Erick Luerken
CS790R

Gorman et. Al. Review

- We first went over the basis of the paper.
  - We want to find the Vulnerable Pts. of the Internet
    - Where are it's Physical Vulnerabilities?
    - Where are it's Digital Vulerabilities?
      - Where are Hub routers?
      - How are they distributed?
- Discussed the Basic Setup of the Digital Network
  - Coasts of the the US are better connected to each other (i.e. LA to NY) better than the interior of the country
  - "World Cities" tend to serve as Hubs (i.e. NY, LA, etc…,)
  - End result is that the internet has become more self-organized
    - Means the network is more efficient
    - Also more sparsely connected
- We glossed over the fact that the paper gives a basic review of different types of networks (i.e. small-world, random, etc…,) but we didn't discuss this as it was just a review
- We then talked about the resiliency of the internet
  - It is highly resilient to random error/attacks on hubs
  - However what makes it resilient to the random failures makes it highly vulnerable to a coordinated/directed attack on hubs.
- The majority of the talk focused around how to find the hubs
  - Several methods were proposed. Based on those methods, which follow below, rankings were generated.
  - Binary approach (count the number of links at each node
  - Accessibility index (count the number of nodes and find the capacity of each of the lines
  - Make Regions & find the number of local (i.e. connections within a region) and global links (i.e. from one region to another)
    - Model seems reasonable, but a possible drawback is that cities on the borders of a region may appear to be a global hub
  - Pick a radius and for each city, anything within the radius is considered local, and anything beyond the radius is considered global.
    - Radius was determined by testing the Global to Local Ratio at increasing distances, and the point of inflection was found to be at 300 miles.
      - 300 miles is also close to the mean distance of all links
  - Small World Approach which picks the number of links to a node beyond a fixed distance

    - Final Approach was to identify relay node hubs (i.e. nodes that aren't the origin or destination, but are traveled through most often to get from one point to another
- We described the model briefly, noting that the source that they were drawing from (Internet providers maps) are largely inaccurate.
- The Primary method of determining the effect of the attacks was by examining how the "diameter" of the internet (i.e. The maximal "shortest path" between any two distinct nodes) changes when primary nodes are removed based on their rankings established by the methods listed above.
    - There was another method of ranking, the S-I index which was a stastical measure based on the ratio of several moments of the distribution of shortest path lengths, though we weren't quite sure what these ratios were supposed to imply
- We then examined the results, which showed that attacks based on the Small-World Hierarchy and the Global Hierarchy had the greatest effect on the network.
    - The results showed that the internet is more resilient than claimed by earlier papers
    - Another key results was that this showed that distance still plays an important role in determining the most crucial nodes.
- We briefly discussed the importance of the physical structure of the network, which examined the effect of removing the cable from Denver to Kansas City and/or the cable El Paso to Houston would have on the rest of the network.
- Due to the length of the paper, there wasn't a lot of extraneous discussion, as it took most of the period to cover the topics of the paper, and most of the discussion that occurred was covered in the bullets listed earlier, outside of mentioning the number of typos and grammatical errors in the paper.