**Robustness Analysis of Social Networks under Different Attack Models**

**Introduction**: Cascading failures can be observed in many social networks, from electrical grids to disease spreading. In its broadest sense, it refers to a complete or partial collapse of a network due to the initial fault starting at a small part of the network. For example, in electricity grids, this might be caused by a random attack on a particular transmission line. In disease spreading, this might be caused when a particular disease becomes epidemic at a single city. This initial fault in the network keeps triggering other faults at other parts of it, and eventually spreads to the whole network.   
  
**Model**: The model is based on the scenario of disaster spreading. It consists of a graph with N nodes and S links, with and with . During the cascading failure, disaster spreads in time. Initially, at time (t)=0, we assume all nodes is at state . This represents the normal function of the nodes. This functioning is disturbed when the neighboring nodes encounter some disturbances. However, these nodes have the so-called threshold parameter for resistance. When the sum of neighboring disturbances add up, and exceed this , we assume this node fails. The interaction of a node with neighboring nodes is modeled by the following first-order differential equation:

Where

(2)

In equation (1), the first term represents the ability of a node to recover from external disturbances. The second term represents the net affect towards a node due to disturbances at its adjacent nodes; the recovery rate is denoted by . The function reflects the robustness of a node to external disturbances, where is the out-degree of node j. In equation (2), is the gain parameter.

**Abstraction of the Problem and the Goal**: With this differential equation, disease spreading in a social network (like cities or countries) will be investigated. Our analysis is based on N-1 contingency. Meaning, it will be investigated whether or not the system is robust under single node failure; here failure implies node being infected by a disease. The goal of the project is to run N-1 contingency analysis with each of the nodes of the network attacked, for various kinds of real and artificial networks, and investigate which network is the most robust one. Various attack models will be used in the project-

(1) Targeted attacks

(2) Random attacks

(3) Attack under certain probability distribution

The number of nodes that fail, under the attack of initial node, will be registered. The same will be done for all the nodes in the network. The result will be averaged out and normalized with the system size and threshold parameter of the network. This will be done for several real and artificial networks, and the result compared to see the robustness of these networks under these attack models. Ultimately, the aim of this project is to construct a weighted robustness metric for social networks, which can very well be used across many disciplines like gas flow network, electricity grids, etc. given the dynamics of the cascading failure follows equation (1). In addition, the evolution of cascading failure will also be investigated in the project. In other words, number of nodes that fail in each iteration also will be recorded, and the evolution of failing nodes displayed for each iteration.

Reference: The model for this project is adapted solely from the following paper:

*Efficient Response to Cascading Disaster Spreading, Dirk Helbing et al 2008*

Group: Manish Jung Thapa, Dinesh Acharya, Partha Ghosh