ASSESSING NETWORK RESILIENCY USING CENTRALITY TECHNIQUES

Mahyar A. Amouzegar, *Department of Economics and Finance, University of New Orleans, New Orleans, LA 70148, 504-280-6595, mahyar@uno.edu*
Khosrow Moshirvaziri, *Department of Information Systems, California State University, Long Beach, Long Beach, CA 90840, 562-985-7965, moshir@csulb.edu*
Michael Shafae, Department of Computer Science, California State University, Fullerton, Fullerton, CA 92831 657-278-3291, mshafae@fullerton.edu

ABSTRACT

We apply various graph theoretical methods to show resiliency of communication networks under directed or random attack. We illustrate these methods with two illustrative examples, based on military communication system and terrorism network.

BASICS OF GRAPH AND NETWORK THEORY[1]

Graph is a set of points in a two or three-dimensional space and lines that join these points including joining a point to itself (i.e. a loop). Mathematically, a graph $G = (V, E)$ is defined by two finite sets *V* and *E*. The elements of *V* are called vertices (or nodes), and the elements of *E* are called edges (or arcs). Each edge has a set of one or two vertices associated with it, called its endpoints.

A graph may also be viewed as a collection of distinct or overlapping graphs. That is, graph may be defined as a set of sub-graphs. If every pair of vertices is joined by an edge then a graph is called *complete* and has no sub-graphs. Graphs may be bidirectional (i.e., both directions of the flow are allowed) or unidirectional (i.e., only a one-way traffic allowed). A Graph with all directed edges is called a *directed graph* or *diagraph*. A graph with a mix of direction is called a *mixed graph* or a *partially directed graph*. Finally, when a graph has neither self-loops nor multi-edges (multiple edges with identical end-points) then it is called a *simple graph*. Most graphs can be converted to a simple graph by adding redundant vertices and therefore for the remainder of this paper and unless it's specified we will use the term graph to mean simple graph.

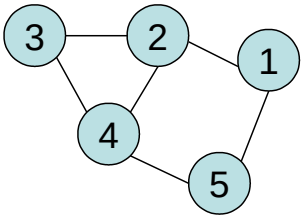
Another important concept is the *degree* (or *valence*) of a vertex in a graph. A degree of a vertex *v*, denoted by *deg(v)*, in Graph G is defined as the number of proper edges incident on vertex *v*. Two new terms are required to represent a graph by a matrix. If vertex *s* is joined to vertex *t* by an edge then we say vertex *s* is an adjacent or a neighbor of *t*. Therefore, a graph can be formally represented by a matrix of neighboring vertices. This type of matrix is called an adjacency matrix with a row for each vertex containing the list of neighbors of that vertex (see Figure 1). The matrix denoted by A_G is a symmetric matrix with its rows and columns representing the ordering of the vertices such as

$$A_G[s,t] = \begin{cases} 1 & \text{if s and t are adjacent} \\ 0 & \text{otherwise} \end{cases}$$

[1] For a more detailed description of graphs and its properties see [1]

NETWORK TOPOLOGY

A network topology represents the structure of the connectivity amongst the vertices (i.e. connections of edges and vertices). The distance from vertex *s* to vertex *t* is denoted by *d* (*s*, *t*) and is the length of *shortest path* or a *geodesic path* from *s* to *t*, if one exits. The length (in number of edges) of the longest geodesic path between any two vertices is called the *diameter of the graph*. The diameter of the graph is also sometimes called the average geodesic distance in a graph. In Figure 2, three different types of network topologies are presented, where from left to right the dependency of the network on a single vertex increases.



$$A_G = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

Figure 1: A Simple Graph and its Adjacency Matrix

RANDOM GRAPHS AND SCALE FREE GRAPHS

Most common random graph is the so-called Erdös–Rényi denoted by G(n,p), in which every possible edge occurs independently with probability p. [2, 3] In general, the probability that a graph has *m* edges is $p^m(1-p)^{M-m}$ where, $M = .5n(n-1)$ is the maximum possible number of edges. A closely related model, assigns equal probability to all graphs with exactly M edges. This graph can be conceptualized as starting with *n* vertices and no edges and at each step adding one new edge chosen uniformly from the set of missing edges.

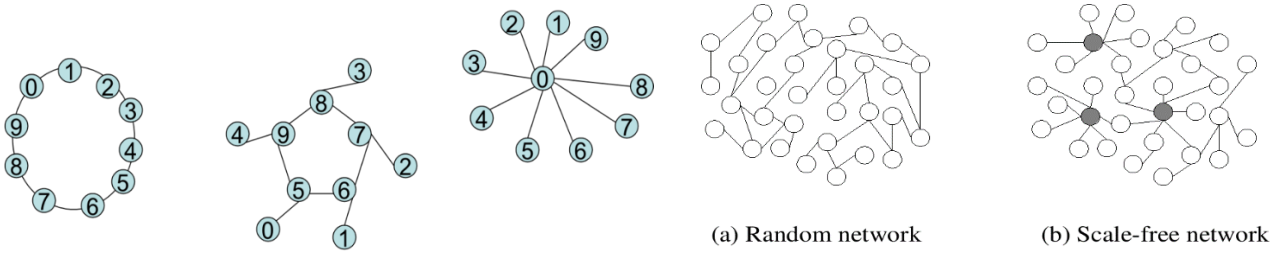


Figure 2: Network Topology

Another related graph is the so-called infinite random graph, where the starting point is an infinite set of vertices with every possible edge occurring independently with probability *p*. Except in the trivial cases when *p* is 0 or 1, an infinite random graph has the property that for any *n* + *m* elements $a_1, a_2, ..., a_n, b_1, b_2, ..., b_m \in V$ there is a vertex $c \in V$ that is adjacent to each of $a_1, a_2, ..., a_n$ and is not adjacent to any of $b_1, b_2, ..., b_m$.

The theory of random graphs studies typical properties of random graphs, those that hold with high probability for graphs drawn from a particular distribution. We may be also interested in computing the probability distribution of a graph. In a Poisson degree distributed graph, the probability that a vertex has degree *k* is given by

$$p_k = \binom{n}{k} p^k (1-p)^{n-k} \cong \frac{\mu^k e^{-\mu}}{k!}$$

where the last approximate becomes in equality in the limit for large *n* and fixed *K* and $\mu = np$, hence the term, *Poisson random graph*. This type of networks has many desirable properties, in particular despite the random placement of links between the nodes, the behavior of the resulting system can be calculated exactly. The most interesting property of random networks is that they exist in two different systems. The network, depending on the exact distribution of the degrees of vertices, may either be made up of many small clusters of vertices connected together by edges (i.e., components) or it may contain a group of connected vertices that form a significant portion of the whole network (i.e., *giant component).* The latter regime's size scales up with the size of the whole network.

The nature of random networks makes them susceptible to accidental (or random) failure. That is a random network can become fractured (and develop into non-communicating networks) very quickly by accidental failure of a number of nodes. Examples of such network failure include cascading effect of energy surge in a power grid, or damage to oil flow through a pipeline system. It should be noted that global cascades in most real-life networks (e.g., economic systems or engineered networks) occur rarely but when they do, it is large. It has been argued under different conditions, a random network may exhibit both types of behavior [4]. For example, in a sparse network, the cascading effect is limited due to the global connectivity and when the network is dense, it is kept at bay by the stability of individual nodes. On the other hand, in a sparse network, surges follow a power-law distribution at the corresponding critical point and the most highly connected nodes are critical in triggering cascades. In the dense network, nodes with average connectivity are more likely to trigger cascades given their large numbers in the system. If random networks described above resemble the U.S. highway system (i.e., cities connected to other cities following a bell curve distribution) with most nodes (cities), on average, having the same number of links (roads) then in contrast, the airline transportation system would be a network that has some (few) nodes (hubs) with a large number of links.

Diverse systems with complex topology such as genetic networks or human interaction seem to have developed a common property in terms of how their vertices connected to each other. The vertices in these systems tend to follow a scale-free power-law distribution. Such networks have been, in recent year, the focus of great deal of attention and have been referred to as *scale-free networks* [6] (See Figure 2: b). In particular, researchers who were attempting to map the World Wide Web were surprised to learn that only a relatively few web pages were highly connected. "More than 80 percent of the [web] pages on the [network] map had fewer than four links, but a small minority, less than .01 percent of all nodes, had more than 1,000" [6]. One of the key characteristics of scale-free network is its resiliency against random or accidental failure. The reliability of scale-free networks allows the Internet to function properly despite the routine failure of thousands of routers at any given time. The same resiliency allows living system to function despite thousands of errors in cells development or mutation. In general, scale-free networks have amazing tendency to manage and respond to random failures. In contrast, scale-free networks are susceptible to coordinated or focused attack or disruption. Moreover, scale-free networks have exhibited key dynamical advantage over other types of network topologies (and possibly the reason for their prevalence in biological systems) [7].

TYPES OF NETWORK FAILURES

Network failures can be classified into three categories: node (vertex) failure, edge (arc) failure, and path failure.

- **Vertex failure**: Hardware or human error as well as malicious attack may cause vertex failure. Vertices could be networking devices such as routers or a transceiver.
- **Edge failure**: Physical or electronic attack on an edge (arc) may cause losing network connectivity. Physical attacks may include cutting of fiber optics, damage to switching equipment.
- **Path failure**: Failure of consecutive edges is referred to as path failure. Denial of Service (DoS) attacks or routing loops are examples of such failures. One method attack on path is the DoS attack with packet flooding [8].

CENTRALITY AND OTHER METRICS

In a social context, a member with a favored position (e.g., popularity in a social network, or economic might in a business transaction) can extract better bargains in exchanges, exerts greater influence and is a focus for deference and attention (positive or negative) from those in less favored positions.
The relative power of individuals and institutions, or in terms of graph theory, the relative importance of a node in a graph, is determined by the various measures of the centrality of a vertex within a graph. These centralities measure the importance of a person within a social network, evaluate the importance of a service desk in a large complex, or compute worth of a computer or a server within a network.

Degree

A degree is simply the number of direct (adjacent) neighbors of a node (i.e. number of nodes that a given node is connected to). For example, if a graph represents a social network of who knows whom, degree centrality is the number of people that a given person knows. A degree centrality is the number of degrees in a nondirected graph.

Betweenness

A central notion in graph theory is the concept of the shortest path between two vertices. Loosely speaking, betweenness centrality is defined as the number of geodesic paths that pass through a node. It is the number of "times" a node acts as a bridge along the shortest path between two other nodes. In general, betweenness centrality $C_B(v)$ of a vertex v is the total number of shortest paths between all possible pairs of vertices that pass through this vertex. Vertices that occur on many shortest paths between other vertices have higher betweenness than those that do not.

Closeness

Closeness is defined as the total graph-theoretic distance to all other nodes in the network. For example, in Figure 3 below, node 4 has a closeness score of 8 because it is one link away from 1, two links away from 2 and 5, and three links away from 3. It should be clear that the lower this number the more central the node and when node is highly central (i.e., a low closeness value) it tends to receive anything flowing through the network "very quickly".

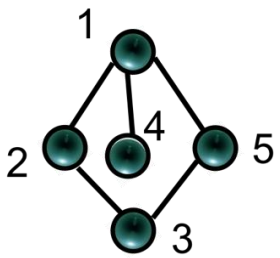


Figure 3: Closeness Centrality

MODELING NETWORK THREATS

A typical mission or operation may be mapped onto an end-to-end network, which may include missions/operations packages, nodes of operations, command and control and communication. Each mission is a complex network, connecting various operational nodes. An example of a mission network with 104 nodes of operations, average degree of 3.56, and max degree of 14 is illustrated in Figure 4.

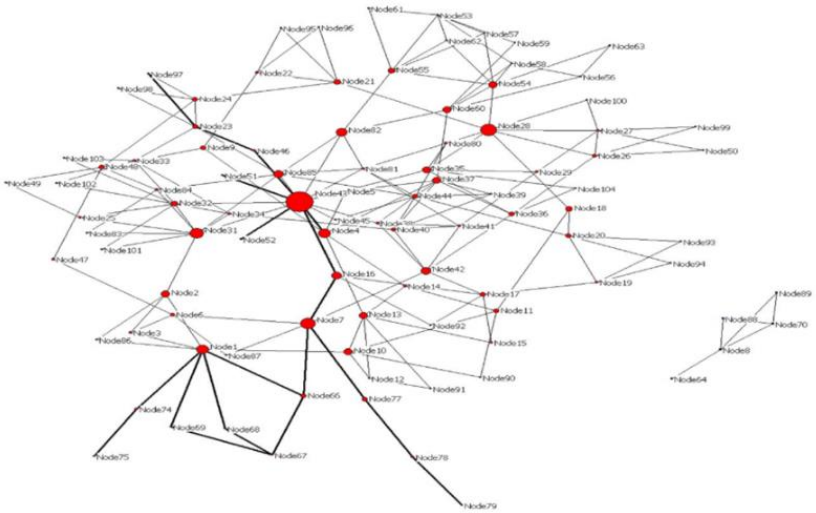


Figure 4: Mission Network

If we compute betweenness centrality (see Figure 5), important nodes appear with their valued rank. For example, node 43 (degree14), node 28 (degree 8) and node 7 (degree 6) have become key nodes in this network

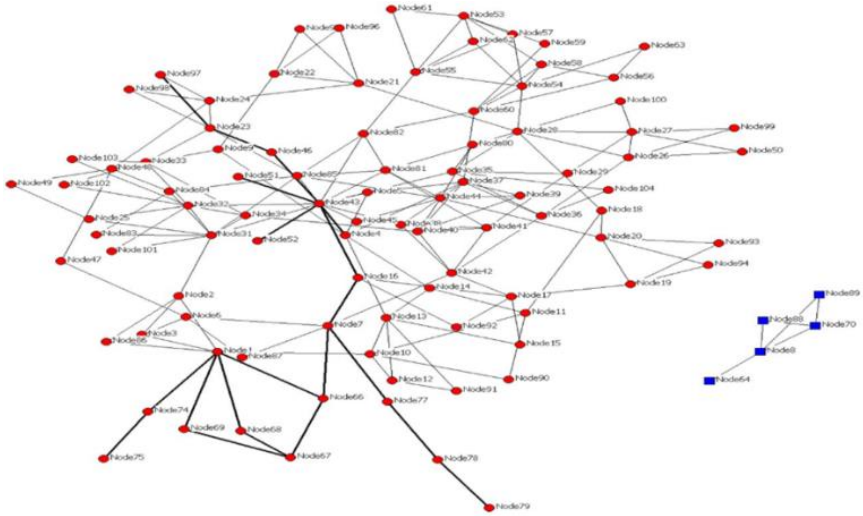


Figure 5: Betweenness Centrality

Table 1 shows the results of our network analysis using betweenness and degree centrality measures. Key common nodes across various centralities are highlighted in the table. What we can learn from this analysis is that attack based on betweenness centrality (
) is effective. For example, by attacking nodes 7, 28, 31 and 43, we can isolate and create four different islands. However, the core of the network is still intact and therefore the systems is functioning with some degree of reliability.

Table 1: Results of Network Analysis

Betweenness	Degree
Node 43	Node 43
Node 28	Node 31
Node 7	Node 1
Node 31	Node 28
Node 1	Node 32
Node 4	Node 37
Node 82	Node 44
Node 85	Node 54
Node 16	Node 85
Node 42	Node 13

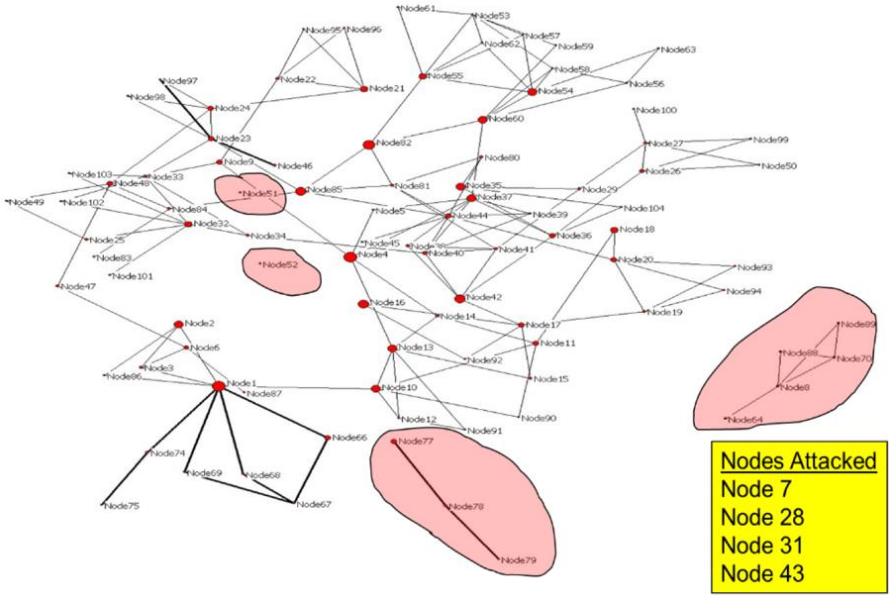


Figure 6: Centrality Attack

A judicious attack based on a dynamic analysis, however, provides a better result. For example, attacking only three nodes, in particular nodes 1, 7, and 43, would have a large impact on the network (Figure 7).

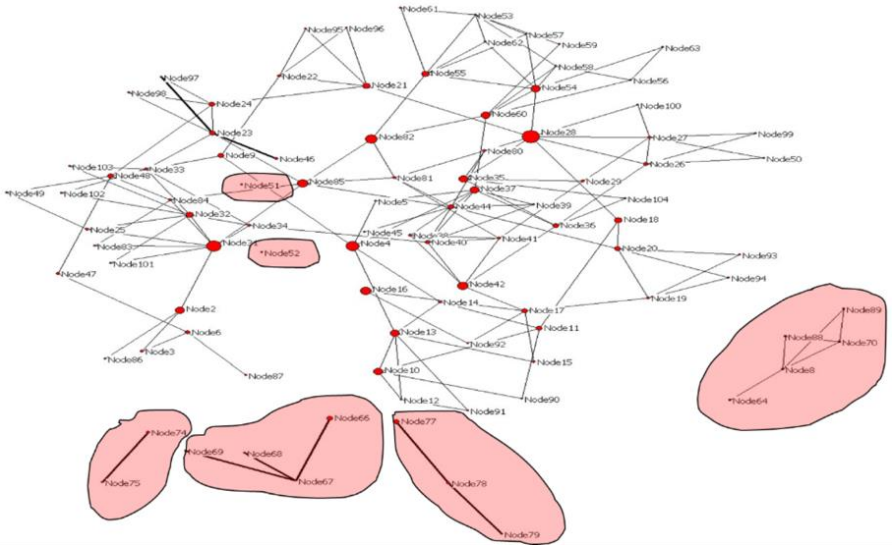


Figure 7: Dynamic Attack

REFERENCES

[1] Gross, J.L. and Yellen, J., Graph theory and its applications. Chapman and Hall/CRC, 2005.

[2] Erdös P. & A. Rényi. On Random Graphs, Publ. Math. Debrecen 6 (1959), 290-297.

[3] Solomonoff, R. and A. Rapoport, Connectivity of Random Nets, Bulletin of Mathematical Biophysics, 13 (1951)

[4] Watts, Duncan, "A Simple Model of Global Cascades on Random Networks," Proceedings of the National Academy of Sciences, Volume 99(9), PP 5766-5771, 2002

[5] Barabasi, A., R. Albert, Emergence of Scaling in Random Network, Science, PP 509-512, Volume 286, 15 October,1999

[6] Barbasi, A., E. Bonabeau, "Scale-free Network", Scientific America, May 2003

[7] Willeboordse, F., "Dynamical Advantages of Scale-free Networks," Physical Review Letters,Volume 96(1), 2006

[8] Garber, L., Denial of Service Attacks Rip the Internet, Computer, Volume 33, PP12-17, April 2000.