Engineering Networks for Optimal Robustness

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

Abstract

Military and civilian network-oriented operations have followed very high growth rates in recent years. Along with this expansion has been the advancement of sophisticated attacks against such networks and increased probability of network failure. In order to handle such failures, networks must be designed to be robust. The physical characteristics (i.e. the channel bandwidth and transmission media), routing and communication protocols, and the topological properties of a network have a large impact on the measure of robustness of networks to such events. In this paper we present research findings that attempt to measure network robustness, optimize existing network topologies to attain maximal robustness, and even construct arbitrary networks to exhibit high resistance to network failures. In doing so, we also discuss some of the common sources of topology changes in a network that stimulated this research, such as targeted and random network failures. We then conclude with observations about the current state-of-the-art in network structures and their relationship with network robustness, which serve as heuristic guidelines for network engineers when designing such systems.

Introduction

Military and civilian communications have followed two common trends in recent years: an increase in network-oriented operations and an increase in high-risk malicious attacks against networks that facilitate such operations (Bernard, n.d.). It is vital that the underlying network infrastructure for such operations is able to defend against these emerging attacks and other sporadic failures that threaten the functionality of the communication network. This requirement has stimulated research that is focused on improving the stability of communication protocols as a reactive countermeasure to such attacks and failures. In addition, it has also sparked research in the topological analysis of networks as a proactive countermeasure to structural changes in the network. Each of these research avenues seek to improve the resilience of networks to modern attacks and failures, where the resilience is a measurement commonly referred to as network robustness. This metric is a topic in data communications and networks that has been studied analytically and experimentally in recent years.

The physical properties of networks, such as the channel bandwidth and transmission media, have a significant effect on the measure of robustness of a network due to the constraints they place on traffic routing changes in the event of network failures. Similarly, the communication and routing protocols that are utilized to handle the traffic flow also affect the traffic load for individual nodes and links when network failures occurs, which in turn affects the network robustness. However, recent research efforts have approached the study of network robustness from the topological domain. Such an analysis calls on methods from graph theory, statistics, and probability theory in order to solve more general questions about the relationship between the structure of a network and its robustness.

In this paper we survey research that has been centered around the theoretical analysis of network topology and its impact on the measure of robustness. In doing so, we also discuss some common sources of topology changes in networks, including targeted attack models and failures, techniques to measure the robustness of a network, and methods that have been utilized to study and optimize network robustness for random networks with arbitrary structural characteristics.

Fundamentals and Notation

It is natural to model a communication network as a weighted undirected graph $G = (V, E)$, where V is a set of nodes (or vertices) and E is a set of edges (or links) that represent physical connections between such vertices. We also assign weights $w \in \mathbb{R}$ for each edge, where unweighted edges receive a weight of 0. For convenience, we let $N = |V|$ and $M = |E|$. It is now possible to represent the topology of a network using elements from these two sets.

In order to discuss network robustness and analytical techniques used to study it 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 incident to u. We denote the minimum and maximum degree over all vertices in a graph G as $\delta(G)$ and $\Delta(G)$, respectively. 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 and $P(k)$ as the average degree and degree distribution for a graph G, respectively.

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 maximal connected component in G (i.e. the entire graph). A graph is **disconnected** if and only if it is not connected.

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 $G = (V, E)$, denoted as $d(u, v)$, is defined as the sum of the edge weights along the shortest path between u and v.

Network Performance

In general, high performance networks exhibit high throughput and low latency between nodes in the same network. Other quality metrics include the number of hops between nodes, distance between two nodes, jitter on the transmission medium, channel loss rate, and the channel bandwidth (or capacity) (Van Mieghem, 2005). These measurements are often used to assign weights to the links in a network in order to analytically determine optimal network designs. In particular, the weight of links are usually expressed as a linear combination of such quality metrics that can be modified to reflect the real-world nature of the networks. However, when considering only the topology of a network, it is common to assign uniform weights of 1 to all link edges. By doing so, we need only consider the topology of the network when quantifying its performance.

Perhaps the most natural topology-based measurement for performance is the average geodesic path length between any two nodes in a network. This measurement equates to the average shortest path and vertex and edge betweenness (which are essentially measures of centralities within a graph) (Holme, Kim, Yoon, & Han, 2002). Mathematically, the average geodesic length L can be defined as follows:

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

where $N(N-1)$ 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. A high measure of centrality may indicate more traffic funnels through a node or a link, which means that there may be more backup nodes available in the event that this node or link fails. High measures of centrality also imply that any attacks on the associated node or link would most likely have a 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 these metrics, Holme et al. propose the use of the following definitions for vertex $C_B(v)$ and edge $C_B(e)$ centrality (Holme et al., 2002).

$$C_B(v) = \sum_{w \neq x \in V(G)} \frac{\sigma_{wx}(v)}{\sigma_{wx}} \tag{2}$$

$$C_B(e) = \sum_{w \neq x \in V(G)} \frac{\sigma_{wx}(e)}{\sigma_{wx}} \tag{3}$$

In these equations, $\sigma_{wx}(v)$ 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 $\sigma_{wx}(v) \leq \sigma_{wx}$). Also, $\sigma_{wx}(e)$ 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 an edge are not the same metrics. Also, it is clear that a robust network will have an overall high level of vertex or edge centrality, as this indicates that there are more backup nodes or links available to use in the event of a network failure.

Attack Models

Targeted Attacks

Attacks on large scale networks are not usually ad-hoc; they are based on a logical and structured strategy for decreasing the connectivity of the network by removing select nodes or links from the network in as few steps as possible. Clearly, deleting all nodes from a network would yield the maximum decrease in connectivity. However, such attacks are not practical, so these strategies must be considered at a smaller scale.

Most practical attacks are 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 physically interrupting individual network links or bringing a node or server with a high measure of centrality offline. Such attacks would decrease the number of edges in the network graph and increase the average geodesic path length, respectively, which both result in decreased performance by some factor.

From the definitions presented earlier, 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 $2|E(G)| = \sum_{v \in V(G)} deg(v)$). In addition, 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 or edges, as well as randomized attacks that have no specific targets.

In general, most targeted attacks fall under one of the following four categories: (1) *ID removal*, or initial degree distribution vertex or edge removal, (2) *IB removal*, or initial betweenness distribution vertex or edge removal, (3) *RD removal*, or recalculated degree distribution vertex or edge removal, and (4) *RB removal*, recalculated betweenness distribution vertex or edge removal. An example of initial and recalculated edge-centric attacks on a fixed graph topology is shown in Figure 1 (Holme et al., 2002).

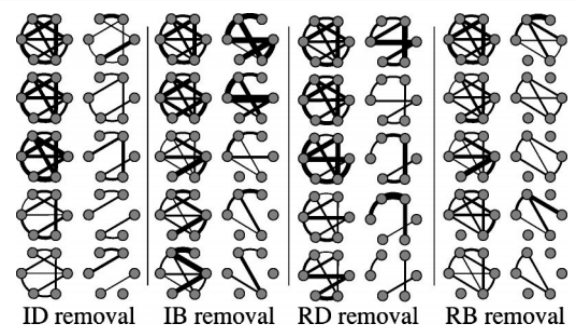

Figure 1. Various edge-centric attacks for a fixed graph topology.

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 the new degree distribution and centralities 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.

Furthermore, it should be noted that both the ID and RD attacks are computationally less taxing than IB and RB attacks (Holme et al., 2002). 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 $O(NM)$. The implication of this is that the adversary must make trade-offs based on their knowledge of the network infrastructure when determining which attack to conduct.

Random Failures

While targeted attacks model common scenarios in the real-world, it is often useful to disregard the source 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 known and is not important. Furthermore, failures are typically seen as independent events (Albert, Jeong, & Barabási, 2000).

Such models are useful when analyzing complex networks such as the Internet and other related military communication networks. This is primarily because it is difficult to formulate precise relationships between the network structure and its robustness under arbitrary failures when analyzing specific network topologies modified by select attacks. Generalizing the concept of network failure into probabilistic events and assuming as little information as possible about the structure of a network enables researchers to study the problem of network robustness at a very high-level, which usually yields results that can apply to most networks.

Network Robustness

Static Robustness Measurements

Two common ways to calculate the robustness of a network are to consider the topological changes that are induced from the removal of nodes or links. Examining the robustness of a network from the perspective of individual nodes is more frequently done in the literature since they are usually the primary victims of network attacks and failures. Using this idea, Herrmann et al. defined a concise equation for calculating the robustness based on the largest connected component $S(q)$ after q hub nodes are removed from the network. Mathematically, this can be defined as follows (Herrmann, Schneider, Moreira, Jr, & Havlin, 2011):

$$R_N = \frac{1}{N} \sum_{q=1/N}^{1} S(q) \tag{4}$$

This equation has been 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 special types of RD vertex attacks.

From the perspective of the communication links that exist in a network, the most successful attacks are those that 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 (Zeng & Liu, 2012). One common measurement of the robustness of a network with respect to these metrics and the largest component of a network $S(p)$ after the removal of p links is shown below:

$$R_M = \frac{1}{M} \sum_{p=1/M}^{1} S(p) \tag{5}$$

This equation is mathematically similar to the previous node-based calculation, but instead of considering the density of the nodes in the entire component S, 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 offline, it is natural to extend the concept of network robustness to consider both node and link failures simultaneously. However, 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 desired 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 t that have been completed at a given instance in time. Mathematically, this hybrid measurement R can be computed as follows (Zeng & Liu, 2012):

$$R_S = \frac{1}{M} \sum_{t=1}^{M} S(t) \tag{6}$$

Dynamic Robustness Measurement

It is also possible to measure the robustness of a network by simulating artificial node or link failures and analyzing the effect on the underlying connection graph. One recently proposed method that follows this approach is called the Dynamic Network Robustness ($DYNER$) method (Singer, 2006). The novel idea behind the $DYNER$ method is that it measures the robustness of a network in terms of the amount of available backup nodes or links that can replace nodes or links that fail sporadically. Naturally, the measurement of the robustness is also heavily based on the centrality of individual nodes and links, because nodes and links with a higher measure of centrality are more likely to have candidate backups in the event of failure.

Mathematically, the $DYNER$ measure $\Gamma(G)$ for a graph G is defined as follows:

$$\Gamma(G) = \left[\sum_{v \in V} \sum_{u \in V_v} \frac{1}{\sum_{w \in V_v} \delta(u,w)} - \frac{1}{\sum_{w \in V_v} \delta(u,w)} \right]^{-1}, \tag{7}$$

where V_v is the set $V(G) - \{v\}$. It is clear that high values for Γ indicate a high measure of robustness. This is because the summation $\sum_{w \in V_v} \delta(u,w)$ will remain relatively constant for networks with many backup nodes and links. However, should the number of backup

nodes or links decrease, we know that this summation will increase, meaning that the inverse of this term will decrease and thus lead to a decrease in $\Gamma(G)$.

The algorithmic procedure used to calculate $\Gamma(G)$ is presented in (Singer, 2006). In essence, however, it iterates over all vertices $v \in V(G)$ and then all vertices $u, w \in V(G) - \{v\}$, and uses a breadth-first search procedure to compute the shortest path $\delta(u, w)$ used in the equation. The resulting Γ value is then compounded during each iteration until all vertices have been traversed.

It is important to note that since this measurement requires global network knowledge it is mostly useful in the offline study of network robustness. In real-world environments it is not always possible to determine this global network information in real-time, which means that it has limited use as a robustness measurement technique in the field.

Random Graphs Utilized in Topological Analysis

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 the Cartesian product $V(G) \times V(G)$ that determines its presence in the graph. 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 each edge probability p is independent from the rest (Van Mieghem, 2005). When studied in the context of computer simulations, 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 exhibit Poisson degree distributions due to the random construction nature of the graph (Sonawane, Abhijeet R., Bhattacharyay, A., Santhanam, M.S., & Ambika, G., 2012).

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 commonly used as the basis for random graph analysis (Tanizawa, Paul, Cohen, Havlin, & Stanley, 2004).

Graphs with Bimodal Degree Distribution

In statistics, a bimodal distribution is one that has two different modes or central moments, as shown in Figure 2. 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 (Sonawane, Abhijeet R. et al., 2012). Firstly, the local mean degree (k_{loc}) of a vertex v is greater than the average degree. Such vertices are often referred to as "super-peers". Secondly, the local mean degree (k_{loc}) of a vertex v is less than or equal to the average degree. 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 increases from 2 to ∞, the degree distribution among all vertices in the graphs, along with 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.

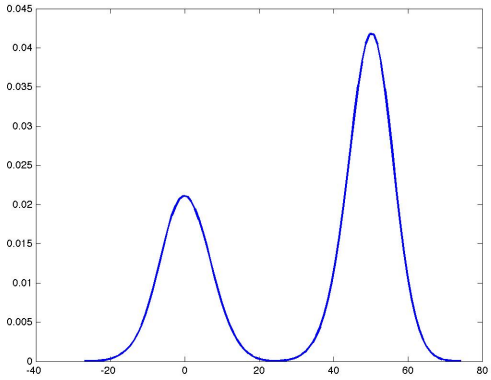

Figure 2. A sample bimodal distribution with two distinct modes.

Network Robustness Optimization Methods

The standard robustness optimization method used in literature has been the application of large-scale stochastic simulations (usually in the form of Monte Carlo simulations) that perform robustness calculations for random graphs after individual links or nodes are removed from the network. As such, the problem of finding network topologies that yield optimal values for robustness are translated into optimization problems that attempt to maximize the number of nodes or links that must be removed from the network in order for it to become globally disconnected. In this section, we discuss a sample of such efforts and the results that were found.

Fractional Node Deletion Investigations

Paul et al. studied the robustness of random graphs in the context of random node deletions (Paul, Sreenivasan, Havlin, & Stanley, 2006). Their work was driven by 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 in terms of the number of hub nodes q that must be removed. In order to find the optimal value for q, a Monte Carlo search was performed over a large set of Erdös-Rènyi and scale-free random graphs that were structured according to a special degree distribution that assumes each network consisted of q hub nodes and $N - q$ leaf nodes. The search algorithm utilized during these simulations is shown in Algorithm 1.

Algorithm 1 Monte Carlo q Search

1. Let $n_r = 0$.
2. Initialize a graph G with N vertices.
3. Randomly delete a node in the network and calculate $\kappa(G)$.
4. Increment n_r by 1 node.
5. If $\kappa < 2$, G has become disconnected, so, terminate and return n_r. Otherwise, decrement n_r by 1 and go to step 3.

The resulting fraction of nodes that needed to be deleted was $f_c = \langle n_r \rangle / N$, which is referred to as the fractional threshold. This threshold was then compared against q to determine the robustness of graphs in terms of the number of hub nodes. This is natural because the hub nodes provide more backup routines for traffic in the event of random failures in the network. It was determined that the optimal value of q that maximizes the network robustness is as follows:

$$q = \left[(\langle k \rangle - 1) / \sqrt{\langle k \rangle} \right] \sqrt{N}, \tag{8}$$

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

Paul et al. also examined the the relationship between q, f_c, and N, as shown in Figure 3. In essence, they were able to conclude that the number of *hub* nodes needed to achieve optimal robustness increased logarithmically with the increase in N. This result implies a network construction heuristic that assumes the number of hubs should be logarithmically proportional to the size of a network.

Fixed-Degree Distribution Investigations

Independent to the work done by Paul and his team, Herrmann et al. 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 procedure is outlined in Algorithm 2.

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 2 is repeated for a very large number of iterations until an ideal level of robustness has been obtained, albeit at the sake of sometimes massive computations (as is the case with Monte Carlo methods). An interesting result from their optimization efforts was that every network structure seemed to converge towards an onion-like topology, meaning that there are distinct layers of nodes that are connected, and that each layer i has more connectivity than its parent layer $i + 1$ (Herrmann et al., 2011). 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, which is an indication that the degree distribution closely resembles a bimodal distribution. An example of such a graph with 124 nodes and 366 edges is shown in Figure 4.

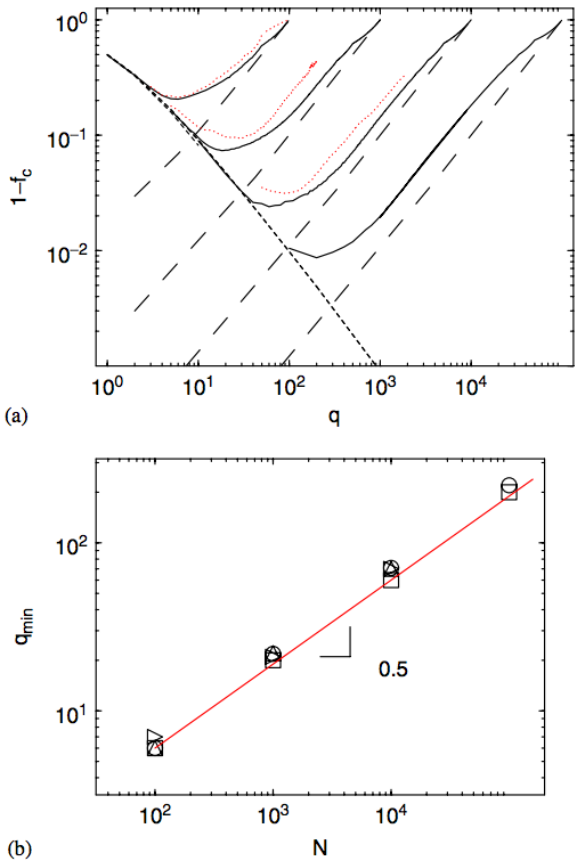

Figure 3. Figure *a* shows that as the number of hub nodes increases in a network of N nodes, the fraction of nodes that needs to be deleted increases (since the value $1 - f_c$ decreases). Figure *b* shows that the number of hubs q increases logarithmically with the number of nodes in a network of N nodes.

Evolutionary Network Construction

As shown in the previous section, networks with bimodal degree distributions tend to have high measures of robustness against targeted attacks and random failures. While it is possible to perform optimization on an existing graph of N vertices to obtain such graph topologies (as was done in the work by Herrmann et al.), such initial network knowledge is not always known or cannot be assumed. Therefore, various methods to construct networks with bimodal degree distributions have been proposed to address this issue.

One recent evolutionary method developed by Sonawane et al. iteratively constructs a network with a bimodal degree distribution by adding nodes and links to the network with probability p and then removing arbitrary links with probability $(1 - p)$ at each iteration (Sonawane, Abhijeet R. et al., 2012). Their approach has been empirically verified to generate graphs with bimodal degree distributions with Monte Carlo simulations that run up to $10,000$ iterations (i.e. generate networks with $10,000$ nodes). A high-level pseudocode description of the evolution procedure is shown in Algorithm 3.

In order to further test the correctness of this method the authors varied the con-

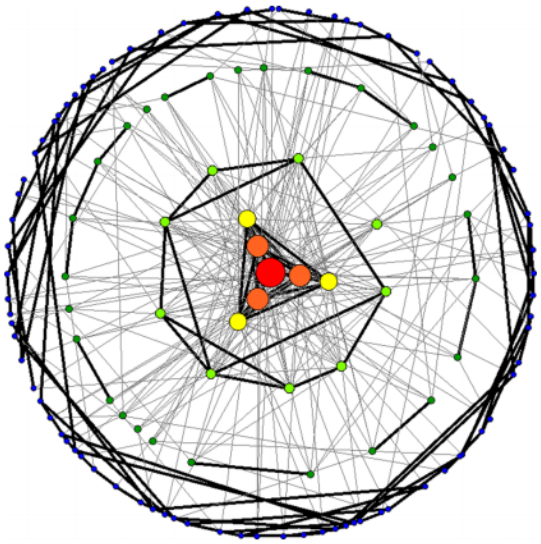

Figure 4. An example of a graph with 124 nodes and 366 edges that exhibits the onion-like topology.

Algorithm 3 Bimodal Network Evolutionary Generation

1. Let $G = (\emptyset, \emptyset)$.
2. Create a new vertex v_1 and add it to G
3. Iteratively create new vertices v_i and add them to G with probability p and link them to other vertices $v_j \in V(G)$ with probability $1 - p$. Repeat until the desired iteration count has been reached.

struction probability p used in the algorithm. Their simulation results indicated that the resulting degree distribution was minimally affected by the variation in p. Lower order networks showed the most impact by varying p, as indicated in Figure 5. In order to revive the bimodal degree distribution it is necessary to evolve the network using the same algorithm to a larger number of vertices, because the size of the network corresponds to its correlation with the bimodal degree distribution when constructed in this manner (Sonawane, Abhijeet R. et al., 2012).

Conclusion

Network robustness is a very important issue that must be considered when designing and constructing mission-critical networks of every scale that are susceptible to targeted attacks or random failures. The robustness of every network is highly influenced by its underlying topology. Furthermore, those with the most optimal measures of robustness tend to resemble the onion-like structure or are characterized by having scale-free or bimodal degree distributions.

Since it is difficult to arbitrarily construct networks with specific degree distributions, it is sometimes necessary to utilize construction methods similar to the one developed by Sonawane et al. These results yield topological templates that can be followed by network

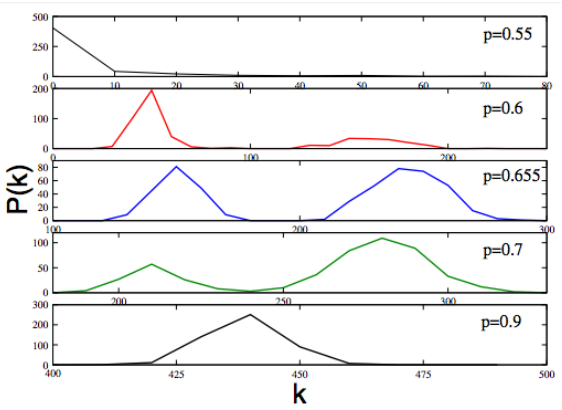

Figure 5. The degree distribution $P(k)$ for a network of 500 vertices with average degree k by varying p over the set of values $\{0.55, 0.6, 0.655, 0.7, 0.9\}$. Notice that the inner three values for p resulted in the most bimodal distribution, while the remaining values tended towards other distributions.

engineers when constructing networks with optimal robustness.

Current research trends will surely continue to reveal more information about the relationship between the network topology and its measure of robustness. However, it is up to the engineers to utilize this information in order to make emerging networks resistant to any kind of failure that could impact the functionality and usefulness of the network.

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`

Paul, G., Sreenivasan, S., Havlin, S., & Stanley, H. E. (2006). Optimization of network robustness to random breakdowns. *Physica A: Statistical Mechanics and its Applications*, *370*(2), 854 - 862. Available from `http://www.sciencedirect.com/science/article/pii/S0378437106002457`

Singer, Y. (2006). Dynamic measure of network robustness. In *Electrical and electronics engineers in israel, 2006 ieee 24th convention of* (pp. 366–370).

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*.