The Impact of Imperfect Information on Network Attack

J. Caloca (Boise State University), A. Melchionna (University of Rochester)
S. Squires, M. Girvan, E. Ott, T. Antonsen (University of Maryland)

ABSTRACT

A complex network can be used as an effective basis for modeling systems in which connectivity is important. Examples include the internet, social networks, and genetic regulatory networks. We study the effect of attacks on complex networks, where the assumed purpose of the attack is to reduce the size of the largest connected component of the network. We consider attacks that consist of successive removal of network nodes, and we evaluate the impact of the attacker having imperfect information about the network (i.e., false and/or missing network links). We observe that dynamical importance and betweenness centrality-based attacks are surprisingly robust to the presence of a moderate amount of imperfect information and are more effective compared with simpler degree-based attacks.

BACKGROUND

• A network is a set of N nodes connected by M edges (or links).
• The giant connected component (GCC) is the largest interconnected subnetwork.
• An important question in these systems is how the GCC disintegrates when nodes are removed via different “attack” strategies.
• Many real world networks are inferred from imperfect information. Our goal is to understand how imperfect information impacts the effectiveness of attack strategies.

METHODS

Imperfect Information

We introduce imperfect information by defining two types of noise (link errors), generating a noisy network from a true network:

- αM false links are added between random node pairs, with α ≥ 0.
- A fraction, δ, of all links in the true network are deleted, with 0 ≤ δ ≤ 1.

Attack Strategies

Attacks proceed by successive node removals, with nodes chosen according to a measure redetermined after each removal. Three such measures are considered:

- The degree (DEG) of a node is the number of edges connected to the node.
- The betweenness centrality considers the shortest paths between all pairs of nodes. The betweenness (BTW) of a node is the number of such paths that run through it.
- The dynamical importance (DI) of a node is determined from the network adjacency matrix: Aij = 1 if there is a link from node i to node j and is zero otherwise. (For undirected networks Aij = Aji.) The dynamical importance of a node is the change in the largest eigenvalue in response to the node’s removal.

RESULTS

• We plot the size of the GCC in the true network as a function of the fraction of nodes removed, using attack strategies made based on information in the noisy network.
• True networks studied here are undirected Erdős–Rényi random networks, in which M node pairs, chosen uniformly at random, are connected by links.

The Case of Perfect Information

- With perfect information (α = δ = 0), Betweenness and Dynamical Importance attack strategies destroy the GCC after removing 25% of nodes.

The Effects of False Links

- We consider the effectiveness of attack strategies when they are determined from a noisy network, with α = 0.25 and δ = 0:

- Betweenness and dynamical importance strategies remain effective even with a large number of false links added (α = 0.25), taking only 0.5SN more nodes to destroy the GCC than in the noise-free case.
- To illustrate the impact of false links, we plot the area under the GCC curve for a range of values of α, with δ = 0.

RESULTS, Cont’d

• We see that dynamical importance and betweenness based attack strategies remain effective as α is increased to 0.50.

The Joint Effects of False and Missing Links

• Here we show the effectiveness of betweenness and dynamical importance attack strategies under perfect information (α = 0, δ = 0) and in cases of imperfect information with false (α = 0.25) and/or missing (δ = 0.25) links.

- A significant number of missing links diminishes attack effectiveness more than the same number of additional false links.

CONCLUSIONS

• The more sophisticated attack strategies remain effective even when the network information contains a significant number of link errors.
• The effectiveness of attack strategies is more robust to the addition of false links compared with the deletion of true links.
• We have also obtained results for directed networks and for true networks with more structure than the Erdős–Rényi random networks considered here. We find that the above conclusions also apply in these cases.

References:


REU program sponsored by the National Science Foundation Award Number: PHY1156454