Engineering Networks for Optimal Robustness

Christopher A. Wood
Department of Computer Science
Rochester Institute of Technology

Abstract

Due to the growing pervasiveness of civilian and military networks for the transmission of safety-critical and real-time data, it is critically important that they are resistant to selective and random network node deletions. Network robustness is a measure of the performance and throughput responsiveness of a network in response to such deletions. The nature of this metrics lends itself to the application of percolation theory, which can be used to describe the behavior of connected clusters in a random graph. This theory can be utilized to design and construct optimally robust networks in order to yield the best performance in the event of node deletions. This paper presents some background information on network robustness and its importance in modern communication systems, with a specific focus on wireless sensor networks, presents some recent advances made in the topic, and concludes with avenues of future work that can be explored by researchers in the field.

Introduction

Military and civilian communications have seen two common trends in rencent years: an increase in network-oriented operations and an increase in high-risk malicious attacks against networks that facilitate such operations (?, ?). In order to sustain this growth pattern such operations, it is vital they their underlying network infrastructure can defend against emerging attacks that focus on specific nodes or links in the network or random failures that occur throughout the network. The measure of resilience to such attacks or failures is referred to as the robustness of a network, and is a topic that has been analytically and experimentally studied extensively in recent years.

The physical properties of networks (i.e. the channel bandwidth, routing protocols, transmission media) have an a significant effect on the measure of robustness of a network. However, recent research efforts have approached this problem from the topological domain and studied it using analytical methods from graph theory and statistics in order to solve more general questions about the relationship between the structure of a graph and its robustness.

Adapted (and at times just copied) from a similar document by Athanassios Protopapas who is at the Institute for Language & Speech Processing Athens, Greece. (email: protopap@ilsp.gr)

William Revelle may be contacted at `email:revelle@northwestern.edu)`

In this paper we focus on recent research that has been centered around the theoretical analysis of graph topology and its impact on the robustness of a network. We also discuss some of optimization techniques that have been applied to further such results about the topology of specific graphs. In doing so, we also discuss some of the common sources of topology changes (e.g. attacks and failures).

Fundamentals and Notation

It is natural to model a communication network as a weighted undirected graph $G = (V, E)$, which has a fixed set of vertices (nodes) V and edges (links) E that represent physical connections between such vertices, and weight for each link. For conveniene, we let $N = |V|$ and $M = |E|$. The topology of a network can thus be visualized graphically using elements from these two sets. For the remainder of this paper, we use the term vertex as a synonom for node and edge as a synonom for communication link.

In order to discuss the measures of network robustness and analytical techniques used to study the network robustness in the topological domain, it is necessary to introduce the following definitions.

Definition 1. The **degree** of a vertex $u \in V$ for any graph $G = (V, E)$ is said to be the total number of edges incidenct to u. In other words, $deg(u) = \sum_{(u,v)\in E} 1$ for all $v \in V$. We denote the minimum degree over all vertices in a graph G as $\delta(G)$. In network analysis it is common to utilize the degree distribution of a graph as the basis for many measurements. As such, we denote k as the average degree distribution for a graph G.

Definition 2. A **component** of a graph $G = (V, E)$ is a subgraph $G' = (V', E')$ in which there exists a path between all vertices $u, v \in V'$. Further, a graph G is said to be **connected** if and only if there is at most 1 conneted component in G (i.e. the entire graph). If a graph is not connected, then it is **disconnected**.

Definition 3. The **vertex connectivity** of a graph $G = (V, E)$, denoted $\kappa(G)$, is defined as the minimum number of nodes whose deletion will leave the graph disconnected. Similarly, the **edge connectivity** of a graph G, denoted $\lambda(G)$, is defined as the minimum number of edges whose deletion will leave the graph disconnected.

Definition 4. The **distance** between any two vertices $u, v \in V$ in a graph $G = (V, E)$ is defined as the sum of the link weights along the edges that correspond to the shortest path between u and v.

Network Functionality

Network engineers strive for high performance networks that exhibit high throughput and low latency between any two nodes in the same network. Other similar quality metrics include the number of hops between nodes, the distance between two nodes, the jitter on the transmission medium, the loss rate, and the bandwidth (or capacity) of the channel (?, ?). These quality paremeters are often used to assign weights to the links in a network in order to determine the optimal network designs using mathematical analysis.

In this paper, we refer to the weight of communication links as an arbitrary linear combination of such quality metrics that can be modified by the author during analysis of the underlying weighted graph that represents a network with certain quality metrics. Several mathematical metrics based

on the corresponding graph that represents a network have been proposed to reflect this need. For example, metrics such as the average geodesic path length between any two nodes in a network, which equates to the average shortest path) and vertex and edge betweeness (which are essentially measures of centralities located within a graph).

The average geodesic length L can be defined as follows,

$$L(d(v,w)) = \frac{1}{N(N-1)} \sum_{v \in V(G)} \sum_{w \neq v \in V(G)} d(v,w),$$

where $d(v,w)$ is the distance of the shortest path between vertices v and w, and $N(N-1)$ is the total number of pairs of vertices, independent of whether or not each pair represents an edge in $E(G)$. The most immediate result from this measurement is that large values for L indicate that the average length between any two nodes in the network is long, and thus the latency between two nodes will be proportionally large as well.

Another important metric that measures the functionality of a network is the measure of vertex and edge centrality in the network. Although a high measure of centrality may indicate more traffic funnels through a vertex or an edge, it also implies that any attacks on this vertex or edge would most likely have an negative impact on the traffic in the network by increasing the load on neighboring nodes and increasing the average geodesic path length. Although there is not a single definition for this metric, Holme et al (?, ?) propose the use of the following definitions for vertex, $C_B(v)$ and edge $C_B(e)$ centrality.

$$C_B(v) = \sum_{w \neq x \in V(G)} \frac{\sigma_{wx}(v)}{\sigma_{wx}},$$

where $\sigma_{wx}(v)$ is the number of paths between w and x that pass through v and σ_{wx} is total of paths from w to x (notice that $\sigma_{wx}(v) \leq \sigma_{wx}$).

$$C_B(v) = \sum_{w \neq x \in V(G)} \frac{\sigma_{wx}(e)}{\sigma_{wx}}$$

As in the centrality measure for vertices, $\sigma_{wx}(e)$ is the number of paths between w and x that contain e and σ_{wx} is total of paths from w to x (notice again that $\sigma_{wx}(e) \leq \sigma_{wx}$).

It is important to note that the centrality of a vertex and its measure of centrality are not the same metrics. In fact, as will be shown in section **??**, network attacks can vary based on the measure an adversary is trying to reduce.

Attack Models

Attacks on large scale networks are not usually ad-hoc; they are based on a logical and structured strategy for dereasing the connectivity of the network by taking as little action as possible. Clearly, if one was to delete all nodes from a network, then that would yield the maximum decrease in connectivity. However, such attacks are not practical, so these strategies must be considered at a smaller scale.

From a general perspective, practical attacks are theoretically focused on the objective of decreasing the number of total links in the network or the average geodesic length (or both). Consider, for example, the situations of cutting communication cables or performing a DDOS attack

on a node or server with a high measure of centrality. Such attacks would decrease the number of edges in the network graph and increase the average geodesic path length, respectively.

From the definitions presented in section **??**, we can see that the number of edges in the network is directly related to the degree of each vertex (in fact, we know that $2|E(G)| = \sum_{v \in V(G)} deg(v)$). On the other hand, the measure of centrality of a vertex or edge is more related to the average geodesic path length in the network. As such, we consider practical attack patterns that focus on decreasing both of these measurements by targeting individual vertices and/or edges, as well as randomized attacks that have no specific targets.

In general, most focused attacks fall under one of the following four categories (?, ?).

- **ID removal** - initial degree distribution vertex/edge removal
- **IB removal** - initial betweenness distribution vertex/edge removal
- **RD removal** - recalculated degree distribution vertex/edge removal
- **RB removal** - recalculated betweenness distribution vertex/edge removal

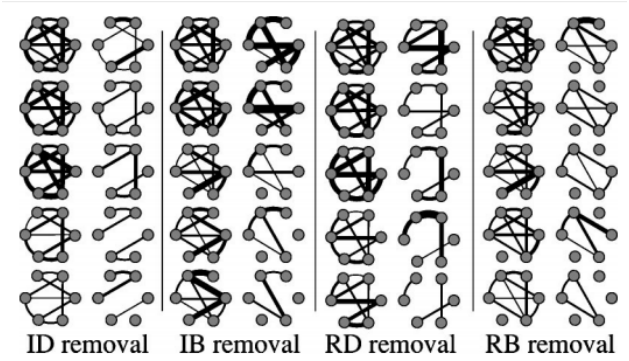

Figure 1. Various edge-centric attacks for a fixed graph topology.

RD and RB attacks on vertices yield the optimal results because they take a greedy approach to decrease the target metric. However, the implication of these attacks is that there exists an efficient and tractable way to measure these metrics after every change, which isn't always the case (especially when the topology of the network is unknown). Therefore, ID and IB attacks are more realistic, but they also assume some prior knowledge of the network infrastructure before the attack begins. Attacks that do not rely on this knowledge are referred to as random attacks, and are discussed in section **??**.

Furthermore, it should be noted that both the ID and RD attacks are computationally less taxing than IB and RB attacks (?, ?). In fact, the time complexity of a successful ID attack (and subsequently, an entire RD attack), runs in linear time with respect to N, whereas the time complexity of betweenness-based attacks has a time complexity of $O(NL)$. The implication of this is that the adversary must make tradeoffs based on their knowledge of the network infrastructure.

Random Failures

While targeted attacks model common scenarios in the real-world, it is often useful to disregard the source of and victim of such attacks and generalize the problem of network failures to encompass both random node and link failures. By doing so, we assume that each node and link has a fixed probability p and q of failing, where the exact cause of the failure is not know and is not important.

Furthermore, failures are typically seen as independent events (?, ?). Such models are useful when analyzing complex networks such as the Internet and other related military communication networks.

Network Robustness

Many different measures for network robustness have been proposed in recent years, all of which tend to use the notion of densely connected components in the corresponding graph.

Robustness Measurements

A natural way to think of network robustness is from the perspective of individual nodes, since they are usually the primary targets in malicious or non-malicious network attacks. Using this idea, Herrmann et al defined a concise equation for calculating the robustness of a network based on the size of connected components in the corresponding graph that is adapted from percolation theory. Mathematically, this can be defined as follows (?, ?):

$$R_n = \frac{1}{n} \sum_{q=\frac{1}{n}}^{1} S(q)$$

This robustness measurement computes the fractions of nodes in the largest connected cluster $S(q)$ after removing q nodes. This is an intuitive calculation, since the goal of engineering robust networks is to ensure the highest measure of connectivity in the event of any node deletions. Furthermore, it has been mathematically verified to represent the exact amount of nodes that need to be deleted for the network to collapse when targeted by high-degree adaptive attacks, which are a specific class of attacks that attempt to remove highly connected nodes from the network.

Another way to study the measure of robustness of a network is to examine its communication links. From the perspective of such links that exist in a network, the most successful attacks are those that take down the take down the most important or centralized communication links. As such, a common research trend has been to examine the largest components of a network with respect to the edge-betweenness, link clustering coefficient, and degree product (?, ?). One common measurement of the robustness of a network with respect to these metrics and the largest component of a network $S(p)$ is shown below:

$$R_l = \frac{1}{M} \sum_{p=1/M}^{1} S(p)$$

This measurement is mathematically similar to the previous node-based calculation, but instead of considering the density of the nodes in the entire component, it considers the density of the edges.

Due to the typical attacks that are launched on networks, such as large-scale DDoS attacks that take both nodes and links to that node offline, it is natural to extend the concept of network robustness to consider both node and link failures simultaneously. However, rather because the two aforementioned measurements are based on two separate dimensions of networks, it is not simply a matter of merging them together to yield the optimum result. Instead, the measurement is typically abstracted into the context of the attack that is launched on a network, where the input parameter into the largest component is now the number of steps that have been completed at a given instance

in time. Mathematically, this hybrid measurement Q can be computed as follows (?, ?):

$$Q = \frac{1}{M} \sum_{step=1}^{M} S(step)$$

Random Graph Topologies

Erdös-Rènyi Graphs

Erdös-Rènyi graphs are the most simple random graphs that are defined by assigning a probabilistic uniform random variable to each edge. In other words, for each vertex $u, v \in V(G)$, where G is a Erdös-Rènyi graph, the edge (u, v) exists in $E(G)$ with probability p, where p is derived from a uniform random distribution, and each edge probability p is independnt from the rest (?, ?). When simulated using computers, it is not uncommon to derive the edge probabilities p from an exponential distribution, due to its simplicity and similarity with the real-world. Another important element of these graphs is that they tend to have Poisson degree distributions, simply due to the random construction nature of the graph (?, ?).

Scale-Free Graphs

Scale-free graphs are special types of random graphs in that the distribution of node degrees $\langle k \rangle$ asymptotically follows a power law (i.e. $P(k) \approx k^{-\gamma}$). Many real-world networks have been found to have structures similar to scale-free graphs, so they are naturally used as the basis for random graph analysis (?, ?).

Graphs with Bimodal Degree Distribution

Given the average degree k for a graph $G = (V, E)$, we say that a graph has a bimodal degree distribution if its nodes fall under one of two categories (?, ?):

- The local mean degree (k_{loc}) of a vertex v is greater than the average degree distribution. That is, $k_{loc} > k$ for small. Such vertices are often referred to as "super-peers".
- The local mean degree (k_{loc}) of a vertex v is less than or equal to the average degree distribution. That is, $k_{loc} \leq k$ for small. Such vertices are often referred to as "peers".

It is interesting to note that as the number of vertex modes or categories for a graph goes from 2 to ∞, the degree distribution among all vertices in the graphs, and the hierarchy of peers in the graph, will begin to resemble that of a scale-free graph. Therefore, one can think of bimodal graphs as a special case of scale-free graphs that are useful when the power-law nature of the degree distribution complicates analytical efforts.

Robustness Optimization

Due to the complexity that exists in the aforementioned random graphs, most optimization algorithms utilize some large-scale stochastic process (similar to a Monte Carlo simulation) to randomly make changes to graph topology and test its measure of robustness. The exact measurement that is used depends on the type of experiements or simulations being performed. In this section, we discuss a sample of such efforts and the results that were found.

Random and Scale-Free Graph Investigations

Following the insight that hostile vertex attacks that target important nodes with large degrees tend to cause the most significant damage to a network, Albert et al. performed extensive studies on the robustness of random and scale-free graphs.

By examining each of these classes of graphs in the context of random vertex deletions and targeted vertex attacks, it has been shown that random graphs are more robust against intentional vertex attacks, whereas the scale-free graphs are more robust against random deletions. This can be seen in Figure **??**, where the breaking point of the largest component of the graphs S drops off quicker for random graphs when attacked randomly (?, ?).

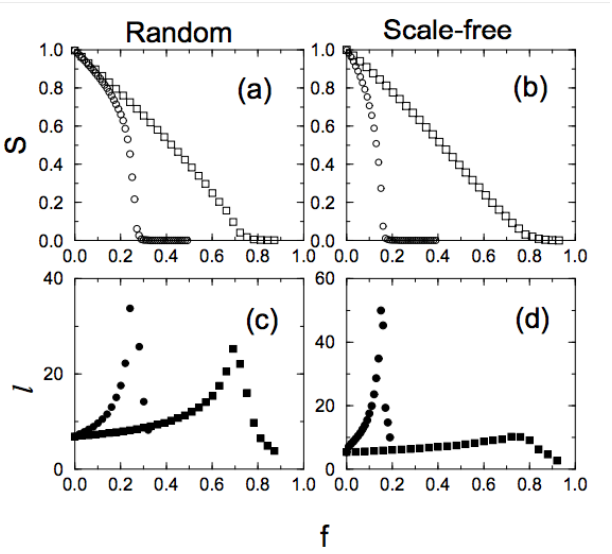

Figure 2. Results of the random and scale-free graphs varied as f, the fraction of nodes removed from each graph, is changed .

Fractional Node Deletion Investigations

Finally, we introduce a metric that characterizes the number of nodes (or rather, a fraction of the total nodes) that need to be removed in order for the graph to become globally disconnected. Let G be a graph with $N - q$ nodes of degree 1. Then, the fraction of total nodes f_c that need to be randomly removed before total connectivity is lost consists of $q = [(\langle k \rangle - 1)/\sqrt{\langle k \rangle}]\sqrt{N}$ nodes of degree $\sqrt{\langle k \rangle N}$.

Paul et al. studied the robustness of random graphs in the context of random node deletions. Their work was driven by Monte Carlo simulations that approximated the fraction of nodes f_c that would need to be removed from random networks in order for the graph to become globally disconnected. Formally, f_c can be defined as in terms of the number of "hub" nodes that must be removed q follows:

$$q = \left[(\langle k \rangle - 1)/\sqrt{\langle k \rangle}\right]\sqrt{N},$$

where each of these vertices have degree $\sqrt{\langle k \rangle N}$ (?, ?). Thus, for a graph with $G = (V, E)$ with N vertices, q "hubs" would need to be removed in order to make G disconnected, and thus $f_c = q/N$.

In terms of the design of a network, it is clear that network designers should strive for values of q that imply high measures of robustness. Such a value of q was determine empirically using a special degree distribution $P(k)$ that represents a network of q hub nodes and $N - q$ leaf nodes, since this is a very general structure for such graphs. The simulation algorithm that was utilized to perform this caluclation is shown in Algorithm **??** (?, ?).

ALGORITHM 1: Monte-Carlo q Determination

1: Initialize a graph G with N vertices.
2: Randomly delete a node in the network and calculate $\kappa(G)$.
3: Increment q by 1 node.
4: If $\kappa < 2$, G has become disconnected, so terminate and return q. Otherwise, decrement q by 1 and go to step 2.

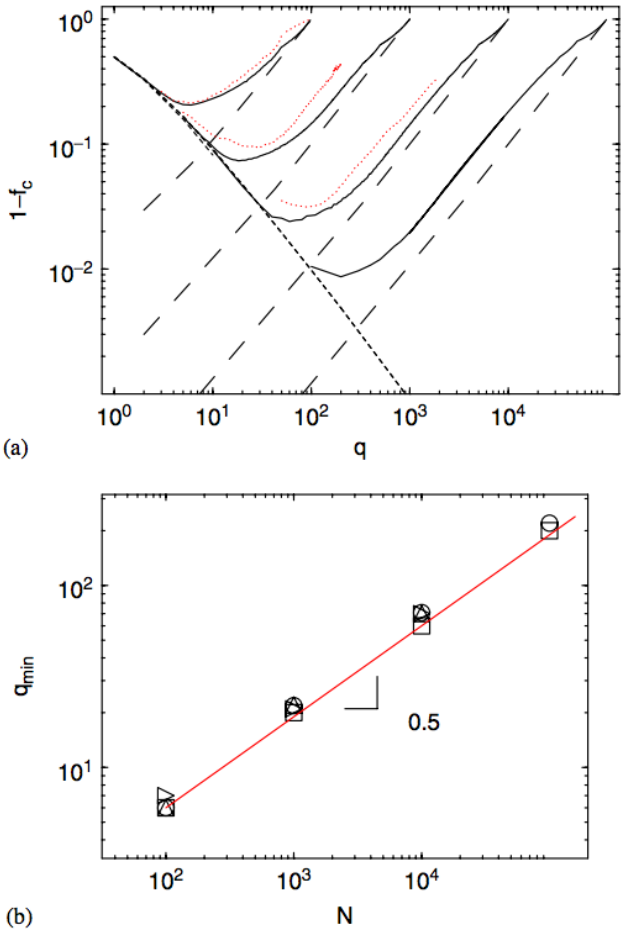

Figure 3. TODO

Fixed-Degree Distribution Investigations

In their study of optimal graph structures that yield the highest resilience to such attacks, Herrmann et al found that most networks will exhibit onion topolgies, meaning that there are distinct layers of nodes that are connected, and that each layer i has more connectivity than its parent layer $i+1$ (?, ?). Another interesting property of the onion graph is that for almost every pair of vertices $u, v \in V(G)$ with the same degree, there exists a a path between u and v that does not contain any vertex of a higher degree. An example of such a graph with 124 nodes and 366 edges is shown in Figure **??**.

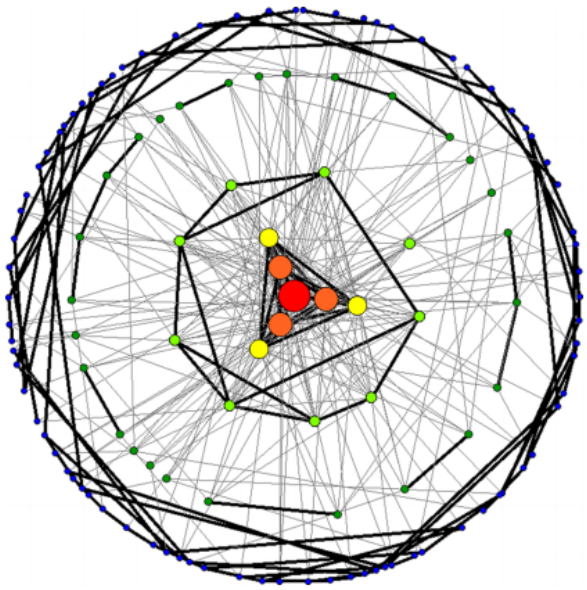

Figure 4. An example of a graph with 124 nodes and 366 edges that exhibits the onion-like topology

Herrmann et al have also conducted research on optimization algorithms that increase this robustness measure while at the same time maintaining the distribution of vertex degrees throughout the network. Their proposed algorithm seeks to re-arrange node edges and connections to improve the resilience of the host network to any kinds of attacks using Monte-Carlo simulations. This algorithm can be described as follows:

ALGORITHM 2: Robustness Optimization

1: Choose two random edges (a, b) and (c, d) from the graph G.
2: Replace these edges with (a, c) and (b, d).
3: If $R_{new} > R_{old}$, accept the swap and go to step 1. Otherwise, revert the swap and goto step 1.

Algorithm **??** is repeated for a very large number of iterations until an ideal level of robustness has been obtained, albiet at the sake of sometimes massive computations (as is the case with Monte-Carlo methods).

One more recent investigation of graphs with fixed degree distributions was performed by Sonawane et al (?, ?).

References

Albert, R., Jeong, H., Barabási, A.-L. (2000, July). Error and attack tolerance of complex networks. , *406*, 378-382.

Bernard, A. D. (n.d.). *Network robustness and graph topology.*

Herrmann, H. J., Schneider, C. M., Moreira, A. A., Jr, J. S. A., Havlin, S. (2011). Onion-like network topology enhances robustness against malicious attacks. *Journal of Statistical Mechanics: Theory and Experiment*, *2011*(01), P01027. Available from `http://stacks.iop.org/1742-5468/2011/i=01/a=P01027`

Holme, P., Kim, B. J., Yoon, C. N., Han, S. K. (2002, May). Attack vulnerability of complex networks. *Phys. Rev. E*, *65*, 056109. Available from `http://link.aps.org/doi/10.1103/PhysRevE.65.056109`

Jenelius, E. (2004). *Graph models of infrastructures and the robustness of power grids.* M. sc. thesis, KTH Royal Institute of Technology.

Sonawane, Abhijeet R., Bhattacharyay, A., Santhanam, M.S., Ambika, G. (2012). Evolving networks with bimodal degree distribution. *Eur. Phys. J. B*, *85*(4), 118. Available from `http://dx.doi.org/10.1140/epjb/e2012-30074-6`

Tanizawa, T., Paul, G., Cohen, R., Havlin, S., Stanley, H. E. (2004, June 23). *Optimization of Network Robustness to Waves of Targeted and Random Attack.* Available from `http://arxiv.org/abs/cond-mat/0406567`

Van Mieghem, P. (2005, oct.). Robustness of large networks. In *Systems, man and cybernetics, 2005 ieee international conference on* (Vol. 3, p. 2372 - 2377 Vol. 3).

Zeng, A., Liu, W. (2012, March). Enhancing network robustness for malicious attacks. *ArXiv e-prints*.