Proceedings of the 2013 Winter Simulation Conference
R. Pasupathy, S.-H. Kim, A. Tolk, R. Hill, and M. E. Kuhl, eds.

ON SIMULATING THE RESILIENCE OF MILITARY HUB AND SPOKE NETWORKS

Robert Bryce
Raman Pall
Ahmed Ghanmi

Centre for Operational Research and Analysis
Defence R&D Canada
Department of National Defence
Ottawa ON K1A 0K2, CANADA

ABSTRACT

Hub and spoke networks, while highly efficient, are fragile to targeted attacks: removal of the central hub destroys connectivity of the network. This fragility has led to the assertion that these networks are not suited to military distribution systems. However, military supply chains have redundancy induced by heterogeneous transportation modes (*e.g.*, road, marine, and air) leading to enriched connectivity over a pure hub and spoke structure. In this paper a global military (hierarchical) hub and spoke network model is developed; the topological resilience of such networks are probed by stochastically sampling an ensemble of networks and simulating both random and targeted edge knockout, and the network properties relevant to resilience measured. It is found that such networks are resilient to continual attack and loss (network erosion), performing well relative to preferential (scale free) and random network benchmarks. This regime of network erosion is descriptive of modern asymmetric warfare.

1 INTRODUCTION

1.1 Resilience of Networks

Delivery systems often make use of hub and spoke structures as they deliver high service quality at low cost – witness the success of FedEx and UPS (Rodrique and Slack 2002). The idealized hub and spoke network resembles a wagon wheel and consists of a central hub servicing nodes on the peripherally of the network. While such networks are highly efficient, they are thought to be very fragile to targeted attacks: removal of the central hub, a single site, completely destroys connectivity and breaks the network into isolated nodes. However, it must be noted that while the idealized single hub and spoke model captures their basic structure, there is natural redundancy in military supply chains induced by their heterogeneous transportation modes (road, marine, and air). In this paper, the topological *resilience* – robustness to node or edge deletion – of military hub and spoke networks subject to connectivity loss under continual attack is probed, where added linkages between nodes are taken into account. Networks are stochastically sampled from an ensemble and subjected to Monte Carlo randomized and targeted edge knockout and key measures are taken.

Cities are hubs in urban systems, with a high density of people, infrastructure, and concentration of otherwise economically valuable assets – and are natural targets for violence, yet in practice cities are not fragile and "regrow" after being destroyed (Allenby and Fink 2005), for example after nuclear attack (Hiroshima) or fire (San Francisco 1906). Dynamic regrowth of disrupted nodes are therefore of interest in full understanding of resilience; however, such dynamics are currently not well understood. Furthermore,

in the short term regrowth cannot occur and it is therefore both easier and useful to consider the resilience of networks to deletion of basic elements (nodes and/or edges).

In considering attack on networks several scenarios are possible: single contest (strike) with a single evaluation leading to targeting a fraction of the network to be removed, staged contest (repeated attack) where network targets are selected in each round until a targeted fraction of the network is removed, and contagion approaches (in which nodes are "infected", changing their state, and this change can spread through the network). The seminal work on network resilience (Albert, Jeong, and Barabasi 2000) considered single contest, finding that scale free, specifically preferential growth, networks are fragile to attack on nodes. The majority of later works in the complex networks literature have also considered single stage removal of nodes. The essential finding is that networks with a few nodes distinguished with many links (hub and spoke, scale free, and the like) are not resilient to targeted removal of those nodes, which has led to the belief that such networks are unsuitable when targeted attack is a possibility.

1.2 Are Hub and Spoke Networks Truly Fragile?

Knocking out a hub will collapse a hub and spoke network. As hubs are desirable targets for disruption this will naturally lead to asymmetric (enhanced) security emphasis which counteracts the targeting. If an adversary can bear the resulting high cost of hub elimination it then seems likely they can equivalently afford to remove all periphery nodes to achieve the same result of total network collapse – the fragility of hub and spoke networks must therefore be carefully interpreted. Can this finite resource (attack/defense budget) consideration be taken further?

Recent work in the economics literature has found that for the case of limited defense (and attack) capability and contagion (where nodes are captured rather than simply removed, with their resources reassigned to the attacker), hub and spoke networks are *optimal* in defending against an intelligent adversary (Goyal and Vigier 2009, Goyal and Vigier 2013). Such scenarios are important, for example, in designing telecommunications networks with good cyber security. While the model is stylized – assuming a given network value metric, security budgets, and redeployment strategy – the assumptions are reasonable and provide additional insight into the simple observation that more important nodes will be allocated increased security budgets. It should also be noted that demoralization can be seen as a contagion effect, which suggests even supply chain/military infrastructure networks in classic contest scenarios may be affected by contagion.

Furthermore, nodes are embedded in real-world environments with differing security, infrastructure, and other attributes. For example, the United Kingdom Border Agency Overseas Network has selected a hub and spoke model for three reasons – two of which are widely recognized attributes of hub and spoke networks: quality/consistency, and high efficiency/productivity. The third reason is greater resilience and flexibility:

> Moving work from expensive and less secure environments to more stable regional hubs has reduced the risks to our staff, and has created a visa network that is more flexible and responsive in the event of natural disasters, political instability and fluctuations in demand (UK Border Agency 2012).

In this paper the case of repeated attack is studied on a hub and spoke-like model, which are descriptive of global military distribution systems, in order to probe the resilience of these networks under continual erosion and loss of functionality. The goal is to provide insight into the case where no catastrophic strike is made; rather continual smaller scale strikes occur which typify modern insurgency and asymmetric warfare situations (Bohorquez et al. 2009). Military supply chain networks have often suffered from such link removal. Two notable examples are the attacks on the USS Cole in 2000, which led to the temporary closure of the port of Aden in Yemen (Lumpkin 2006, Wright 2006); and the closure of the road network from Kandahar, Afghanistan to Karachi, Pakistan due to political disputes (Whitlock 2011, Bryce 2007). The first example led to the temporary closure of the port of Aden (and thus sealift); however both air

and road transport were still possible. Contrastingly, the second example resulted in the ongoing closure of the road network from Kandahar to Pakistan for military transport, but airlift from Kandahar remained possible. It is hard to determine if such attacks are targeted, or are random in nature.

2 NETWORK MODELING

2.1 Basic Network Metrics and Network Attack

Networks are made up of nodes and edges connecting them, and are parameterized by two numbers: the total number of nodes (n) and the mean degree ($\langle k \rangle$) of a node (*i.e.*, the average number of edges of a node). For undirected networks the mean degree is equal to $2m/n$, where m is the number of edges. Hub and spoke networks are a special case of tree networks, which have one less edge than the number of nodes – asymptotically, as n increases, hub and spoke networks thus have $\langle k \rangle \to 2$, and the smallest $\langle k \rangle$ possible for a tree is one (in a two node, single edge, "dimer" network).

An innovation here is that *redundant* edges are considered in hub and spoke networks (see Section 2.2 below), allowing direct comparison with other network types. Prior work in the literature has not considered redundant edges when considering resilience of tree networks. As few empirical networks will happen to have $\langle k \rangle \approx 2$, tree networks, without redundant edges, are not comparable to most networks of interest. The redundant edges considered in this paper mirror how military distribution systems are structured, due to heterogeneous transport modes, which impart added resilience to hierarchical hub and spoke networks. The result is improved resilience relative to pure (single edge) tree structures, and by allowing redundant edges, tree structures can be directly compared to empirical networks of arbitrary $\langle k \rangle$.

In considering resilience, networks are "trimmed" either via node or edge knockout. In general edge removal can emulate all node knockout scenarios, and allows improved resolution. In this paper, single edge removal per attack round is considered. Random edge elimination is performed by Monte Carlo: selecting one of the existing edges, removing it, and iterating until the desired fraction is eliminated. For targeted attack the following scheme is used. Nodes are ranked by importance, with number of edges signifying their importance. Edges are targeted by randomly removing one of the highest value edges, and the process (valuing, targeting) is iterated until the desired number of edges are removed. This attack regime emulates the continual attack and small scale loss on a network, and probes the ability of a network to perform under erosion.

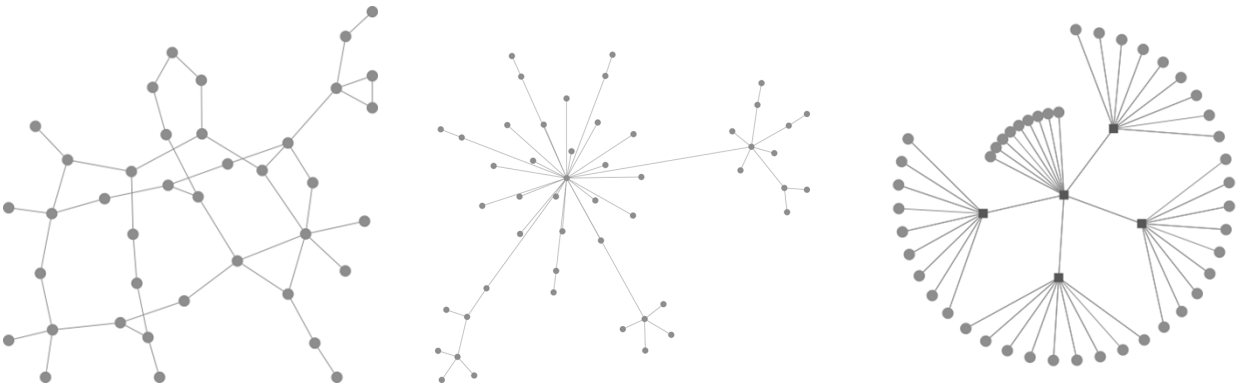
Several metrics allow robustness of networks to be considered, and Thadakamalla et al. (2004) is taken as an inspiration. *Survivability* is defined as the fraction of a network's nodes remaining in its largest component after attack, scaled by the original number of nodes. *Responsiveness* is captured by the average shortest path between nodes, as well as the diameter (the longest such possible path); both are measured in the largest surviving component. In addition Thadakamalla et al. (2004) state *adaptivity*, the ability to replace eliminated nodes or edges, and to do so efficiently, is important (but do not measure it; in general dynamics are difficult to quantify and model); as is *flexibility*, which is defined as the number of alternative paths (measured by the clustering coefficient). Note that trees have a clustering coefficient of zero, which makes them inflexible according to Thadakamalla et al. (2004). In Thadakamalla et al. (2004) clustering coefficients are given for full networks for several considered graph types, however the effects of network attack on the clustering coefficient were not considered. Arguably flexibility is also best described by dynamics, and, for example, if an edge is removed from the current list of *de facto* edges a search for a new route would occur. Thus thresholding is an important consideration: for example, if a supply road is destroyed a previously inferior road may be available and "thresholded" and brought into the network; issues such as this are crucial in interpreting neuroimaging applications and are discussed in van Wijk et al. (2010). In Thadakamalla et al. (2004) three properties are considered in detail: survivability (termed robustness therein), average shortest path, and diameter; these are well defined and interpretable, and therefore also considered in detail in the present paper. It is worth noting that short path distances

correspond to both quicker delivery due to shorter distances, but also incur fewer logistical losses arising from frequent handovers, which can cause both delays and result in misplaced items.

2.2 Military Hub and Spoke Networks: Stochastic Model

Operational Support Hubs (OSH) (Bacot 2009; Girard et al. 2008) are a network scheme used in the Canadian Forces, where global operations are regionally supported with local hubs. In this matter the global theatre is decomposed into regions allowing global reach and improved service by decreasing distances (physical, but also reducing social and climate distances). In general, regional hubs can be linked together in an arbitrary manner. As military distribution systems are often based on hub and spoke structures the concept is modeled in this paper using hierarchical hub and spoke (hH&S) networks, where each region is a hub and spoke, and the regions are connected in a "super" hub and spoke structure as illustrated in Figure 1. The global (root) hub corresponds to the national (Canadian) hub and each local regional hub is an OSH; *i.e.*, a tree which is maximally two levels deep.

In this paper, the number of global regions is set to five, corresponding to a reasonable decomposition of the "non-integrating gap" of unstable states and a home hub (Girard et al. 2008; Barnett 2004). The non-integrating gap is a contiguous region of unstable states and includes the Middle East, most of Africa and South Asia, Southeast Asia, and the Caribbean, Central America, and northwest South America. Given the cultural, geographic, and climate distances involved, and taking a national base as a given, requires roughly five regions, with political, infrastructural, diplomatic, cost, and other considerations being factors involved in setting the number and locations of OSH in the global network (Girard et al. 2008).



(a) Random network (b) Preferential growth network (c) Hierarchical hub and spoke

Figure 1: Network topologies. Three network models are represented: (a) a random network, (b) a preferential growth network, and (c) a two-level hierarchical hub and spoke model. For illustrative purposes, 50 nodes and a mean degree of approximately 2 are set for each example.

The hH&S networks to be considered are stochastically sampled from an ensemble described by a random number of hubs (Poisson distributed) each with a random number (again, Poisson distributed) of attached nodes – each local region is a replica of the network, *i.e.*, the mean number of regions and mean number of periphery nodes in those regions describe the network model. Setting regions as replicas constrains the model, thus simplifying the analysis, and corresponds to networks with balanced regions. It should be noted that the Poisson distribution can return zero elements; a floor of one is dictated to address this. Redundancy in edges is modeled as air and sea linkages between global hubs, and road and air linkages within a local network. Global hubs are always redundant, and local redundancy is tuned to match a desired mean degree (see Appendix A).

The expected number of nodes in a network realization n is fixed at 1000 nodes and the mean degree $\langle k \rangle$ is set to 3.63, in order to allow comparison with a real world complex network topology designed

to be robust: the Defense Advanced Research Projects Agency's (DARPA) *UltraLog* project (Zhao et al. 2011; Thadakamalla et al. 2004; Bates 2005). The mean number of global regions is set to five, as stated previously.

2.3 Benchmark Models: Random and Preferential Networks

Benchmark comparisons are taken against random networks (specifically Poisson Erdos-Renyi random graphs (Erdos and Renyi 1960; Callaway et al. 2001)), and a preferential attachment model. The preferential attachment model (Barabasi and Albert 1999; Albert, Jeong, and Barabasi 2000) considered here is a tree with redundant edges added in order to tune the mean degree to a desired value (see Appendix A).

Random graphs are grown by randomly adding edges between nodes and undergo a phase transition from small clusters of isolated components to the existence of a "giant component" (GC) spanning a large fraction of the network, as edges are added (Erdos and Renyi 1960); this transition occurs at a mean degree of one.

Preferential attachment models start with a few nodes, and the network grows by adding new nodes with a set number of edges which are linked preferentially to high degree nodes; the resulting distribution of edges/node is power law/scale free, and makes up a canonical model of "complex networks" (Albert, Jeong, and Barabasi 2000), describing, for example, the internet. In the present paper a tree structure is imposed by setting the number of edges per added node to be one, with possible "double edges" (redundancy) probabilistically added such that $\langle k \rangle$ is set to the desired value (Appendix A). This choice is made to create a network that is in some sense "close to" an hH&S network as described above.

Simulations were done in *NetLogo 5.02*, an interpreted language implemented in Scala on the Java Virtual Machine (Wilensky 1999). Networks were stochastically created from their models and disruptions simulated with random and targeted edge removal. Fractions to be deleted were done from 0.05 to 0.95, in steps of 0.05. For each network type and fraction deleted 10 repetitions were performed (*i.e.*, 1140 graphs are considered). Typically mean values are reported in the literature, here error bars (standard deviation) and worst case are also reported for a subset of the data in order to illustrate inherent variability (see Section 3.2.1 for further discussion). Worst case was defined by lowest fraction remaining, and longest average shortest path/diameter, of the 10 repetitions.

Regarding time complexity of the algorithms, finding the largest component with a depth first search algorithm is $O(n+m)$, while finding the average shortest path is $O(n^3)$ (Floyd 1962). Finding the diameter can also be performed in $O(n^3)$ (Floyd 1962), as the diameter is simply the longest of all such shortest paths. However a more naïve algorithm was used that considered the shortest path (Dijkstra's algorithm; $O(m+n\log n)$ (Fredman and Tarjan 1987)) between all pairs of nodes ($O(n^2)$), which increased costs to $O(n^2(m+n\log n))$ – *i.e.*, an extra factor of $\log n$ is picked up. This moderate, yet notable, worse asymptotic time complexity was a result of having access to a function in *NetLogo* that supplied the average shortest path but *not* the diameter (which can be found as a byproduct) as well as having access to a function that calculates the shortest path between a given pair of points (Dijkstra's algorithm); there is a tradeoff involved between code clarity and performance.

3 APPLICATION AND RESULTS

3.1 Targeted Attack

As targeted attack in an network erosion regime is of most interest, being both a novel contribution and of special interest for military distribution systems, it is considered first and with most detail in the figure. Random attack is considered next, while those results are also given in this paper for the first time (node deletion is considered in the prior art, edge deletion here), they are most comparable to existing literature.

3.1.1 Random Networks

Of the considered networks the random network displays the lowest variability in survivability (left most panel in Figure 2). The most distinguishing feature is a dramatic transition as half of the edges are removed, with quite slow (mildly dropping, concave down) erosion until near the transition. At the transition variability in survivability increases dramatically, as expected for finite systems undergoing phase transitions. At and after the transition survivability is poor – random networks erode well, until a sudden collapse in the network. Regarding path distances, performance degrades (distances increase) up to the transition, where a sharp peak occurs (indicating divergence for large networks). After the transition path distances rapidly improve, which can be attributed to the small remaining network (*e.g.*, a low fraction surviving results in a relatively tiny network which can be rapidly transversed).

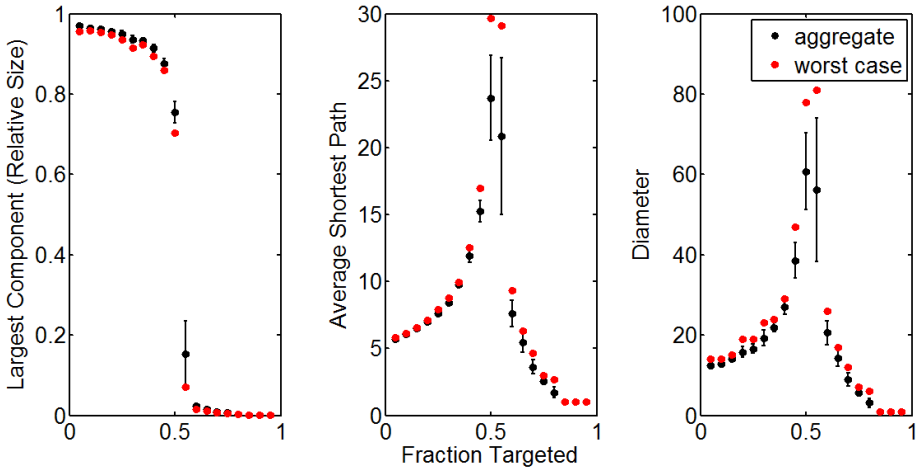


Figure 2: Random network. A transition can clearly be observed near a value of 0.5, with survivability (largest component remaining after attack) transitioning from concave down to concave up as the network rapidly drops in survivability. The path lengths diverge at the transition, and display better quality at the extremes of remaining network size.

3.1.2 Preferential Networks

The scale free preferential network demonstrated rapid, exponential-like, decay in survivability when subject to repeated targeted attack on the edges (see Figure 3, left panel); the network has poor survivability, with rapid initial (low fraction targeted) drop off. It is notable that there is high variability, and the worst case survivability is quite poor (*e.g.*, approximately 50% of the network eliminated with 5% of the edges removed). The path lengths monotonically drop, in a linear-like manner (Figure 3, middle and right panel). This indicates that the network smoothly erodes in size.

3.1.3 Hierarchical Hub and Spoke Networks

The hH&S network fared fairly well under targeted attack. The survivability drops in a linear-like manner, with some modulation evident (see Figure 4, left panel). This modulation is most evident in the worst case data and can be attributed to the hierarchical structure. The path lengths (average, middle panel, and diameter, right panel; Figure 4) show modest absolute (albeit sizable relative) variation; as expected for shallow tree structures the diameter is close to the average shortest path. The diameter looks piecewise constant, with sizable relative fluctuations (however, note the worst case which clearly demonstrates discrete

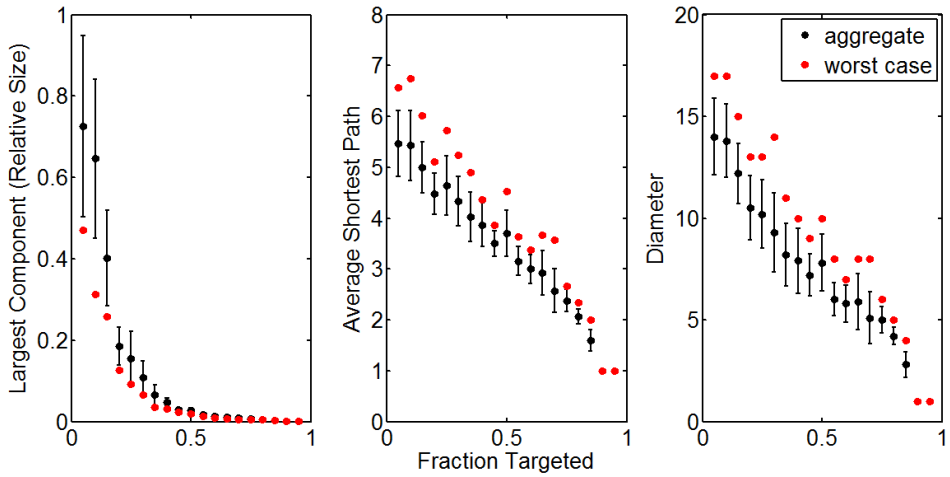


Figure 3: Preferential network. Survivability shows a rapid exponential-like decay in the network size. Path length (average, diameter) on the remaining network is quasi-linear, with smooth improvement in service quality (due to reduced network size).

steps), this again can be attributed to the hierarchical tree structure. As the network continually erodes, the number of levels, which sets the diameter, will show discrete jumps as they are eliminated.

3.1.4 Targeted Attack: Mean Comparison of Networks

In Figure 5 the mean values for each metric and each model are plotted together, allowing ready comparison. Overall, it can be seen that hH&S networks perform the best regarding path lengths – approximately half the distance relative to either random or preferential networks – under moderate loss. Short paths are a key strength of tree structures, and it is clear that this advantage remains even with loss occurred by continual attack. Note that this cannot be attributed to poor survivability leading to small networks – hH&S networks perform better than preferential networks, which display the worse survivability over all fractions targeted and removed. Indeed, hH&S networks display good survivability under iterated targeted attack on edges (leftmost panel, Figure 5). For moderate (up to 15%) loss hH&S networks perform quite comparably to random networks for survivability, suffering little loss. As the fraction of edges increases hH&S networks monotonically decrease in size; moderations and discrete jumps/sudden partial collapses are not evident when averaged over sampled networks and simulated loss (however, see Figure 4 where such modulation is more apparent in the worse-case data).

It is interesting that random graphs display quite good survivability, the best of the three networks considered when up to 50% of the edges were removed. The cost of this survivability is long paths, and a sudden collapse at the transition. This excellent survivability is likely due to the existence of the GC, which is densely connected and thus will be robust against loss of edges.

3.2 Random Attack

Random removal of edges is now considered. This regime of attack is not currently addressed in detail in the literature, and in particular has not been studied for the graphs considered in this paper. Random attack of nodes however is well explored.

It is found that the peaking in path lengths for the random network is shifted to a larger fraction removed, and with more gradual transition in survivability, relative to targeted attack (compare Figure 5, above, with Figure 6, below). Of note is that survivability of all network types become more similar to each other, in particular the preferential model shows dramatic improvement.

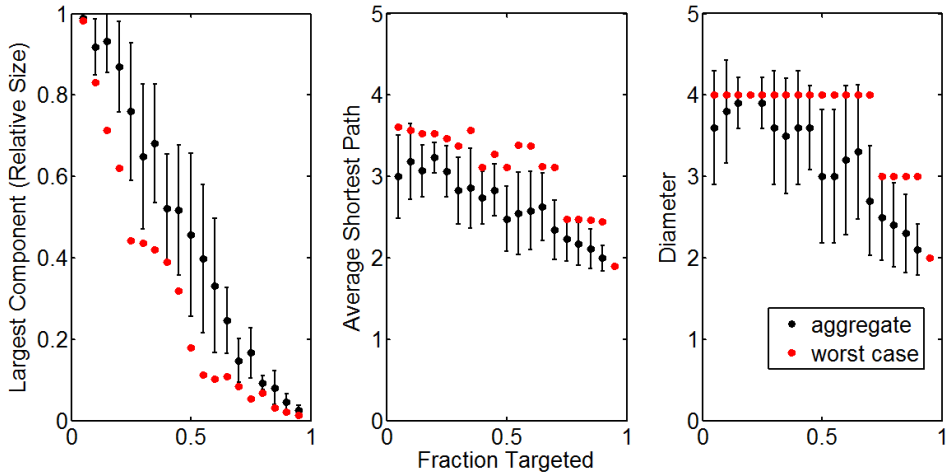


Figure 4: Hierarchical hub and spoke network. The network shows good survivability, with approximate linear loss of network size. Modulation in decay can be observed (best seen looking at the worst case data), which can be attributed to the hierarchical topology. The average path length slowly improves, in a near linear-like fashion, while the diameter looks piecewise constant (with sizable relative fluctuations; however, note the worst case steps).

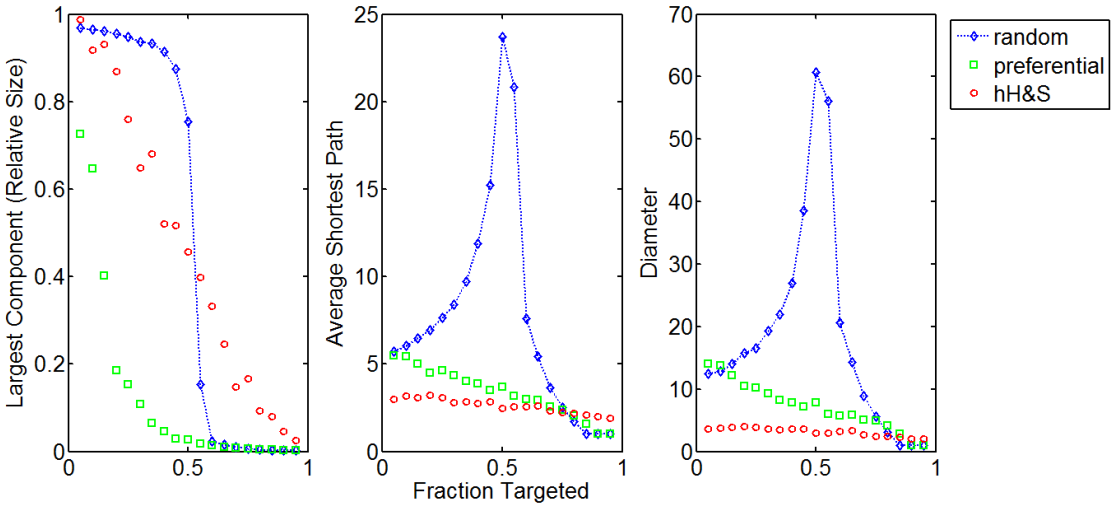


Figure 5: Survivability and resilience of network models to targeted continual attack. It can be seen that the hierarchical hub and spoke (hH&S) model outperforms the preferential model, except near total destruction of the network. The giant component transition of the random graph can clearly be seen at the theoretical transition value of 0.5, at this transition the average shortest path and network diameter diverge. Before the transition the random network displays better survivability, yet worse transport quality; note that close to total destruction the random graph performs best on the remaining network.

While direct comparison of edge and node deletion is not possible, as these are differing regimes of attack, qualitatively behavior should be quite comparable – if the fraction removed is suitably interpreted (most notably, removing a single node can, and typically does, remove many edges, this should result in stretching/compression of the x-axis between node/edge deletion plots). Therefore the *UltraLog* and random network data in Thadakamalla et al. (2004), where node knockout is considered, is included in the present paper. The data is estimated from their Figure 6, and replotted here (Figure 6). They report data in the range of 0.05 to 0.75 of the network eliminated, in steps of 0.05. The preferential model explored in Thadakamalla et al. (2004) is excluded to prevent overly cluttering Figure 6, in general their preferential and *UltraLog* model data are quite similar for their reported measures.

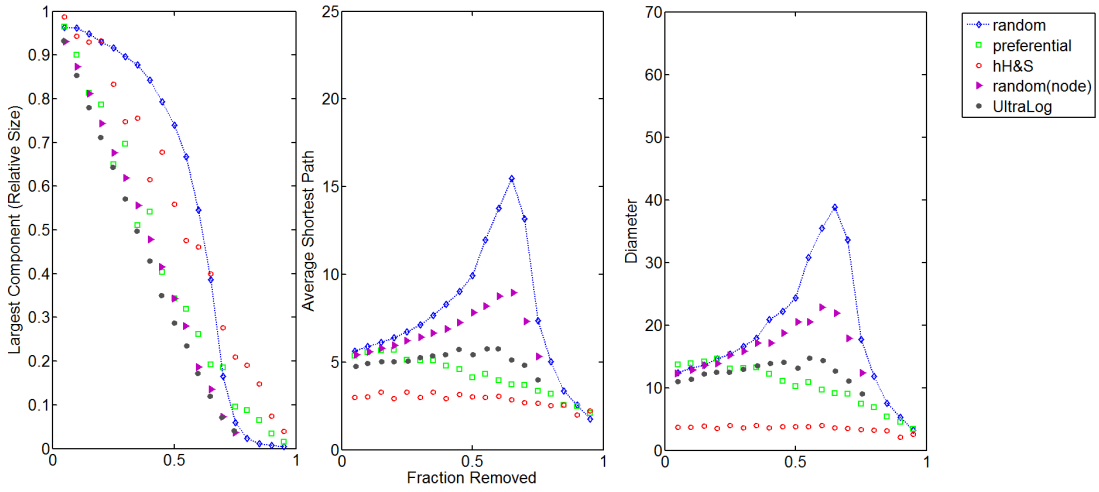


Figure 6: Survivability and resilience of network models to random attack of edges. Relative to targeted attack the survivability of the networks is improved, with decay delayed, and differences between network types are muted (compare with Figure 5). The divergence in path properties for the random graph is delayed, peaking between 0.65 to 0.75, and performance is roughly $^2/_3$ better. The improvement of the preferential model is weaker than in targeted attack, and qualitatively changes from quasi-linear to concave down. The hH&S model is very similar for targeted and random attack. Results from Thadakamalla et al. (2004) investigating random attack on nodes for the random and *UltraLog* complex network topologies are included to allow comparison with established literature.

Comparing the diameter of random edge deletion (in the present paper) and node deletion (Thadakamalla et al. 2004) shows similar behavior for random graphs, and somewhat surprisingly the node knockout and edge removal peaks occur near the same point. The *UltraLog* network data is quite comparable, in an absolute sense, to the preferential model considered here. The near identical behavior found between random and *UltraLog* network survivability, for random node knockout, is puzzling (Thadakamalla et al. 2004); it is surprising that the structure inherent to the *UltraLog* network does not lead to a clear distinction in survivability, relative to a "structureless" (random) network.

It is worth noting that the *UltraLog* complex network topology (Bates 2005) was designed to be robust to targeted attack; in Thadakamalla et al. (2004) it was found that *UltraLog* path performance was better than random networks and mildly worse than a preferential model when subject to random attack (see their Figure 6, as well as Figure 6 here) and worse than either random or preferential networks when subject to moderate (up to 10%) targeted attack (additionally, the *UltraLog* network had worse survivability than comparators under targeted attack, over all considered fraction of nodes removed). This comparable performance to

standard benchmarks under random attack and poorest performance when subject to moderate targeted attack indicates the difficulty in designing network topologies for resilience.

3.2.1 Variations

Regarding variation in results (see error bars and worse case data in Figures 2 to 4, and mild visual scatter in all mean values as seen in Figures 5 and 6) the 10 repetitions per data point give good information relative to the computational cost; especially note that the error in the mean will approximately be described by the standard error (*e.g.*, roughly a third of the size of the standard deviations shown). The number of repetitions is typically unreported in the literature, however qualitatively the scatter seen in Figures 5 and 6 is comparable to reported studies such as in Thadakamalla et al. (2004). As a rough approximation, to improve the estimates of the mean by an order of magnitude, 100 times more simulated data would be required (*e.g.*, 1000 repetitions per data point rather than 10). This is prohibitive in the currently interpreted *NetLogo* environment and consideration of a C/C++ package with best in class algorithms (such as *igraph*) would be recommended (Scardi and Nepusz 2006). While obtaining tighter error bars on the mean will provide diminishing returns, of more value is consideration of the variability in response (as illustrated in Figures 2 to 4 by the standard deviation and worse cases).

4 CONCLUSIONS

This paper provides a means of constructing hH&S networks which allow comparisons with a wide range of other networks: redundant edges are considered, allowing the mean degree to be tuned in addition to setting the number of nodes. The approach is simple, and general. Here specific decisions were made in order to concretely model a global military supply chain, where redundant edges are the norm, and a two-level hub and spoke model consisting of regions locally serviced by regional hubs forming a hub and spoke network is considered. For the first time network erosion is considered, where iterative targeted edge removal is performed, simulating continual small scale loss which is representative of asymmetric and insurgent warfare. It is found that two-level hH&S networks, which model global military supply chains, are resilient to erosion – showing both good survivability and retaining the best responsiveness as measured by path lengths. In regards to future work, focus on regeneration of edges and/or nodes after knockout is difficult to model but potentially of great value: understanding the time dynamics of disruption is important for deep understanding of resilience. One advantage of *NetLogo* in terms of regeneration is that it is built for agent based modeling, a methodology that is specifically targeted to questions regarding dynamics. In this paper a specific model for global supply chains was considered, in order to capture the parameter space and likely variability in network structure required to service the non-integrating gap, and which incidentally should be relevant to many global organizations. Specifically modeling a current or proposed hierarchical structure, or otherwise modifying the considered model, is a fruitful avenue for consideration as the methodology proposed here generalizes for *arbitrary* tree structures, allowing a wide range of networks to be considered.

ACKNOWLEDGMENTS

Robert Bryce acknowledges the support of NSERC and DRDC through an NSERC Visiting Fellowship.

A REDUNDANCY TO MATCH $\langle \mathbf{k} \rangle$

A key innovation in this paper is adding redundancy via double edges, allowing the mean degree of a tree to be increased beyond its (single edge) constraint of $\langle k \rangle \in [1,2)$. Details required for implementation are given in this appendix. Note that in this work double edges are considered, in general multi-edges (2, 3, 4, ...) can be considered if multiple transport modality or routes exist.

The mean degree of an undirected network is given by

$$\langle k \rangle = \frac{2m}{n}.$$

For the hH&S model explored here the edges are of three types, the hub-to-hub edges, the hub-spoke edges, and the required redundant edges required to achieve $\langle k \rangle$ matching. Hub-to-hub edges are all redundant in the specific implementation chosen. The resulting equation is

$$\langle k \rangle = \frac{2 \cdot 2(H-1) + 2(H \cdot n_s) + 2\delta}{H + H \cdot n_s},$$

where H is the number of hubs, n_s is the number of spokes in a region, and δ is the number of redundant/double edges. Solving for δ determines how many redundant edges are required to match $\langle k \rangle$, and scaling by $H \cdot n_s$ – the number of candidate edges to make double (hub-to-hub links are already doubled, and are thus excluded from the pool) – dictates the probability, p, a double edge should be formed:

$$p = \frac{\frac{\langle k \rangle H(1+n_s)}{2} + 2 - 2H - H \cdot n_s}{H \cdot n_s}.$$

Similar manipulations lead to the required probability of adding edges in the preferential tree model outlined above in Section 2.3:

$$\langle k \rangle = \frac{2((n-1)+\delta)}{n},$$

where n is the total number of (single) edges forming the "skeleton" of the tree. Solving for δ and scaling by the number of candidate edges gives the probability with which to add an edge:

$$p = \frac{\langle k \rangle n - 2n + 2}{n-2}.$$

Note the scaling by $(n-2)$, which is due to pre-seeding the growth of the network with a dimer (two nodes, one edge).

REFERENCES

Albert, R., H. Jeong, and A. Barabasi. 2000. "Error and Attack Tolerance of Complex Networks". *Nature* 406:378–382.

Allenby, B., and J. Fink. 2005. "Towards Inherently Secure and Resilient Societies". *Science* 309:1034–1036.

Bacot, R. 2009. "Global Movements and Operational Support hub Concept: Global Reach for the Canadian Forces". *The Canadian Air Force Journal* 2:8–17.

Barabasi, A., and R. Albert. 1999. "Emergence of Scaling in Random Networks". *Science* 286:509–512.

Barnett, T. 2004. *The Pentagon's New Map*. New York, New York: G.P. Putnam's Sons.

Bates, J. 2005. "UltraLog: Securing Logistics Information on the Battlefield". *Army Logistician* 37.

Bohorquez, J., S. Gourley, A. Dixon, M. Spagat, and N. F. Johnson. 2009. "Common Ecology Quantifies Human Insurgency". *Nature* 462:911–914.

Bryce, R. 2007. "Logistical Vulnerabilities and the Afghanistan War: The Pakistan Fuel Connection". *Heinrich Böll Foundation*. Accessed Mar. 14, 2013. http://www.boell.de/downloads/worldwide/bryce_logistical_vulnerabilities.pdf.

Callaway, D., J. Hopcroft, J. Kleinberg, M. Newman, and S. Strogatz. 2001. "Are Randomly Grown Graphs Really Random?". *Physical Review E* 64:041902.

Erdos, P., and A. Renyi. 1960. "On the Evolution of Random Graphs". *Publications of the Mathematical Institute of the Hungarian Academy of Science* 5:17–61.

Floyd, R. 1962. "Algorithm 97: Shortest Path". *Communications of the ACM* 5:345.

Fredman, M., and R. Tarjan. 1987. "Fibonacci heaps and their uses in improved network optimization algorithms". *Journal of the ACM* 34:596–615.

Girard, S., A. Martel, J. Berger, A. Boukhtouta, M. Chouinard, A. Ghanmi, and A. Guitouni. 2008. "Canadian Forces Overseas Supply Network: Strategic Need and Design Methodology". Technical Report CIRRELT-2008-34, Centre interuniversitaire de recherche sur les réseaux d'enterprise, la logistique et le transport, Québec, Canada.

Goyal, S., and A. Vigier. 2009. "Robust Networks". In *Microsoft Research Workshop on Networks, Auctions, and Pricing*. Cambridge, UK.

Goyal, S., and A. Vigier. 2013. "Attack, Defense and Contagion in Networks". *Working paper*.

Lumpkin, J. 2006. "USS Cole bombing". *GlobalSecurity.org*. Accessed Mar. 14, 2013. http://www.globalsecurity.org/security/profiles/uss_cole_bombing.htm.

Rodrique, J., and B. Slack. 2002. "Logistics and National Security". In *Science, Technology, and National Security*, edited by S. Majumdar, L. Rosenfeld, E. Miller, S. Alexander, and M. Rieders. Easton, PA: Pennsylvania Academy of Science.

Scardi, G., and T. Nepusz. 2006. "The igraph software package for complex network research". *InterJournal Complex Systems*:1695.

Thadakamalla, H., U. Raghavan, S. Kumara, and R. Albert. 2004. "Survivability of Multiagent-Based Supply Networks: A Topological Perspective". *IEEE Intelligent Systems* 19:24–31.

UK Border Agency 2012. "United Kingdom Border Agency Overseas Network". Accessed Mar. 15, 2013. http://www.ukba.homeoffice.gov.uk/aboutus/organisation/overseas-network/.

van Wijk, B., C. Stam, and A. Daffertshofer. 2010. "Comparing Brain Networks of Different Size and Connectivity Density Using Graph Theory". *PLoS ONE* 5:0013701.

Whitlock, C. 2011. "U.S. turns to other routes to supply Afghan war as relations with Pakistan fray". *Washington Post*. Accessed Dec. 25, 2012. http://articles.washingtonpost.com/2011-07-02/world/35267868_1_pakistan-routes-afghanistan-karachi.

Wilensky, U. 1999. "NetLogo". Center for Connected Learning and Computer-Based Modeling, Northwestern University. Evanston, IL. Accessed Dec. 25, 2012. http://ccl.northwestern.edu/netlogo/.

Wright, L. 2006. *Looming Tower*. New York, New York: Knopf.

Zhao, K., A. Kumar, T. Harrision, and J. Yen. 2011. "Analyzing the Resilience of Complex Supply Network Topologies Against Random and Targeted Disruptions". *IEEE Systems Journal* 5:28–39.

AUTHOR BIOGRAPHIES

ROBERT BRYCE is a NSERC Visiting Fellow with DRDC CORA. He received a Ph.D. in physics from the University of Alberta and his research interests include modern data analysis, algorithms, and computation. His email address is Robert.Bryce@drdc-rddc.gc.ca.

RAMAN PALL received a B.Sc. and an M.Sc. in mathematics from the University of Ottawa. He is currently a defence scientist with DRDC CORA. His research interests include military operations research, multi-criteria decision analysis, simulation modeling, transportation modeling, inventory management, and operational logistics. He has been published in a wide range of peer-reviewed journals and has authored several internal technical papers. His email address is Raman.Pall@drdc-rddc.gc.ca.

AHMED GHANMI received a B.Sc. in engineering, an M.Sc. and a Ph.D. in applied mathematics from Université Laval. He is a senior operational research scientist with DRDC CORA. His research interests include military operations research, operational logistics, decision analysis, and optimization of military problems. He has published widely in international journals and conference proceedings. His email address is Ahmed.Ghanmi@drdc-rddc.gc.ca.