Complex Network Topologies Resilient to Centrality Attack

{ Rachel Fiolek, Swami Iyer, Timothy Killingback } UMass Boston, Physics, Computer Science, Mathematics

Introduction

Many complex systems can naturally be described by networks, where the essential components are represented by vertices in the network and the connections between the components are represented by edges between the corresponding vertices. An important issue involving complex networked systems is the resilience of the overall system to the failure of its constituent parts. Extending previous studies of network structural changes by determining the topology of those networks which are most resilient to targeted vertex removal is both theoretically and practically important.

Methods

Our research made use of five different vertex removal strategies: random removal, and degree, betweenness, closeness, and eigenvector centrality removal. Here, we will only focus on two of these methods: degree and closeness centrality removal.

- Degree centrality refers to the idea that the number of edges connected to a vertex reveals that vertex's importance. So, a removal strategy based on degree would have the highest degree vertices destroyed.
- Closeness centrality refers to the average distance of one vertex to all other vertices in the network. So, the vertex that has the shortest average distance, based on the number of edges traversed in going from one vertex to another, is destroyed.

In order to produce the most robust networks, a base network is subjected to random rearrangements of some number of its edges, producing random structural variations. The variant network most robust to a given centrality attack is taken as the new base network. This process is repeated until a topology emerges whose robustness cannot be increased.

We make use of simultaneous targeted attack for both of these strategies, which means that the centrality measure is calculated for all network vertices and then a specified fraction of these vertices are removed, from highest to lowest, according to the centrality measure. In other results, we have made use of sequential targeted attack, where the centrality measure is calculated for all vertices in the initial network, and the vertex with the highest centrality measure is removed, resulting in a variant network. The centrality measures of all vertices in the new network are recalculated, and the highest ranked is removed. This iterative process is continued until the desired fraction of vertices has been removed.

Results 1

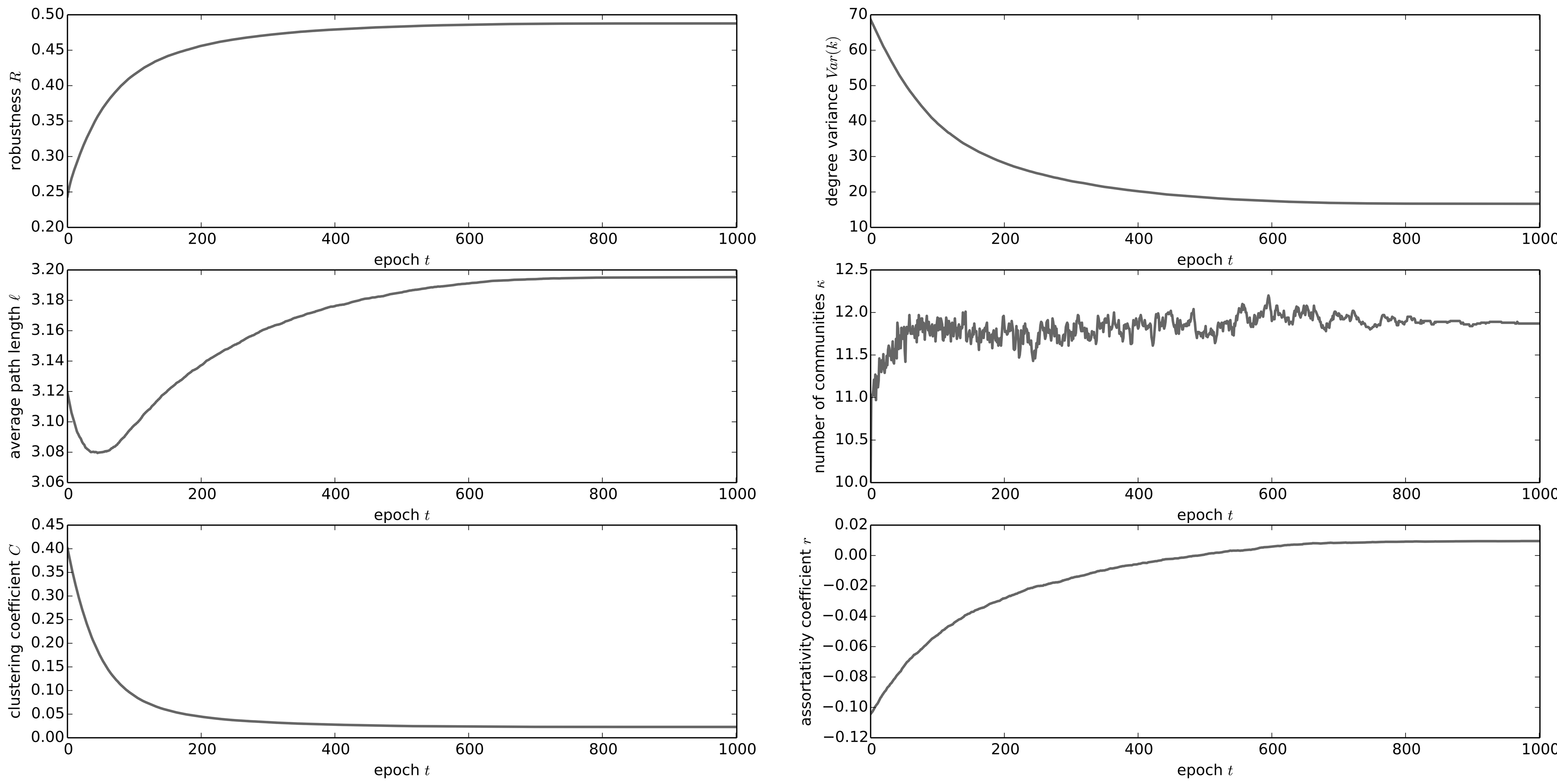

Figure 1: Time evolution of network characteristics starting from a clustered scale-free network of average degree 8 under simultaneous degree centrality attack (results averaged over 100 replicates).

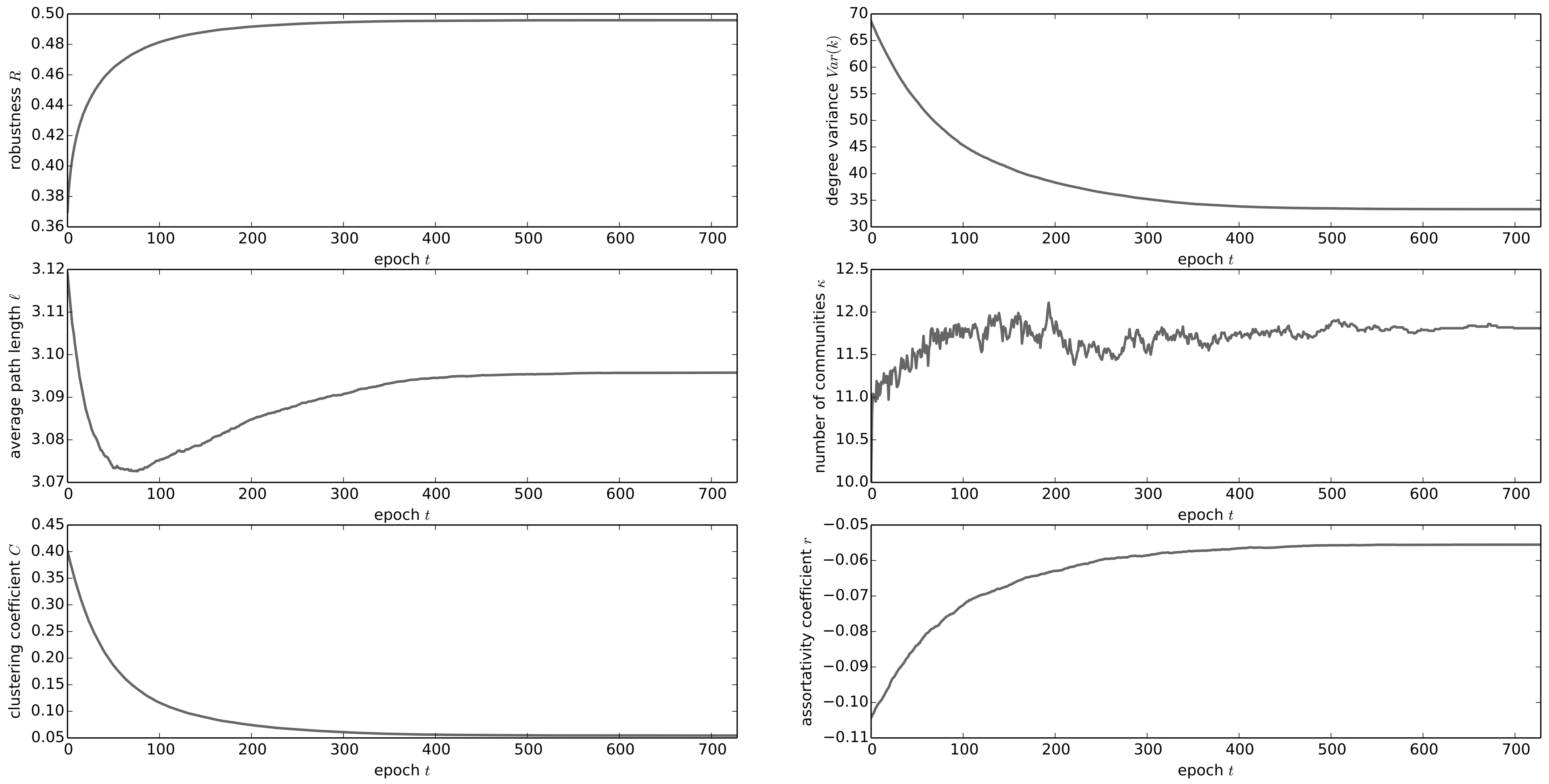

Figure 2: Time evolution of network characteristics starting from a clustered scale-free network of average degree 8 under simultaneous closeness centrality attack (results averaged over 100 replicates).

Results 2

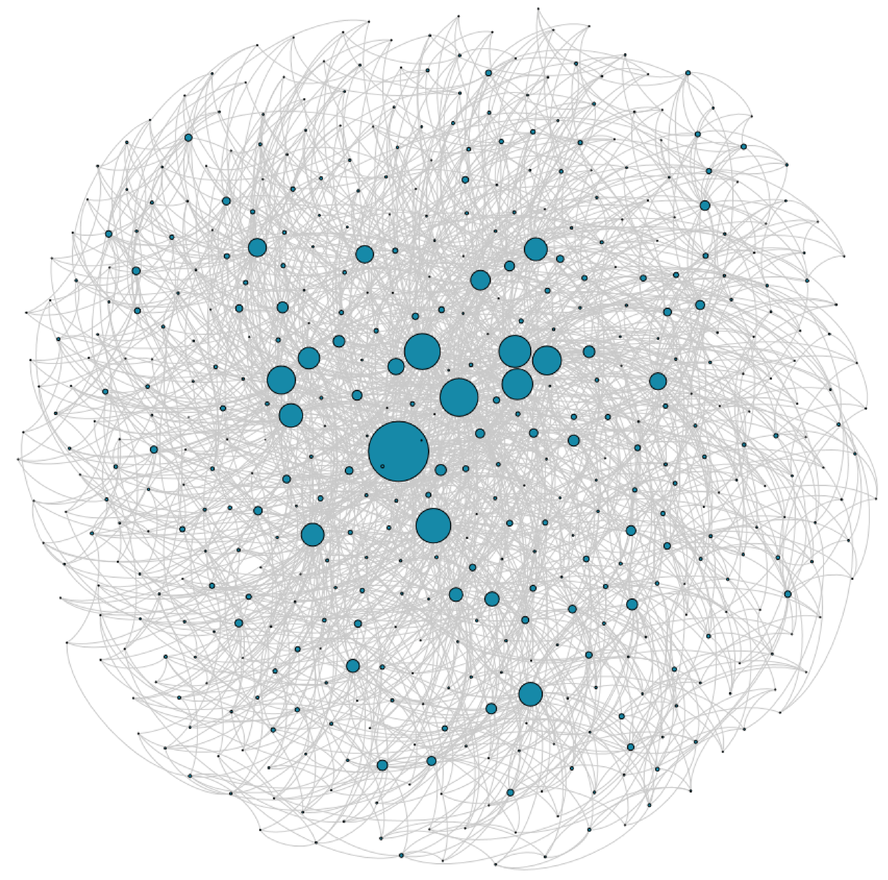

Figure 3: Clustered seed network, with vertex size proportional to its degree.

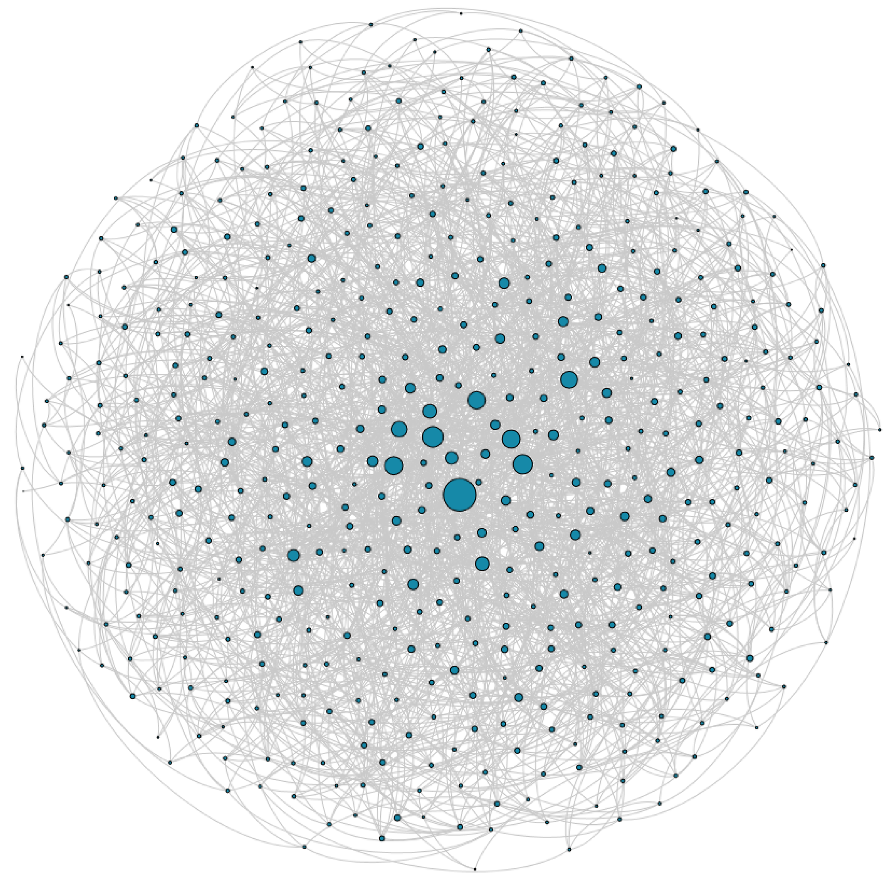

Figure 4: Clustered seed network after having been subjected to vertex removal by degree centrality with simultaneous attack. Vertex size proportional to its degree.

References

[1] Iyer et al. Attack Robustness and Centrality of Complex Networks. *PLoS ONE*, 8(4):1–17, April 2013.

[2] S. Strogatz. Exploring Complex Networks. *Nature*, 410:268–276, 2001.

Conclusions and Future Research

In comparing the degree and closeness centralities, it can be seen that for each respective time evolution, the curves of all six graphs converge to nearly the same value. In fact, the networks display the same qualitative behavior for all centrality measures. It can be seen that with degree attack, convergence takes twice as long as with closeness attack. The visualizations of the seed and evolved network show that the variance in degree for the evolved network is lower than for the seed network. We intend to extend this research to both clustered and assortative networks, and to networks under sequential attack for the four different centrality measures. It would also be interesting to collect data for networks where robustness is minimized.