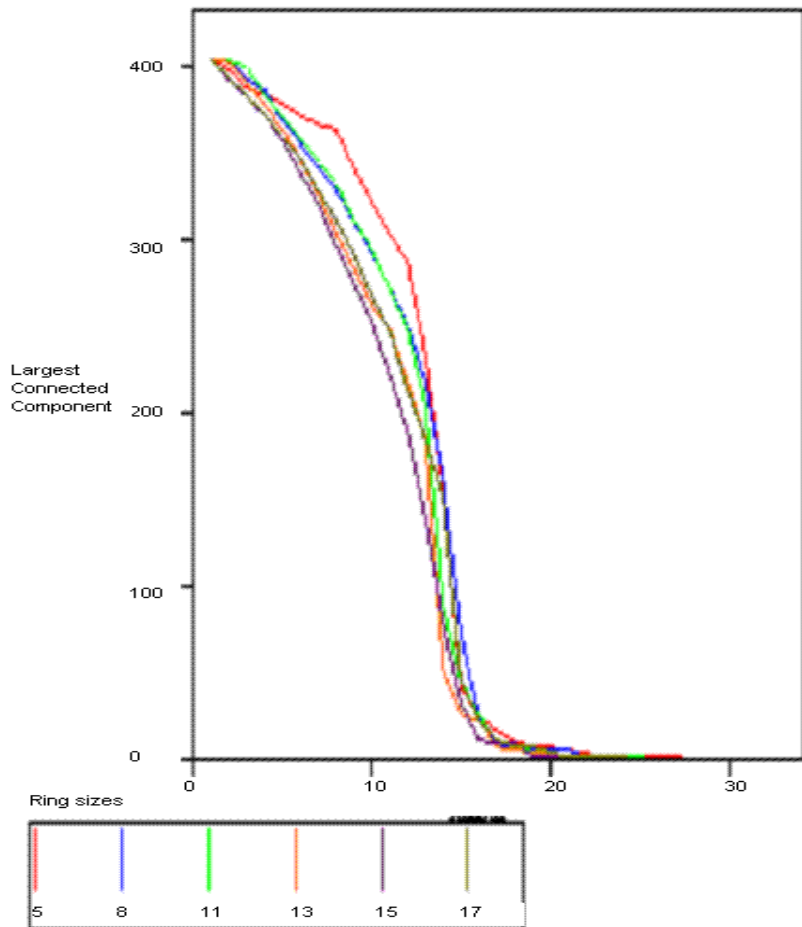


- vertex order attack, No adaptation
- - + - vertex order attack, Rings
- ...^... vertex order attack, Cliques

Analysis – Recovery under vertex order attack

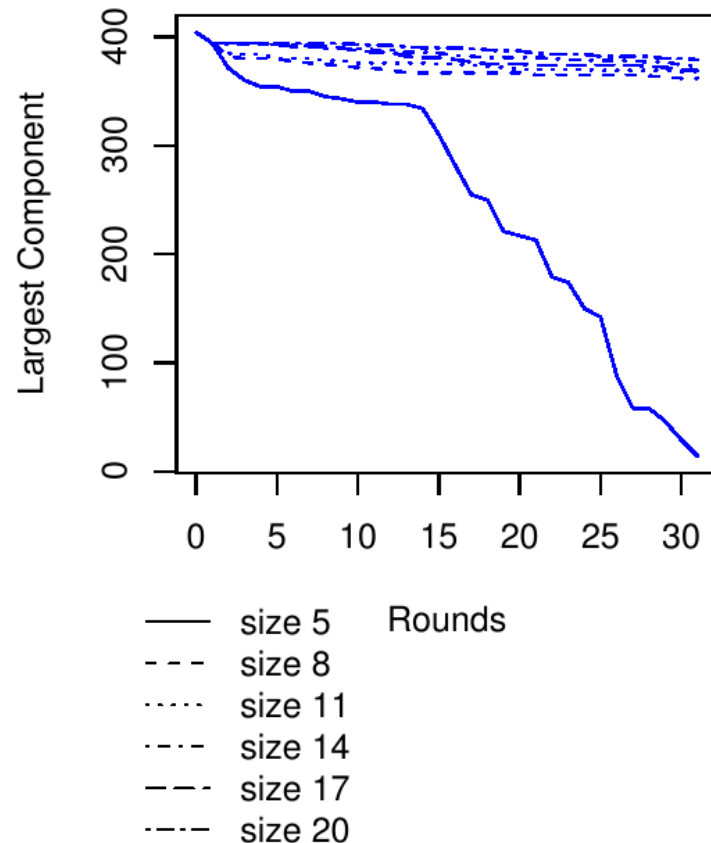
Rings

Ring recovery with various ring sizes under a vertex-order attack



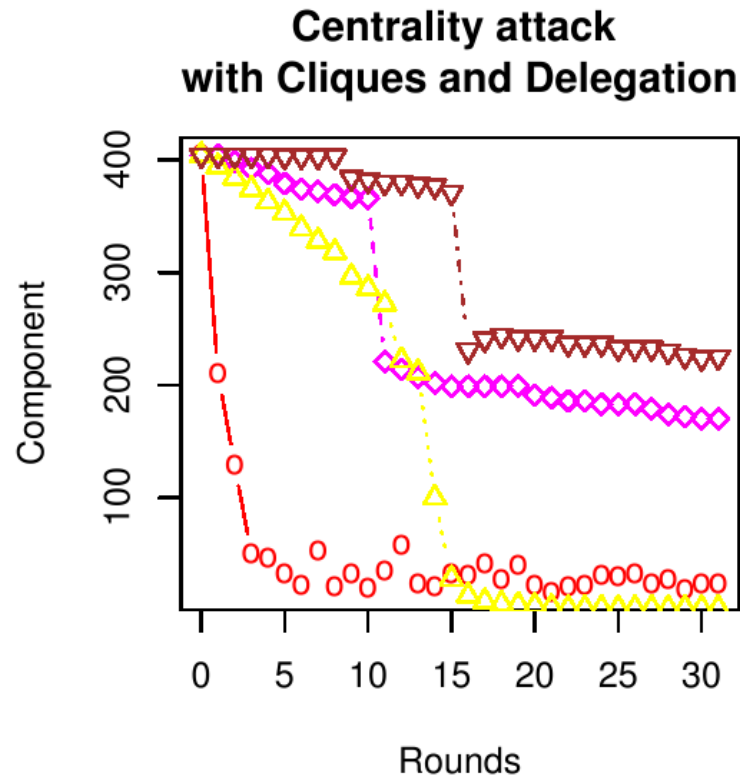
Cliques

Vertex order attack with various clique sizes



Attack - Betweenness centrality

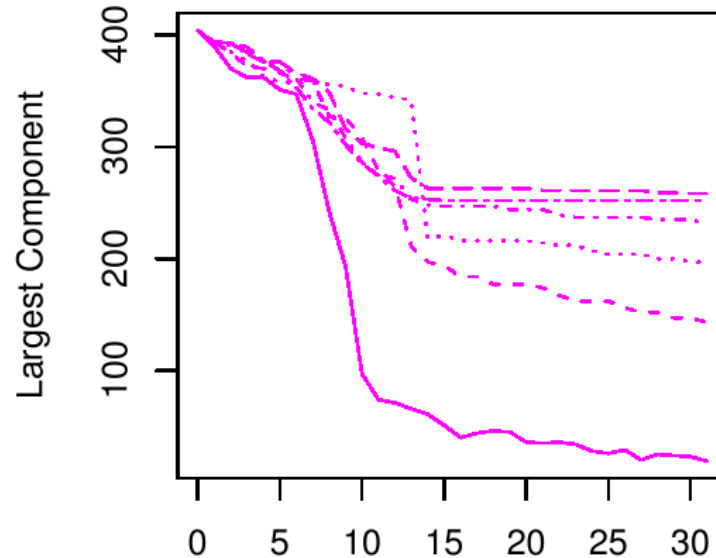
Defence - Cliques and Delegation



- No replenishment
- △- Delegation
- ◇- Clique
- ▽- Clique + Delegation

Clique recovery with different sizes of clique

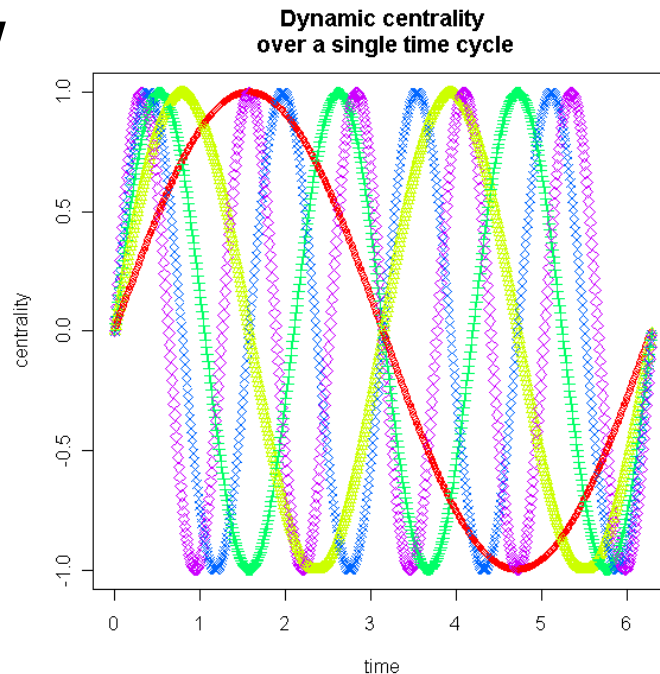
Centrality attack
with various clique sizes



- size 5
 - - - size 8
 - size 11
 - · - · size 14
 - - - - size 17
 - · · · · size 20
- Rounds

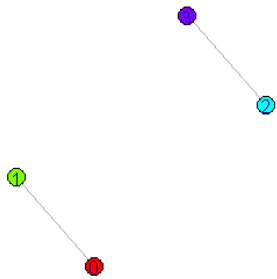
Dynamic Centrality

- Is there a world where centrality is dynamic?
- What local-information – local-action protocols result in emergent dynamic centrality

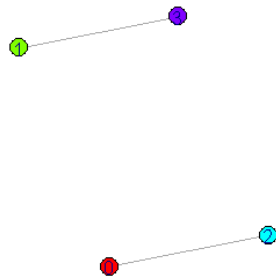


An emergent centrality protocol

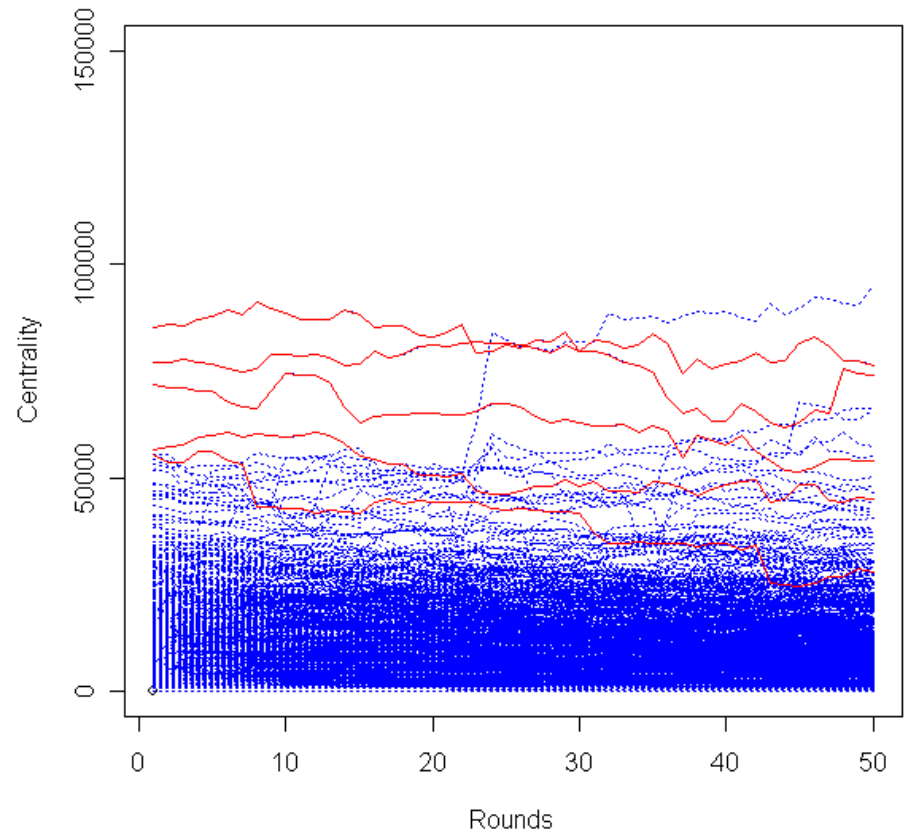
Before rewiring



After rewiring

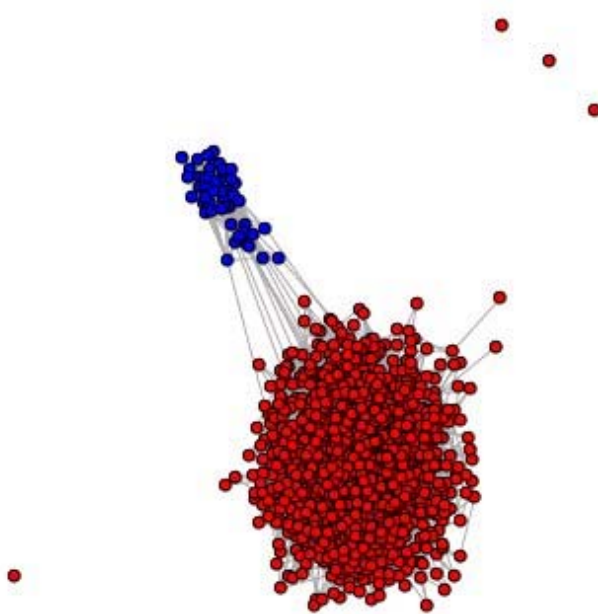


Betweenness centrality of all the nodes in the network



The topology of community hiding!

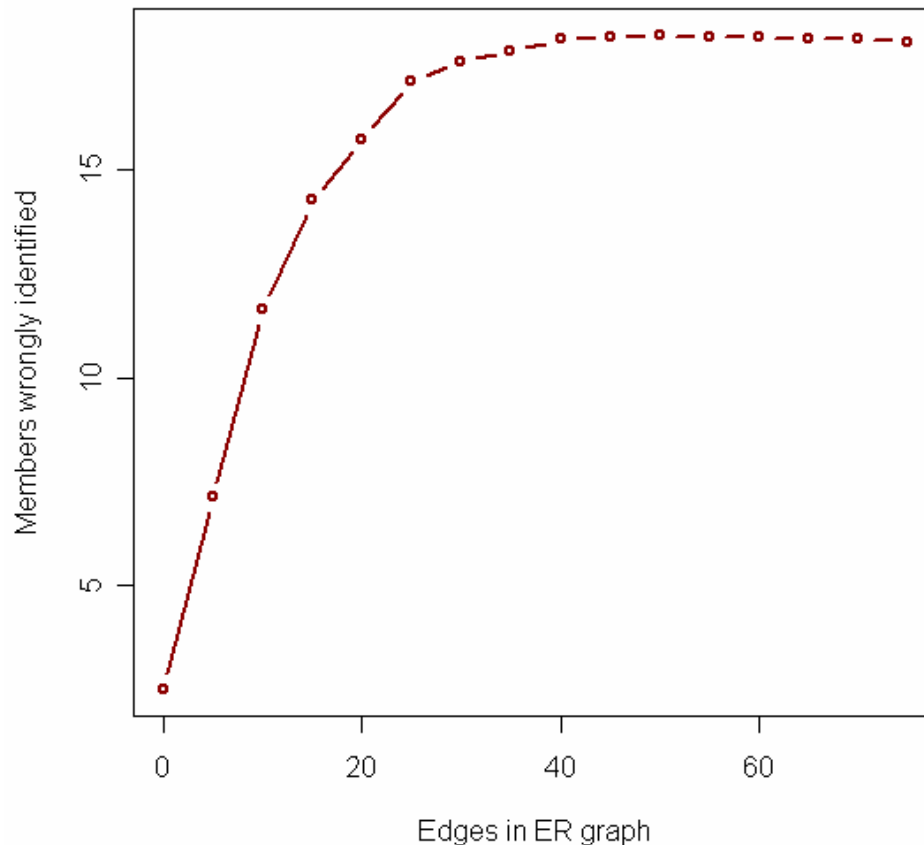
BLUE – Covert network
RED - Rest of the network



How do we detect the covert network?

Error rates of mincut methods

**Error in Community Detection
vs size of ER graph**



Partitioning methods:
Kernighan-lin
Laplacian
Betweenness centrality



Modularity based detection

- Intuition: Where are the edges vis a vis where we expect them?
- Where are the edges - Adjacency matrix
- Where are the edges expected – Edge expectancy matrix $P_{ij} = d_i d_j / (2E)$
- Calculate eigen-values and eigen-vectors of $B_{ij} = A_{ij} - P_{ij}$ to obtain partition.
- Error rate is **Linear!**



Conclusion

- We get insights into why revolutionaries use cells, and how ring based peer to peer systems like Chord might be vulnerable.
- Simulations let us explore many new attack and defense strategies in the lab.
- Dynamic centrality is locally achievable!
- Implications for all sorts of networks – computer, social, political ...
- Barabasi and Albert attack model from the static case to the dynamic case.



Future work

- Complete the bridge between network analysis and evolutionary game theory.