NETWORK ANALYSIS - 90530

Dashboard / My courses / 90530 / 19 April - 25 April / Second assignment: Network robustness

Second assignment: Network robustness

In this **2nd assignment** you will investigate the **robustness of networks by simulating random failures and target attacks**. The assignment is composed of two parts.

Part 1: Use small graphs

(there are 2 options, number 1 and number 2, select only one of the two)

1) Use any synthetic graphs

a. In the first part, you can use some graphs obtained by using the **Networx library** or the library of your choice.
b. For each selected graph (max 2 or 3) you can **perform different types of attack:** turn off nodes at random, turn off the highest degree nodes, those with the highest pagerank, those with the highest betweenness, ...
c. After each removal, compute new measures, for example the **size of the giant component** or the **diameter of the network** and then plot these measures with respect to node failures.
d. Be careful, some of the functions you will use work only for undirected, **connected** graphs and therefore you need to instrument your code to work on the entire graph first, and then on the several components after the split of the original graph into smaller clusters.

2) Conspiracy in Social Networks

In a Big Brother society, the thought police wants to follow a "divide and conquer" strategy by fragmenting the social network into isolated components. You belong to the resistance and want to foil their plans. There are rumours that the police wants to detain individuals that have many friends and individuals whose friends tend to know each other. The resistance puts you in charge to decide which individuals to protect: those whose friendship circle is highly interconnected or those with many friends. To decide you simulate two different attacks on your network, by **removing** (i) the nodes that have the **highest clustering coefficient** and (ii) the nodes that have the **largest degree**.

Study the **size of the giant component** in function of the fraction of removed nodes for the two attacks on the following networks:

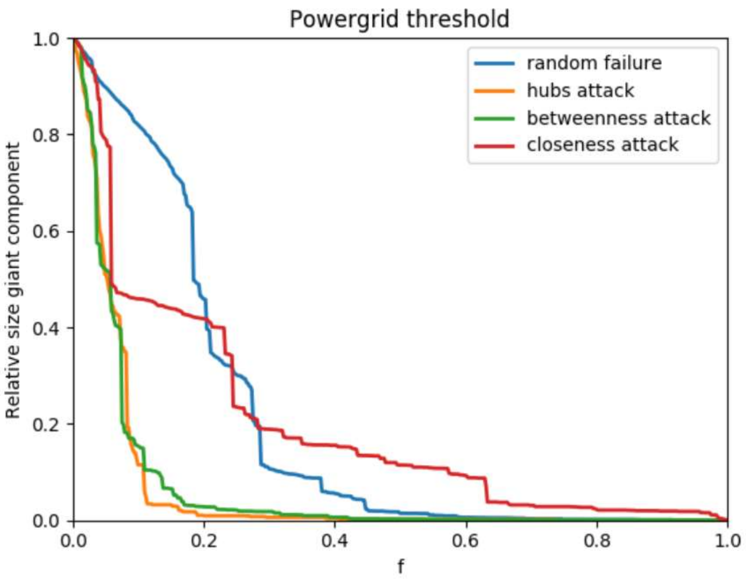
a. A network with $N = 10^4$ nodes generated with the configuration model (https://en.wikipedia.org/wiki/Configuration_model) and power-law degree distribution with $\gamma = 2.5$.
b. A network with $N = 10^4$ nodes generated with the hierarchical model (https://en.wikipedia.org/wiki/Hierarchical_network_model).

Which is the most sensitive topological information, clustering coefficient or degree, which, if protected, limits the damage best? Would it be better if all individuals' information (clustering coefficient, degree, etc.) could be kept secret? Why?

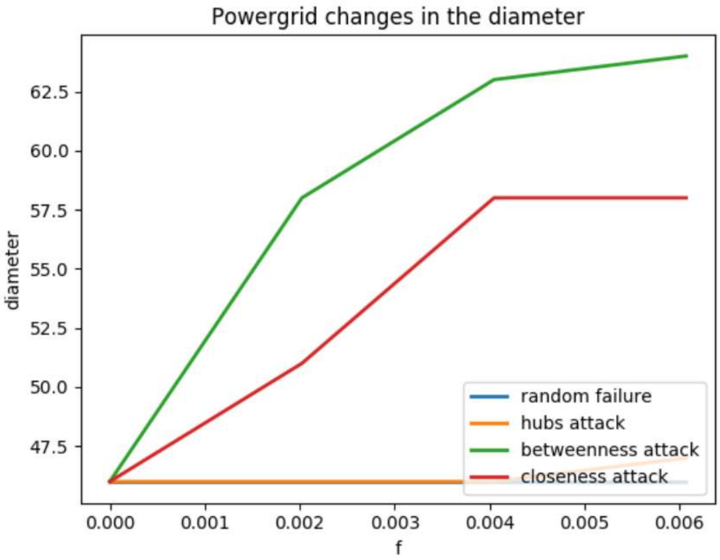
Part 2: Use the large graph of the 1st assignment

Repeat the same steps described in Part 1 with the realistic graph you have chosen for the 1st assignment.

The two images below provide an example of a student who worked on a power grid dataset and show possible analysis that can be performed for this assignment.



From this plot, we can notice that the critical threshold for the random failure scenario is roughly f = 0.6 (as reported also in a table in the last lecture's slides).
In addition, the power grid network seems to be very vulnerable to target attacks towards hubs and nodes with high betweenness as we have seen in the previous synthetic simulation on the Barabasi-Albert model.
However, in this case the critical point in the random failure scenario is not absent but quite evident because the network is not actually a scale-free network.



Moreover, these two last plots show how target attacks towards nodes with high betweenness and closeness have a significant impact on the diameter and average shortest path, while hub attacks seem to have an impact more similar to that of random failures.
This happens because, as we have seen in the plots collected in the second laboratory, there is no correlation between degree and betweenness/closeness. Therefore, attacking hubs is quite similar to a random failure.
On the other hand, we have seen that nodes with high betweenness usually have also high closeness and vice versa, so attacking this nodes has a significant impact on the diameter and on the average shortest path.

Last modified: Thursday, 22 April 2021, 10:55 AM

◄ Exercise num 7. Analyse a real (relatively small) graph

Jump to...

Slides and papers ►