An Investigation to Improve Community Resilience using Network Graph Analysis of Infrastructure Systems

Sarah Dunn

School of Civil Engineering and Geosciences

Newcastle University

Thesis submitted for the degree of Doctor of Philosophy

February 2014

ABSTRACT

Disasters can have devastating effects on our communities and can cause great suffering to the people who reside within them. Critical infrastructure underpins the stable functioning of these communities and the severity of disasters is often linked to failure of these systems.

Traditionally, the resilience of infrastructure systems is assessed by subjecting physically based models to a range of hazard scenarios. The problem with this approach is that it can only inform us of inadequacies in the system for the chosen scenarios, potentially leaving us vulnerable to unforeseen events. This thesis investigates whether network graph theory can be used to give us increased confidence that the system will respond well in untested scenarios by developing a framework that can identify generic system characteristics and hence describe the underlying resilience of the network. The novelty in the work presented in this thesis is that it overcomes a shortcoming in existing network graph theory by including the effects of the spatial distribution of geographically dispersed systems.

To consider spatial influence, a new network generation algorithm was developed which incorporated rules that connects system components based on both their spatial distribution and topology. This algorithm was used to generate proxy networks for the European, US and China air traffic networks and demonstrated that the inclusion of this spatial component was crucial to form the highly connected hub airports observed in these networks. The networks were then tested for hazard tolerance and in the case of the European air traffic network validated using data from the 2010 Eyjafjallajökull eruption. Hazard tolerance was assessed by subjecting the networks to a series of random, but spatially coherent, hazards and showed that the European air traffic network was the most vulnerable, having up to 25% more connections disrupted compared to a benchmark random network. This contradicts traditional network theory which states that these networks are resilient to random hazards. To overcome this shortcoming, two strategies were employed to improve the resilience of the network. One strategy 'adaptively' modified the topology (crises management) while the other 'permanently' modified it (hazard mitigation). When these modified networks were subjected to spatial hazards the 'adaptive' approach

produced the most resilient network, having up to 23% fewer cancelled air routes compared to the original network, for only a 5% change in airport capacity. Finally, as many infrastructure networks are flow based systems, an investigation into whether graph theory could identify vulnerabilities in these systems was conducted. The results demonstrated that by using a combination of both physically based and graph theory metrics produced the best predictive skill in identifying vulnerable nodes in the system.

This research has many important implications for the owners and operators of infrastructure systems. It has demonstrated the European air traffic network to be vulnerable to spatial hazard and shown that, because many infrastructure networks possess similar properties, may therefore be equally vulnerable. It also provides a method to identify generic system vulnerabilities and strategies to reduce these. It is argued that as this research has considered generic networks it can not only increase infrastructure resilience to known threats but also to previously unidentified ones and therefore is a useful method to help protect these systems to large scale disasters and reduce the suffering for the people in the communities who rely upon them.

ACKNOWLEDGEMENTS

First I would like to thank my family, particularly my parents, who have supported me not only throughout this research, but for the 7 years that I have been at university.

I would also like to than my supervisory team of Dr Sean Wilkinson, Prof Richard Dawson and Prof Jim Hall. Your support over the last 3 years has been gratefully received.

Finally, I would like to thank the EPSRC who funded this research and made it all possible.

LIST OF PUBLICATIONS

The results of this research have been used to complete three journal paper publications and four conference paper publications. The three journal paper publications form the Appendices for this thesis.

Journal Paper Publications

Dunn, S. and Wilkinson, S. M. (2013). "Identifying Critical Components in Infrastructure Networks using Network Topology" Journal of Infrastructure Systems **19**(2): 157-165.

Dunn, S., Fu, G., Wilkinson, S. M. and Dawson, R. (2013). "Network Theory for Infrastructure Systems Modelling" Proceedings of the ICE – Engineering Sustainability **166**(5): 281-292.

Wilkinson, S. M., Dunn, S. and Ma, S. (2012). "The vulnerability of the European air traffic network to spatial hazards" Natural Hazards **60**(3): 1027-1036.

Conference Paper Publications

Dunn, S., Wilkinson, S. M., Fu, G. and Dawson, R. (2013). "Modelling Infrastructure Systems for Resilience and Sustainability" *International Symposium for Next Generation Infrastructure, 2013*. Wollongong, Australia.

Dunn, S. and Wilkinson, S. M. (2013). "Enhancing the Resilience of Lifeline Systems using Network Graph Theory" *Young Engineers Conference: Society for Earthquake and Civil Engineering Dynamics, 2013*. Newcastle upon Tyne, UK.

Dunn, S. and Wilkinson, S. M. (2013). "Methods to Assess the Hazard Tolerance of Spatial Networks" *International Conference on Civil, Environmental and Infrastructure Engineering, 2013*. Copenhagen, Denmark.

Dunn S., Wilkinson, S. M., Fu, G. and Dawson, R. (2012). "Analysis of Infrastructure Networks" *Conference on Earth Systems Engineering, 2012*. Newcastle upon Tyne, UK.

ABBREVIATIONS

APL	……	(shortest) Average Path Length
CATN	……	China Air Traffic Network
D	……	Diameter
EATN	……	European Air Traffic Network
EU	……	European Union
FIR	……	Flight Information Region
K	……	Node degree
GIS	……	Geographic Information System
NC	……	Number of Clusters
NIN	……	Number of Isolated Nodes
NRA	……	National Risk Assessment
NRR	……	National Risk Register
MCS	……	Maximum Cluster Size
PE	……	Potential Energy
q	……	Flow
R	……	Resistance
UK	……	United Kingdom
USA	……	United States of America
USATN	……	United States Air Traffic Network

Legend information:

CL	……	'Clustered' nodal configuration
D	……	Nodes introduced in order of Distance
EX	……	Exponential network
P	……	Nodes introduced Proportional to distance
R	……	Nodes introduced Randomly
RND	……	Random network
SF	……	Scale-Free network
UA	……	Uniform with Area nodal configuration
UD	……	Uniform with Distance nodal configuration

SUMMARY OF IMPORTANT FIGURES

Presented here is a series of tables listing the important figures in this thesis and also describing the results presented and their relevance to this research. This is done so the reader can quickly find specific results for comparison purposes.

For Chapter 3 (the generation of synthetic networks for the EATN)

Figure	Network Class	Nodal Configuration	Showing
Figure 3.3	Scale-Free	EATN	Plotting the degree distribution for a scale-free network and showing that is not a good fit for the EATN.
Figure 3.5	Exponential	Uniform with area	Showing that the new network generation algorithm is capable of generating networks that are exponential in class.
Figure 3.8	Scale-Free and Exponential	EATN	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the topological structure of the EATN.
Figure 3.9	Scale-free and Exponential	EATN	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the spatial structure of the EATN.
Figure 3.12	Scale-free and Exponential	Bi-Linear	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the topological structure of the EATN.
Figure 3.13	Scale-free and Exponential	Bi-Linear	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the spatial structure of the EATN.
Figure 3.27	Scale-free and Exponential	Clustered	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the topological structure of the EATN.
Figure 3.28	Scale-free and Exponential	Clustered	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the spatial structure of the EATN.

For Chapter 3 (the hazard tolerance of the EATN)

Figure	Network(s)*	Hazard	Showing
Figure 3.29	Actual EATN and synthetic networks generated using the actual airport locations.	Actual Eyjafjallajökull	Showing that the synthetic networks display a similar hazard tolerance to the actual EATN.
Figure 3.31	Actual EATN and synthetic networks with bi-linear and clustered nodal layout	Actual and simulated Eyjafjallajökull	Showing that the synthetic networks display a similar hazard tolerance to the actual EATN, with the exception of the two days of disruption which removed the highest proportion of airspace.
Figure 3.33	Actual EATN and synthetic networks with bi-linear, clustered and actual nodal layout	Random, but spatially coherent	Showing that the synthetic networks display a similar hazard tolerance to the actual EATN, with the exception of a few hazard locations.
Figure 3.36	Actual EATN	Actual Eyjafjallajökull and 'central attack'	Showing that the EATN is more vulnerable to hazards located over the geographic centre of the network than the Eyjafjallajökull event.
Figure 3.37	Actual EATN and synthetic networks with bi-linear, clustered and actual nodal layout	Actual and simulated Eyjafjallajökull	Showing that the connectivity of the EATN, and synthetic networks, decreases with expansion of spatial hazard; but that the efficiency of these networks remains constant.

* All of these figures also include the results for the benchmark network.

For Chapter 3 (the generation of synthetic networks for the CATN and USATN)

Figure	Network Class	Nodal Configuration	Showing
Figure 3.43	Scale-Free and Exponential	CATN	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the topological structure of the CATN.
Figure 3.44	Scale-Free and Exponential	CATN	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the spatial structure of the CATN.

Figure	Network Class	Nodal Configuration	Showing
Figure 3.47	Scale-free and Exponential	Clustered	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the topological and spatial structure of the CATN.
Figure 3.48	Scale-free and Exponential	USATN	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the topological structure of the USATN.
Figure 3.49	Scale-free and Exponential	USATN	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the spatial structure of the USATN.
Figure 3.53	Scale-free and Exponential	Clustered	Showing that an exponential network, with constant radius size and includes the modification of GA is superior at replicating the topological and spatial structure of the USATN.

For Chapter 3 (the hazard tolerance of the CATN and USATN)

Figure	Network(s)*	Hazard	Showing
Figure 3.54	Actual CATN and USATN and the synthetic networks with actual and clustered nodal layouts	'Central attack'	The hazard tolerances of the synthetic networks are generally in good agreement with the actual networks.
Figure 3.55	10 synthetic networks for the USATN with a clustered nodal layout	'Central attack'	Showing that all of the synthetic networks, for the USATN, show approximately the same hazard tolerance.
Figure 3.56	Actual EATN, CATN and USATN	'Central attack'	Showing that the CATN and USATN display an initial resilience to this spatial hazard, whilst the EATN is always vulnerable.
Figure 3.57	Actual EATN, CATN and USATN	'Central attack'	Showing that the connectivity of the CATN degrades quicker than the EATN and USATN and that the efficiency of the USATN is most unchanged by the spatial hazard.

* All of these figures also include the results for the benchmark network.

For Chapter 4

Figure	Network(s)*	Nodal Configuration	Hazard	Showing
Figure 4.7	Scale-free and exponential	Uniform with area	'Central attack'	Introducing nodes with distance creates the most vulnerable network to this hazard location.
Figure 4.8	Scale-free and exponential	Uniform with area	'Perimeter attack'	Networks where nodes are introduced with distance initially show an increased resilience to this spatial hazard.
Figure 4.10 / Figure 4.11	Exponential / Scale-free	Uniform with area	7 locations of spatial hazard	That hazard location has little, or no, effect to the hazard tolerance of networks where nodes are introduced randomly, but can significantly affect those where nodes are introduced with distance.
Figure 4.12 / Figure 4.13	Exponential / Scale-Free	Uniform with distance	7 locations of spatial hazard	Networks with this nodal configuration show an increased vulnerability to hazards located around the geographic centre of the network than those with a uniform with area nodal configuration.
Figure 4.15 / Figure 4.16	Exponential / Scale-Free	Clustered	7 locations of spatial hazard	Networks with this nodal configuration show an increased vulnerability to hazards located around the geographic centre of the network than those with a uniform with area nodal configuration.
Figure 4.20	Random	Uniform with area, uniform with distance, clustered	'Central attack' and 'perimeter attack'	The change in connectivity for the benchmark random networks.
Figure 4.21	Random	Uniform with area, uniform with distance, clustered	'Central attack' and 'perimeter attack'	The change in efficiency for the benchmark random networks.

Figure	Network(s)*	Nodal Configuration	Hazard	Showing
Figure 4.22 / Figure 4.23	Scale-Free / Exponential	Uniform with area, uniform with distance, clustered	'Central attack' and 'perimeter attack'	Networks where nodes were introduced with distance show a lower connectivity, particularly when a high proportion of nodes have been removed.
Figure 4.24	Scale-Free	Uniform with area, uniform with distance, clustered	'Central attack' and 'perimeter attack'	That scale-free networks where nodes are introduced with distance show a decreased efficiency, than a random network.
Figure 4.25	Exponential	Uniform with area, uniform with distance, clustered	'Central attack' and 'perimeter attack'	That all exponential networks maintain efficiency as the hazard removes an increasing proportion of nodes.
Figure 4.28 / Figure 4.29	Scale-Free / Exponential	Uniform with area, uniform with distance, clustered	'Central attack' and 'perimeter attack'	The connectivity of the networks with a uniform with distance or clustered nodal configuration decreases quicker than those with a uniform with area configuration for the 'central attack' hazard, but show an increased connectivity to small sizes of the 'perimeter attack' hazard.
Figure 4.30	Scale-Free	Uniform with area, uniform with distance, clustered	'Central attack' and 'perimeter attack'	The efficiency of the networks with a uniform with distance or clustered nodal configuration decreases quicker than those with a uniform with area configuration.
Figure 4.31	Exponential	Uniform with area, uniform with distance, clustered	'Central attack' and 'perimeter attack'	Nodal configuration has little, or no, effect to the efficiency of exponential networks.

TABLE OF CONTENTS

ABSTRACT ..... **I**

ACKNOWLEDGEMENTS ..... **III**

LIST OF PUBLICATIONS ..... **IV**

ABBREVIATIONS ..... **V**

SUMMARY OF IMPORTANT FIGURES ..... **VI**

CHAPTER 1: INTRODUCTION **1**

1.1: IDENTIFICATION OF RESEARCH GAP 1

1.2: AIM OF RESEARCH 7

1.3: OBJECTIVES FOR THE RESEARCH 7

1.4: SCOPE OF RESEARCH 11

1.5: STRUCTURE OF THESIS 13

CHAPTER 2: INFRASTRUCTURE NETWORKS, RESILIENCE AND GRAPH THEORY ANALYSIS **15**

2.1: TYPES OF INFRASTRUCTURE NETWORKS 15

2.2: DEFINITIONS OF RESILIENCE 21

2.3: IDENTIFICATION OF MAIN THREATS TO INFRASTRUCTURE 28

2.3.1: Summary of the Main Threats To Infrastructure Systems and their Potential Impacts *36*

2.3.1.1: Weather Related Risks 37

2.3.1.2: Ground Condition Risks 40

2.3.1.3: Other Risks 42

2.4: REVIEW OF CURRENT ANALYSIS OF INFRASTRUCTURE SYSTEMS 46

2.5: NETWORK GRAPH THEORY 49

2.5.1: Types of Network Classes and Network Modelling *51*

2.5.2: Network Generation Algorithms *54*

2.5.2.1: Random Networks 55

2.5.2.2: Small-World Networks 56

2.5.2.3: Scale-Free Networks 56

2.5.2.4: Exponential Networks 58

2.5.3: Hazard Tolerance of Network Architectures and Failure Modes *59*

2.5.4: Network Measures *61*

2.5.4.1: Connectivity Measures 61

2.5.4.2: Performance Measures 63

2.5.4.3: Importance Measures 64

2.6: PREVIOUS APPLICATIONS OF GRAPH THEORY TO SOCIAL AND OTHER NETWORKS 70

2.7: APPLICATION OF GRAPH THEORY TO INFRASTRUCTURE NETWORKS 72

2.7.1: Communication Networks *72*
2.7.2: Electrical Distribution Networks (Power Grids) *74*
2.7.3: Transport Networks *78*
2.7.4: Water Distribution Systems *85*
2.8: Development of Spatial Network Models 88

CHAPTER 3: HAZARD TOLERANCE OF REAL WORLD SPATIAL NETWORKS 93

3.1: Case Study: The Disruption Caused to the European Air Traffic Network by the Eyjafjallajökull Volcano 94
3.2: Development of Algorithm to Generate Synthetic Networks for the European Air Traffic Network. 98
3.2.1: Hazard Tolerance of the Synthetic Networks *129*
3.2.2: Application of Network Measures to Quantify Change in Performance and Connectivity *140*
3.3: Hazard Tolerance of other Air Traffic Networks 146
3.3.1: Generating Synthetic Networks for the China Air Traffic Network *149*
3.3.2: Generating Synthetic Networks for the US Air Traffic Network *154*
3.3.3: Hazard Tolerance of the China and US Air Traffic Networks to Spatial Hazards *160*
3.3.4: Application of Network Theory Measures *166*

CHAPTER 4: ASSESSMENT OF THE VULNERABILITY OF GENERIC SPATIAL NETWORKS 171

4.1: Spatial Nodal Layouts 172
4.2: Network Generation Algorithms for Spatial Networks 174
4.3: Effect of Node Introduction Order to Hazard Tolerance 176
4.4: Effect of Spatial Hazard Distance to Hazard Tolerance 185
4.5: Comparison of Hazard Tolerance for Different Nodal Layouts 193
4.5.1: Uniform with Distance Nodal Layout *193*
4.5.2: Clustered Nodal Layout *200*
4.5.2.1: Effect Individual Cluster Density on the Hazard Tolerance of the Network 206
4.6: Quantifying Change in Performance / Connectivity using Network Measures 210
4.6.1: Connectivity and Efficiency of Benchmark Random Networks *210*
4.6.2: Effects of Node Introduction Order and Network Class *215*
4.6.3: Effects of Spatial Nodal Configuration *225*
4.7: Best / Worst Case Combinations for Hazard Tolerance 232
4.8: How Can the Resilience of Existing Real World Infrastructure Systems be Improved? 236
4.8.1: 'Adaptive' Strategy for Improving Resilience *238*
4.8.2: 'Permanent' Strategy for Improving Resilience *246*
4.8.3: Modification of 'Adaptive' Strategy for Improving Resilience *256*

CHAPTER 5: IDENTIFYING CRITICAL COMPONENTS IN INFRASTRUCTURE SYSTEMS 270

5.1: Development of a Reduced Complexity Flow Model 270
5.2: Assessment of using Network Graph Theory in Flow Based Problems 274
5.3: Application of Graph Theory to Identify Specific Vulnerable Areas 285

CHAPTER 6: CONCLUSIONS....292

6.1: MAIN FINDINGS....292

6.2: POSSIBLE FUTURE WORK....295

REFERENCES....298

APPENDIX A....311

APPENDIX B....322

APPENDIX C....332

LIST OF FIGURES

FIGURE 1.1: (A) (WLRN 2010) AND (B) (THE TELEGRAPH 2010) SHOWING THE DEVASTATION IN THE AFTERMATH OF THE MW7.0 HAITIAN EARTHQUAKE IN 2010. 1

FIGURE 1.2: THE NORTH AMERICAN POWER GRID (A) BEFORE AND (B) AFTER A CASCADING FAILURE, AFFECTING 45 MILLION PEOPLE IN 8 US STATES IN AUGUST 2003 (ELVIDGE 2003). 2

FIGURE 1.3: AN ILLUSTRATION OF PARALLEL EDGES/LINKS (BETWEEN NODES A-C AND B-D) AND SELF-LOOPS (NODES C AND D). 12

FIGURE 2.1: THE NINE NATIONAL INFRASTRUCTURE SECTORS AND ASSOCIATED SUB-SECTORS AS DEFINED BY THE UK GOVERNMENT (CABINET OFFICE 2011A)..... 18

FIGURE 2.2: THE FOUR COMPONENTS OF INFRASTRUCTURE RESILIENCE, ACCORDING TO CABINET OFFICE (2011B). 23

FIGURE 2.3: A CONCEPTUAL DEFINITION OF THE RESILIENCE OF AN INFRASTRUCTURE SYSTEM (BRUNEAU ET AL. 2003). 25

FIGURE 2.4: THE TYPICAL PERFORMANCE RESPONSE CURVE OF AN INFRASTRUCTURE SYSTEM FOLLOWING THE OCCURRENCE OF A HAZARD, ACCORDING TO OUYANG ET AL. (2012). 27

FIGURE 2.5: CIVIL EMERGENCIES AS IDENTIFIED IN THE NATIONAL RISK REGISTER (2013), SHOWING (A) RISKS OF TERRORIST AND OTHER MALICIOUS ATTACKS AND (B) RISKS OF NATURAL HAZARDS AND MAJOR ACCIDENTS. IT IS WORTH NOTING THAT THE TWO SCALES FOR RELATIVE LIKELIHOOD SHOWN IN (A) AND (B) ARE NOT DIRECTLY COMPARABLE WITH EACH OTHER. 31

FIGURE 2.6: AN ILLUSTRATION OF THE HIGH CONSEQUENCE RISK FACING THE UK (CABINET OFFICE 2011B). 32

FIGURE 2.7: NATIONAL RISKS TO INFRASTRUCTURE IN NEW ZEALAND (THE INSTITUTION OF PROFESSIONAL ENGINEERS NEW ZEALAND 2012). 35

FIGURE 2.8: THE PROPORTION OF NATIONAL INFRASTRUCTURE ASSETS LOCATED IN FLOOD RISK AREAS (ENVIRONMENT AGENCY 2009). 38

FIGURE 2.9: DAMAGE TO (A) POWER LINES (HOLLINGSHEAD 2007) AND (B) TRANSMISSION TOWERS DUE TO ICE STORMS (CANADIAN ENERGY ISSUES). 39

FIGURE 2.10: THE DISTRIBUTION OF ERODIBLE CLIFFS IN ENGLAND (ENVIRONMENT AGENCY 2010B). 41

FIGURE 2.11: THE POTENTIAL IMPACTS OF SPACE WEATHER. 43

FIGURE 2.12: HAZARD MAP FOR A 2,500 YEAR RETURN PERIOD SEISMIC EVENT IN THE UK (BRITISH GEOLOGICAL SURVEY 2013B). 44

FIGURE 2.13: A HYDRAULIC NETWORK SHOWING THE CONCENTRATION OF A CHEMICAL 15 HOURS AFTER IT WAS INJECTED INTO THE SYSTEM AT THE RIVER SOURCE (GRAYMAN 2006). 48

FIGURE 2.14: THE TEMPORAL VARIATION OF THE CHEMICAL USED TO CONTAMINATE THE HYDRAULIC NETWORK SHOWN IN AT NODE 265 (LOCATED IN THE CENTRE OF THE SYSTEM) (GRAYMAN 2006). 48

FIGURE 2.15: (A) A MAP REPRESENTING THE KONIGSBERG BRIDGE PROBLEM (PAOLETTI 2013) AND (B) A GRAPHICAL REPRESENTATION OF THE PROBLEM, WHERE THE LETTERS HAVE BEEN USED IN EACH IMAGE TO INDICATE CORRESPONDING 'ISLANDS'. 50

FIGURE 2.16: SHOWING (A) THE FOUR COLOUR THEOREM (ROBERTSON ET AL. 2007) AND (B) THE NETWORK USED TO CONSTRUCT THE PROOF OF THE SOLUTION. 50

FIGURE 2.17: SHOWING (A) PART OF A LARGER 100 NODE SCALE-FREE NETWORK (GENERATED USING NETWORK WORKBENCH (NWB TEAM 2006)) AND (B) THE DEGREE DISTRIBUTION FOR THE SAME NETWORK (WHICH FORMS A STRAIGHT LINE ON A LOG-LOG GRAPH). THE BLACK DOTS IN (A) REPRESENT THE NODES AND THE BLACK LINES THE CONNECTIONS BETWEEN THE NODES SHOWN. THE DASHED LINES REPRESENT LINKS TO NODES THAT HAVE NOT BEEN SHOWN FOR CLARITY AND THE NUMBER BESIDE EACH NODE INDICATES ITS DEGREE (I.E. 2 INDICATES THAT A NODE HAS TWO LINKS ATTACHED TO IT). THE DEGREE DISTRIBUTION FOR THIS NETWORK HAS BEEN OBTAINED USING THE METHOD OUTLINED IN THE TEXT. 52

FIGURE 2.18: (A) A SAMPLE RANDOM NETWORK AND (B) ITS DEGREE DISTRIBUTION, WHERE P(K) IN THIS FIGURE IS NOT CUMULATIVE (BARABASI AND OLTVAI 2004). 52

FIGURE 2.19: (A) A SAMPLE SCALE-FREE NETWORK AND (B) ITS DEGREE DISTRIBUTION, WHERE P(K) IN THIS FIGURE IS CUMULATIVE. IT CAN BE SEEN FROM THE DEGREE DISTRIBUTION IN (B) THAT A SCALE-FREE NETWORK FORMS A STRAIGHT LINE ON A LOG-LOG GRAPH (BARABASI AND OLTVAI 2004). 54

FIGURE 2.20: DEGREE DISTRIBUTION FOR THE NORTH AMERICAN POWER GRID, A REAL WORLD EXPONENTIAL NETWORK (DENG ET AL. 2011). NOTE THAT FOR AN EXPONENTIAL NETWORK THIS DISTRIBUTION FORMS A STRAIGHT LINE WHEN PLOTTED ON A LOG-LINEAR SCALE. 54

FIGURE 2.21: FIVE RANDOM NETWORKS, GENERATED USING NETWORK WORKBENCH (NWB TEAM 2006), WITH DIFFERENT VALUES OF LINKING PROBABILITY (L). 55

FIGURE 2.22: SHOWING THE EFFECTS OF THE REWIRING PROBABILITY (P) IN THE SMALL-WORLD GENERATION ALGORITHM (WATTS AND STROGATZ 1998). 56

FIGURE 2.23: DEMONSTRATING THE IDEA OF *PREFERENTIAL ATTACHMENT* USING THE SECTION OF THE SCALE-FREE NETWORK SHOWN IN FIGURE 2.17(A). THE BLACK DOTS SHOW THE NODES THAT ALREADY FORM PART OF THE NETWORK AND THE RED DOT SHOWS THE NEW NODE THAT HAS BEEN ADDED AT THIS 'TIMETEP'. THIS NEW NODE IS LIKELY TO PREFERENTIALLY ATTACH TO THE NODE WITH THE HIGHEST DEGREE IN THE NETWORK (THE NODE WITH A DEGREE OF 6). THIS IS SHOWN BY THE PRESENCE OF A NEW LINK (RED DASHED LINE). IT IS WORTH NOTING THAT THIS NODE IS ASSUMED TO ONLY INTRODUCE ONE NEW LINK TO THE NETWORK. 57

FIGURE 2.24: SHOWING A SCALE-FREE NETWORK (REPRESENTING THE US AIR TRAFFIC NETWORK) SUBJECTED TO THE RANDOM NODE FAILURE AND TARGETED ATTACK STRATEGIES (BARABASI AND BONABEAU 2003). 60

FIGURE 2.25: PLOTTING THE NORMALISED BETWEENESS AND DEGREE OF A NODE FOR THE ITALIAN AIR TRAFFIC NETWORK (BLACK SQUARES) AND A RANDOM NETWORK (GREY CIRCLES) (GUIDA AND MARIA 2007). 66

FIGURE 2.26: (A) PLOTTING THE BETWEENNESS CENTRALITY OF A NODE WITH ITS DEGREE (CIRCLES) FOR THE WORLDWIDE AIR TRAFFIC NETWORK. THIS FIGURE ALSO SHOWS THE RELATIONSHIP FOR A RANDOM NETWORK, WHERE 95% OF THE DATA FALLS INSIDE THE GREY REGION. ALSO SHOWING THE LOCATION OF 25 CITIES THAT HAVE THE HIGHEST (B) DEGREE AND (C) BETWEENNESS CENTRALITY (GUIMERA ET AL. 2005) 67

FIGURE 2.27: AN EXAMPLE OF HOW A NODE CAN HAVE A HIGH VALUE OF BETWEENNESS CENTRALITY AND A LOW DEGREE. IN THIS EXAMPLE, THE RED NODE WILL HAVE A HIGH BETWEENNESS CENTRALITY, AS IT IS ONE THE SHORTEST PATH OF MANY OTHER NODES IN THE NETWORK, AND A LOW DEGREE, AS IT ONLY HAS TWO CONNECTING NODES. 68

FIGURE 2.28: PLOTTING THE DEGREE OF A NODE (K) WITH ITS BETWEENNESS (L) FOR THE ITALIAN ELECTRICAL DISTRIBUTION NETWORK (CRUCITTI ET AL. 2004B). 69

FIGURE 2.29: THE CHANGES IN THE DIAMETER, D, OF THE NETWORK AS A FUNCTION OF THE FRACTION (F) OF THE REMOVED NODES, FOR NETWORKS SUBJECTED TO A TARGETED AND RANDOM FAILURE ATTACK STRATEGIES. (A) SHOWS A

comparison between a random network and a scale-free network, generated using the network generation algorithms of Erdos and Renyi (1960) and Barabasi and Albert (1999). Also showing the changes to the diameter of the (b) Internet and (c) World-Wide-Web (Albert et al. 2000). 73

Figure 2.30: The electrical distribution network for (a) the United Kingdom and (b) Italy and (c) the degree distribution for both of these networks and the European power grid (UCTE) (Rosas-Casals et al. 2006). 75

Figure 2.31: Showing a cascading failure in a sample network, which has one generator node, one demand node and three distributor nodes. In this sample network it is assumed that each node and link has the same resistance and that each link has infinite capacity. (a) Shows the original network, where the direction of flow is indicated by the arrows (on the links), the capacity of each distributor node is shown in white on the node and the flow through each node is shown in black above the node. To initiate a cascading failure the middle distributor node is removed (shown in red in (a)). The removal of this node causes the flow to be redistributed throughout the network (b). This redistribution of flow causes one of the other distributor nodes to fail, as the amount of flow trying to pass through the node is greater than its capacity. The failure of this node results in the network shown in (c) and the resulting redistribution of flow causes the remaining distributor node to be overcapacity and fail. It is worth noting that in this example only the capacity of the nodes was considered. It is likely that in many real world networks the links will also have a fixed level of capacity which, if exceeded, would cause them to fail. 76

Figure 2.32: Connectivity loss in the North American power grid due to the removal of nodes, using one of four different algorithms: randomly (circles), in decreasing order of the node degree (triangles) or load (diamonds), and by recalculating the load every ten steps and removing the ten nodes with the highest load (squares). 77

Figure 2.33: Showing the freeway network of Shanghai, consisting of 27 nodes and 49 links, where node 9 represents the centroid of Shanghai central city (Tu et al. 2013). 79

Figure 2.34: An image of the Romanian railway network (Mathe et al 2013). 80

Figure 2.35: Showing degree distributions for the (a) Indian air traffic network, containing 79 nodes and 442 links (Bagler 2008) and the Brazilian air traffic network in (b) 1995 and (c) 2006 (da Rocha 2009). It is worth noting that these studies only consider the presence of an air route between two nodes in the network (i.e. intercontinental flights are not considered) and the networks are not weighted or directed. 81

Figure 2.36: Degree distributions for each day of the week for the Austrian air traffic network, showing (a) all incoming flights, (b) all outgoing flights and (c) all flights on Monday (Han et al. 2008). 82

Figure 2.37: The change in the mean degree of airports in the Austrian and Chinese air traffic networks for different days of the week. The graph was obtained from (Zanin and Lillo 2013) and produced using the data of (Han et al. 2008) and (Li and Cai 2004). 83

Figure 2.38: The degree distribution for the Italian air traffic network for three different times during the year (a) 1st June 2005 to 31st May 2006, (b) 16th July 2005 to 14th August 2005 and (c) November 2005 (Guida and Maria 2007). 84

Figure 2.39: Showing the degree distribution of the worldwide air traffic network (Guimera et al. 2005).. 85

FIGURE 2.40: SHOWING A GRAPH VIEW OF FOUR WATER DISTRIBUTION NETWORKS, (A) ANYTOWN, (B) COLORADO SPRINGS, (C) EXNET AND (D) RICHMOND (YAZDANI AND JEFFREY 2011). 86
FIGURE 2.41: THE DEGREE DISTRIBUTIONS OF THE FOUR WATER DISTRIBUTION SYSTEMS SHOWN IN FIGURE 2.40 (YAZDANI AND JEFFREY 2011). 87
FIGURE 2.42: A COLOUR-CODED MAP SHOWING THE (A) CLOSENESS AND (B) BETWEENNESS CENTRALITY OF THE URBAN STREET NETWORK IN VENICE, ITALY (CRUCITTI ET AL. 2006). 89
FIGURE 2.43: NETWORKS GENERATED WITH DIFFERENT NODAL CONNECTIVITY, FOR THE SAME NODAL LAYOUT, DEPENDING ON USER PREFERENCE (Λ), WHERE: (A) Λ = 0, (B) Λ = 1/3, (C) Λ = 2/3 AND (D) Λ = 1 (GASTNER AND NEWMAN 2006B). 90
FIGURE 2.44: FACILITY LOCATIONS IN THE US, AS DETERMINED BY THE ALGORITHM OF GASTNER AND NEWMAN (2006A). 90
FIGURE 3.1: OPEN (LIGHT GREEN) AND CLOSED (GREY) FIRS IN EUROPE (I.E. AIRSPACE) FOR (A) 15TH APRIL, (B) 18TH APRIL AND (C) 21ST APRIL 2010 (EUROCONTROL 2010). THE AIRPORTS ARE SHOWN AS DOTS AND THE EYJAFJALLAJÖKULL VOLCANO AS A RED TRIANGLE. ALSO, (D) SHOWING PROPORTION OF TRAVEL DISRUPTION, RELATIVE TO THE PROPORTION OF CLOSED AIRSPACE, DURING THE EYJAFJALLAJÖKULL ERUPTION OF 14TH - 21ST APRIL 2010. THE POINTS ON THE GRAPH REPRESENT THE DIFFERENT DAYS OF DISRUPTION (LABELLED) AND THE RANDOM NETWORK (WITH RANDOM NODAL LAYOUT) IS SHOWN BY THE GREY LINE. 95
FIGURE 3.2: SHOWING THE RESILIENCE RANDOM NETWORK BENCHMARK PLOTTED IN TERMS OF THE PROPORTION OF REMOVED LINKS AND (A) REMOVED NODES AND (B) REMOVED AREA. 96
FIGURE 3.3: PLOTTING THE DEGREE DISTRIBUTION OF THE EATN (BLACK DOTS) AND A GENERATED SCALE-FREE NETWORK (RED DOTS), USING THE ALGORITHM OF BARABASI AND ALBERT (1999). 97
FIGURE 3.4: DEMONSTRATING THE IDEA OF PREFERENTIAL ATTACHMENT BASED ON (A) DEGREE AND (B) DEGREE AND PROXIMITY, IN PART OF A SAMPLE NETWORK. IN THIS NETWORK THE BLACK DOTS REPRESENT NODES (WITH THE ADJACENT NUMBER INDICATING ITS DEGREE), THE BLACK LINES REPRESENT LINKS CONNECTING THESE NODES AND THE DASHED LINES REPRESENT CONNECTIONS TO OTHER NODES IN THE NETWORK, THAT HAVE BEEN OMITTED FOR CLARITY. IN (A) A NEW NODE (RED) IS INTRODUCED TO THE NETWORK, AND USING THE ALGORITHM OF BARABASI AND ALBERT (1999) WOULD BE MOST LIKELY TO ATTACH ITSELF TO THE HIGH DEGREE NODE; HOWEVER, CONSIDERING PROXIMITY AS WELL AS DEGREE ALTERS THE PROBABILITY BECAUSE THE SPATIAL DOMAIN OF THE LOW DEGREE NODE (IN THE CENTRE OF THE RED CIRCLE) INCLUDES THE HIGH DEGREE NODE AND THEREFORE INFLATES ITS PROBABILITY OF ATTACHMENT. 98
FIGURE 3.5: THE DEGREE DISTRIBUTION OF AN EXPONENTIAL NETWORK GENERATED USING THE DEVELOPED ALGORITHM. ... 99
FIGURE 3.6: THE AIR ROUTE DISTANCE BETWEEN AIRPORTS (IN KM) COMPARED TO (A) THE MAXIMUM DEGREE OF CONNECTED AIRPORTS, (B) THE ARITHMETIC MEAN OF THE TWO CONNECTED AIRPORTS AND (C) THE GEOMETRIC MEAN OF THE TWO CONNECTED AIRPORTS FOR THE EATN. ALSO SHOWING (D) THE CORRELATION BETWEEN THE DEGREE OF AN AIRPORT AND THE MAXIMUM DISTANCE FLIGHT FROM THIS AIRPORT. ALL OF THE PLOTS SHOW THAT THERE IS NO CORRELATION BETWEEN THE AIR ROUTE DISTANCE AND VARIOUS MEASURES OF DEGREE OF THE TWO CONNECTED AIRPORTS. 100
FIGURE 3.7: PLOTTING (A) THE DISTRIBUTION OF AIRPORTS AND (B) THE SPATIAL DEGREE DISTRIBUTION OF AIRPORTS FOR THE EATN. 102
FIGURE 3.8: SHOWING THE DEGREE DISTRIBUTION FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM, WHERE NODES ARE INTRODUCED (A) RANDOMLY, (B) PROPORTIONAL WITH DISTANCE, (C) WITH DISTANCE FROM THE GEOGRAPHIC CENTRE AND (D) BASED ON THE POPULATION OF EACH COUNTRY. 104

FIGURE 3.9: SHOWING THE SPATIAL DEGREE DISTRIBUTION FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM, WHERE NODES ARE INTRODUCED (A) RANDOMLY, (B) PROPORTIONAL WITH DISTANCE, (C) WITH DISTANCE FROM THE GEOGRAPHIC CENTRE AND (D) BASED ON THE POPULATION OF EACH COUNTRY. 105

FIGURE 3.10: GIS GENERATED IMAGES SHOWING THE LOCATION AND THE DEGREE OF NODES (RED NODES ARE HIGH DEGREE AND GREEN ARE LOW DEGREE) FOR (A) THE ACTUAL EATN AND GENERATED NETWORKS WHERE THE NODES ARE INTRODUCED (B) RANDOMLY, (C) PROPORTIONAL WITH DISTANCE, (D) WITH DISTANCE AND (E) WITH POPULATION. ALSO SHOWING (F) THE POPULATION DENSITY MAP FOR EUROPE (GFK GEOMARKETING 2013). 108

FIGURE 3.11: (A) SIMULATED RANDOM BI-LINEAR NODAL LAYOUT FOR THE EATN, WHERE THE BLACK DOTS REPRESENT THE NODES AND THE GREY LINE THE SPATIAL BOUNDARY OF THE NETWORK. (B) A COMPARISON FOR THE SPATIAL DISTRIBUTION OF NODES FOR THE EATN (BLACK) AND THE BI-LINEAR NODAL LAYOUT SHOWN IN (A) (GREY). 109

FIGURE 3.12: SHOWING THE DEGREE DISTRIBUTION FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM FOR A BI-LINEAR NODAL LAYOUT; WHERE NODES ARE INTRODUCED (A) RANDOMLY, (B) PROPORTIONAL WITH DISTANCE AND (C) WITH DISTANCE FROM THE GEOGRAPHIC CENTRE. IN THE LEGEND, R REFERS TO THE SIZE OF THE NEIGHBOURHOOD RADIUS AND GA REFERS TO THE MODIFICATION OF GUIMERA AND ALBERT (2004). 110

FIGURE 3.13: SHOWING THE SPATIAL DEGREE DISTRIBUTION FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM FOR A BI-LINEAR NODAL LAYOUT; WHERE NODES ARE INTRODUCED (A) RANDOMLY, (B) PROPORTIONAL WITH DISTANCE AND (C) WITH DISTANCE FROM THE GEOGRAPHIC CENTRE. IN THE LEGEND, R REFERS TO THE SIZE OF THE NEIGHBOURHOOD RADIUS AND GA REFERS TO THE MODIFICATION OF GUIMERA AND ALBERT (2004). 111

FIGURE 3.14: SHOWING THREE NODAL LAYOUTS WHERE THE NODES HAVE BEEN INTRODUCED WITH (A) DISTANCE, (B) PROPORTIONAL WITH DISTANCE AND (C) RANDOMLY. THE BLACK DOTS INCULCATE NODES WITH A HIGH DEGREE AND LIGHT GREY INDICATE THOSE WITH A LOW DEGREE AND THE BLACK LINE INDICATES THE CIRCULAR SPATIAL BOUNDARY OF THE NETWORK. 113

FIGURE 3.15: PLOTTING THE AIRPORTS OF THE EUROPEAN AIR TRAFFIC NETWORK WITHIN A CIRCULAR SPATIAL BOUNDARY. 114

FIGURE 3.16: SHOWING (A) THE SPATIAL LAYOUT OF NODES IN THE WAL-MART DATASET AND (B) THE ASSOCIATED SPATIAL DISTRIBUTION; (C) SHOWING THE SPATIAL LAYOUT OF NODES FOR THE TARGET DATASET AND (D) THE ASSOCIATED SPATIAL DISTRIBUTION. THE GEOGRAPHIC CENTRE FOR THE WAL-MART DATASET IS LOCATED APPROXIMATELY 130KM NORTH-EAST OF ST LOUIS AND FOR THE TARGET DATASET IS LOCATED 250KM WEST OF ST LOUIS. THE RESULTS HAVE BEEN SHOWN IN TERMS OF THE PERCENTAGE DISTANCE FROM THE GEOGRAPHIC CENTRE DUE TO ENABLE A DIRECT COMPARISON BETWEEN THE TWO DATASETS (AS THEY HAVE A DIFFERENT MAXIMUM RADIUS) 115

FIGURE 3.17: SHOWING THE EXTREME VALUES FOR THE NEAREST NEIGHBOUR INDEX DEVELOPED BY EBDON (1977), WHERE 0 INDICATES A COMPLETELY CLUSTERED LAYOUT, 1.00 A RANDOM LAYOUT AND 2.15 A COMPLETELY DISPERSED LAYOUT. 116

FIGURE 3.18: A NODAL DISTRIBUTION USED TO SHOW AN EXAMPLE OF THE NEAREST NEIGHBOUR INDEX CALCULATION. THE NODES ARE REPRESENTED BY THE BLACK DOTS (WITH THEIR NODE NUMBERS), THE GREY ARROWS INDICATE THE NEAREST NEIGHBOUR OF EACH NODE (DETERMINED BY DISTANCE) AND THE GREY DOTTED BOX DEFINES THE SPATIAL BOUNDARY OF THE NODES. 116

FIGURE 3.19: SHOWING THREE INDIVIDUAL CLUSTERS FROM THE WAL-MART DATASET: (A) DENVER, (B) HOUSTON AND (C) MINNEAPOLIS, WHERE THE DOTS SHOW THE LOCATION OF STORES. THE AREA OF EACH CLUSTER IS DEFINED AS A CIRCLE, WHERE THE FIRST STORE OPENED IS THE MIDPOINT (I.E. THE FIRST NODE INTRODUCED) AND THE RADIUS EXTENDS FROM THIS POINT TO THE STORE FURTHEST FROM THE CENTRE. GRAPHS SHOWING HOW THE RADIUS OF EACH CLUSTER CHANGES WITH EACH OPENED STORE HAVE BEEN PLOTTED FOR EACH CLUSTER: (E) DENVER, (F), HOUSTON AND (G) MINNEAPOLIS. 119

FIGURE 3.20: SHOWING THE RELATIONSHIP BETWEEN THE NUMBER OF NODES IN AN INDIVIDUAL CLUSTER AND THE RESULTING CHANGE IN RADIUS OF THAT CLUSTER (GREY LINE) USED IN THE ALGORITHM AND THE ACTUAL RELATIONSHIP BETWEEN THESE TWO VARIABLES FOR THE DENVER CLUSTER IN THE WAL-MART DATASET (BLACK DOTS). 121

FIGURE 3.21: SHOWING THE PROGRESSION OF THE CLUSTERING ALGORITHM FOR TWO GENERATED NETWORKS ((A)-(D) AND (E)-(H)) WITH DIFFERENT C_D VALUES (200 AND 400 RESPECTIVELY). WHERE THE BLACK DOTS REPRESENT THE STARTING NODES AND THE GREY DOTS SHOW THE ADDED NODES, THE OUTER CIRCLE DEFINES THE SPATIAL BOUNDARY OF THE NETWORK. (A) AND (E) SHOW THE SEED NODES (ALL OF THE STARTING NODES HAVE THE SAME RADIUS); (B) AND (F) SHOW THE LAYOUT AFTER 150 NODES HAVE BEEN ADDED; (C) AND (G) SHOW THE LAYOUT AFTER 350 NODES HAVE BEEN ADDED; (D) AND (H) SHOW THE FINAL NODAL LAYOUT. 122

FIGURE 3.22: SHOWING THREE SEED NODES (BLACK) WITH DIFFERENT RADII VALUES AND THE SUBSEQUENT ADDED NODES (GREY). THE TOP LEFT STARTING NODE HAS A RADIUS VALUE OF 800, THE CENTRAL STARTING NODE HAS A RADIUS OF 500 AND THE BOTTOM RIGHT NODE HAS A RADIUS OF 10. 123

FIGURE 3.23: SHOWING THE GENERATED SPATIAL DISTRIBUTION OF THE NODES (GREY) COMPARED TO THE ACTUAL DISTRIBUTION OF STORES (BLACK) FOR (A) WAL-MART AND (B) TARGET. 124

FIGURE 3.24: SHOWING (A) ONE CLUSTER FROM THE PROXY WAL-MART NETWORK, WHERE THE SEED NODE IS SHOWN AS A BLACK DOT, THE ADDED NODES AS GREY DOTS AND THE SPATIAL BOUNDARY IS INDICATED BY THE BLACK LINE; AND (B) SHOWING HOW THE RADIUS OF THE CLUSTER CHANGES WITH ADDED NODES 125

FIGURE 3.25: SHOWING THE LOCATION OF STORES IN THE WAL-MART DATASET AND HIGHLIGHTING TWO POSSIBLE BOUNDARIES FOR THE MINNEAPOLIS CLUSTER. 125

FIGURE 3.26: (A) SIMULATED CLUSTERED NODAL LAYOUT FOR THE EATN, WHERE THE BLACK DOTS REPRESENT THE INITIAL NODES, THE GREY DOTS THE ADDED NODES AND THE BLACK LINE THE SPATIAL BOUNDARY OF THE NETWORK. (B) A COMPARISON FOR THE SPATIAL DISTRIBUTION OF NODES FOR THE EATN (BLACK) AND THE CLUSTERED NODAL LAYOUT SHOWN IN (A) (GREY). 126

FIGURE 3.27: SHOWING THE DEGREE DISTRIBUTION FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM WITH A CLUSTERED NODAL LAYOUT; WHERE NODES ARE INTRODUCED (A) RANDOMLY, (B) PROPORTIONAL WITH DISTANCE AND (C) WITH DISTANCE FROM THE GEOGRAPHIC CENTRE. IN THE LEGEND, R REFERS TO THE SIZE OF THE NEIGHBOURHOOD RADIUS AND GA REFERS TO THE MODIFICATION OF GUIMERA AND ALBERT (2004). 127

FIGURE 3.28: SHOWING THE SPATIAL DEGREE DISTRIBUTION FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM WITH A CLUSTERED NODAL LAYOUT; WHERE NODES ARE INTRODUCED (A) RANDOMLY, (B) PROPORTIONAL WITH DISTANCE AND (C) WITH DISTANCE FROM THE GEOGRAPHIC CENTRE. IN THE LEGEND, R REFERS TO THE SIZE OF THE NEIGHBOURHOOD RADIUS AND GA REFERS TO THE MODIFICATION OF GUIMERA AND ALBERT (2004). 128

FIGURE 3.29: THE ACTUAL EATN (BLACK DOTS) AND THE AVERAGE OF 10 SYNTHETIC EATN NETWORKS (BLUE DOTS) SUBJECTED TO THE ACTUAL EYJAFJALLAJÖKULL EVENT, PLOTTING THE RESULTS IN TERMS OF PERCENTAGE LINKS REMOVED (I.E. PERCENTAGE OF CLOSED AIR ROUTES) AND (A) PERCENTAGE OF NODES REMOVED (I.E. PERCENTAGE OF CLOSED AIRPORTS) AND (B) PERCENTAGE AREA REMOVED (I.E. PROPORTION OF CLOSED AIR SPACE). ALSO SHOWN ARE TWO RANDOM NETWORKS, ONE WITH THE ACTUAL EATN NODAL LOCATIONS (GREY DOTS) AND THE OTHER WITH RANDOM NODAL LOCATIONS (GREY LINE). 132

FIGURE 3.30: SHOWING THREE SIZES OF THE SIMULATED EYJAFJALLAJÖKULL EVENT, IN WHICH THE HAZARD STARTS AT THE SPATIAL BOUNDARY OF THE NETWORK (BLACK LINE) AND GROWS OUTWARDS UNTIL THE WHOLE NETWORK AREA IS COVERED (I.E. FROM (A) TO (B) TO (C)). 133

FIGURE 3.31: THE ACTUAL EATN (BLACK DOTS) SUBJECTED TO THE EYJAFJALLAJÖKULL EVENT AND THE AVERAGE OF 10 SYNTHETIC NETWORKS FOR BOTH THE BI-LINEAR (LIGHT BLUE LINE) AND CLUSTERED NODAL LAYOUTS (DARK BLUE LINE), SUBJECTED TO A SIMULATED EYJAFJALLAJÖKULL EVENT (FIGURE 3.30). ALSO SHOWING ONE RANDOM NETWORK WITH RANDOM NODAL LOCATIONS (BLACK LINE). THE RESULTS ARE PLOTTED IN TERMS OF THE PERCENTAGE OF LINKS REMOVED AND THE PERCENTAGE OF (A) NODES AND (B) AREA REMOVED. 134

FIGURE 3.32: SHOWING THREE LOCATIONS AND SIZES OF THE SIMULATED RANDOM SPATIAL HAZARD, THE CENTRE OF THE HAZARD IS A RANDOMLY GENERATED POINT WITHIN THE SPATIAL BOUNDARY OF THE NETWORK AND HAS A RANDOMLY GENERATED RADIUS VALUE. UNLIKE THE SIMULATED EYJAFJALLAJÖKULL EVENT (FIGURE 3.30), THESE HAZARDS DO NOT 'GROW' OUTWARDS. 135

FIGURE 3.33: THE ACTUAL EATN (BLACK DOTS) SUBJECTED TO A RANDOM SPATIALLY COHERENT HAZARD AND THE AVERAGE OF 10 SYNTHETIC NETWORKS FOR THE BI-LINEAR (RED DOTS), CLUSTERED (RED DOTS) AND ACTUAL (GREY DOTS) SUBJECTED TO THE SAME RANDOM SPATIALLY COHERENT HAZARDS. DUE TO THE DIFFERENCES IN THE CO-ORDINATE SYSTEMS THERE ARE SLIGHT VARIATIONS IN THE PERCENTAGE AREA CALCULATED BETWEEN THE ACTUAL AND SYNTHETIC NETWORKS (I.E. THE ACTUAL NETWORK IS ON A CURVED SURFACE AND THE SYNTHETIC NETWORKS ARE ON A FLAT SURFACE). 136

FIGURE 3.34: GIS GENERATED IMPACTS SHOWING FOUR POSITIONS OF THE RANDOM SPATIAL HAZARD OVER THE EATN, WITH APPROXIMATELY THE SAME HAZARD AREA (AROUND 10%) WHERE THE AIRPORTS ARE SHOWN AS GREEN DOTS, THE WEIGHTED GEOGRAPHIC CENTRE IS SHOWN AS A RED DOT, THE FIRS ARE INDICATED BY THE BLACK LINES, THE CENTRE OF THE RANDOM SPATIAL HAZARD IS SHOWN BY A BLACK DOT AND THE SHADED BLUE CIRCLE INDICATES THE SIZE OF THE HAZARD. IT IS WORTH NOTING, THAT ONLY THE AREA OF THE HAZARD WHICH LIES WITHIN THE FIR OF THE EATN IS CONSIDERED AS PART OF THE HAZARD AREA. 138

FIGURE 3.35: SHOWING THREE SIZES OF THE SIMULATED 'CENTRAL ATTACK' SPATIAL HAZARD, IN WHICH THE HAZARD STARTS AT THE SPATIAL CENTRE OF THE NETWORK AND GROWS OUTWARDS UNTIL THE WHOLE NETWORK AREA IS COVERED (I.E. FROM (A) TO (B) TO (C)). 139

FIGURE 3.36: SHOWING THE ACTUAL EATN SUBJECTED TO THE ACTUAL VOLCANIC EVENT (BLACK DOTS) AND ALSO SUBJECTED TO THE 'CENTRAL ATTACK' SPATIAL HAZARD (FIGURE 3.35) (BLACK LINE). ALSO SHOWING A BENCHMARK RANDOM NETWORK, WITH RANDOM NODAL LOCATION (GREY LINE). THE RESULTS ARE PLOTTED IN TERMS OF THE PERCENTAGE OF LINKS REMOVED AND THE PERCENTAGE OF (A) NODES AND (B) AREA REMOVED. 140

FIGURE 3.37: SHOWING THE CHANGE IN (A, B) MCS AND (C, D) APL FOR THE EATN AND THE AVERAGE OF 10 SYNTHETIC NETWORKS WHEN SUBJECTED TO THE ACTUAL / SIMULATED EYJAFJALLAJÖKULL EVENTS. 142

FIGURE 3.38: A COMPARISON BETWEEN THE NUMBER OF LINKS IN A NETWORK AND ITS SHORTEST AVERAGE PATH LENGTH (APL) FOR RANDOM NETWORKS (BLACK) AND EXPONENTIAL NETWORKS (GREY). THE TREND LINES FOR BOTH THE RANDOM AND EXPONENTIAL NETWORKS FOLLOW A POWER LAW. 145
FIGURE 3.39: SHOWING THE AIRPORT LOCATIONS OF THE (A) CHINA AND (B) US AIR TRAFFIC NETWORKS. 146
FIGURE 3.40: SHOWING THE DEGREE DISTRIBUTION, PLOTTED ON A LOG-LOG AND LOG-LINEAR SCALES, RESPECTIVELY, FOR THE (A, B) CHINA AND (C, D) USA AIR TRAFFIC NETWORKS. 147
FIGURE 3.41: SHOWING THE SPATIAL DISTRIBUTION OF AIRPORTS AND THE SPATIAL DEGREE DISTRIBUTION, RESPECTIVELY, FOR THE (A, B) CHINA AND (C, D) USA AIR TRAFFIC NETWORKS. 148
FIGURE 3.42: SHOWING THE SPATIAL DISTRIBUTION OF NODES FOR (A) THE CHINA AIR TRAFFIC NETWORK AND (B) THE US AIR TRAFFIC NETWORK AND A GENERATED BI-LINEAR NODAL CONFIGURATION. 148
FIGURE 3.43: SHOWING THE DEGREE DISTRIBUTION FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM FOR THE ACTUAL NODE LOCATIONS, WHERE NODES ARE INTRODUCED (A) RANDOMLY AND (B) WITH POPULATION TO THE NETWORK. 149
FIGURE 3.44: SHOWING THE SPATIAL DEGREE DISTRIBUTIONS FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM FOR THE ACTUAL NODE LOCATIONS, WHERE NODES ARE INTRODUCED (A) RANDOMLY AND (B) WITH POPULATION TO THE NETWORK. 150
FIGURE 3.45: GIS GENERATED IMAGES OF THE (A) ACTUAL CHINA AIR TRAFFIC NETWORK AND (B) A GENERATED NETWORK (THE BLUE LINE IN FIGURE 3.43(A) AND FIGURE 3.44(A) WHERE THE COLOUR OF THE NODE INDICATES ITS DEGREE (RED TO GREEN, FOR HIGH TO LOW DEGREE). THE BLACK DOT IN EACH PART SHOWS THE LOCATION OF THE GEOGRAPHIC CENTRE OF THE ACTUAL NETWORK (NOTE THAT THIS IS NOT RECALCULATED FOR THE SYNTHETIC NETWORK). 151
FIGURE 3.46: (A) SIMULATED CLUSTERED NODAL LAYOUT FOR THE CHINA AIR TRAFFIC NETWORK (CATN), WHERE THE BLACK DOTS REPRESENT THE SEED NODES, THE GREY DOTS THE ADDED NODES AND THE BLACK LINE THE SPATIAL BOUNDARY OF THE NETWORK. (B) A COMPARISON FOR THE SPATIAL DISTRIBUTION OF NODES FOR THE CATN (BLACK) AND THE SYNTHETIC NODAL LAYOUT (GREY) 152
FIGURE 3.47: SHOWING DEGREE DISTRIBUTION AND SPATIAL DEGREE DISTRIBUTIONS, RESPECTIVELY, FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM, WHERE NODES ARE INTRODUCED RANDOMLY TO THE NETWORK FOR THE CLUSTERED NODAL LAYOUT (FIGURE 3.46). 153
FIGURE 3.48: SHOWING THE DEGREE DISTRIBUTION FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM FOR THE ACTUAL NODE LOCATIONS, WHERE NODES ARE INTRODUCED (A) RANDOMLY AND (B) WITH POPULATION TO THE NETWORK. 154
FIGURE 3.49: SHOWING THE SPATIAL DEGREE DISTRIBUTIONS FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM FOR THE ACTUAL NODE LOCATIONS, WHERE NODES ARE INTRODUCED (A) RANDOMLY AND (B) WITH POPULATION TO THE NETWORK. 155
FIGURE 3.50: GIS GENERATED IMAGES OF THE (A) ACTUAL US AIR TRAFFIC NETWORK AND (B) A GENERATED NETWORK (THE BLUE LINE IN FIGURE 3.53(A, B), WHERE THE COLOUR OF THE NODE INDICATES ITS DEGREE (RED TO GREEN, FOR HIGH TO LOW DEGREE). 157
FIGURE 3.51: SHOWING POPULATION DENSITY MAPS FOR (A) CHINA (CHINA TRAVEL GO 2013) AND (B) THE US (MAPSOFUSA.NET 2013). 157

FIGURE 3.52: (A) SIMULATED CLUSTERED NODAL LAYOUT FOR THE US AIR TRAFFIC NETWORK (USATN), WHERE THE BLACK DOTS REPRESENT THE INITIAL NODES, THE GREY DOTS THE ADDED NODES AND THE BLACK LINE THE SPATIAL BOUNDARY OF THE NETWORK. (B) A COMPARISON FOR THE SPATIAL DISTRIBUTION OF NODES FOR THE USATN (BLACK) AND THE CLUSTERED NODAL LAYOUT SHOWN IN (A) (GREY). 158

FIGURE 3.53: SHOWING THE (A) DEGREE DISTRIBUTION AND (B) SPATIAL DEGREE DISTRIBUTION, FOR THE EXPONENTIAL (BLUE, GREEN) AND SCALE-FREE (RED, ORANGE) NETWORKS GENERATED USING THE SYNTHETIC NETWORK GENERATION ALGORITHM, WHERE NODES ARE INTRODUCED RANDOMLY TO THE NETWORK THE CLUSTERED NODAL LAYOUT (FIGURE 3.52)..... 159

FIGURE 3.54: THE HAZARD TOLERANCE OF THE (A, B) CHINA AIR TRAFFIC NETWORK AND (C, D) US AIR TRAFFIC NETWORK AND TWO OF THEIR SYNTHETIC PROXIES TO THE CENTRAL ATTACK SPATIAL HAZARD (FIGURE 3.35). ALSO SHOWING THE HAZARD TOLERANCE OF RANDOM NETWORKS WITH THE SAME NODE LOCATIONS AS THE AIR TRAFFIC NETWORKS (GREY LINE) AND RANDOM NODE LOCATIONS (BLACK LINE). IT IS WORTH NOTING THAT THE RANDOM NETWORKS WITH THE SAME NODAL LOCATIONS AS THE AIR TRAFFIC NETWORKS SHOW THE SAME RESULTS AS THE RANDOM NETWORKS WITH RANDOM NODAL LOCATIONS IN (A) AND (C) AND THEREFORE CANNOT BE DISTINGUISHED IN THE GRAPHS..... 161

FIGURE 3.55: SHOWING THE HAZARD TOLERANCE OF TEN SYNTHETIC NETWORKS FOR THE USATN WITH GENERATED NODAL LOCATIONS (DIFFERENT FOR EACH NETWORK) SUBJECTED TO CENTRAL ATTACK SPATIAL HAZARD, PLOTTING THE RESULTS IN TERMS OF (A) PERCENTAGE NODES REMOVED AND (B) NODES REMOVED WITHIN A SPECIFIED DISTANCE FROM THE GEOGRAPHIC CENTRE OF THE NETWORK. 163

FIGURE 3.56: SHOWING THE PERCENTAGE OF LINKS REMOVED AND THE PERCENTAGE DISTANCE FROM THE GEOGRAPHIC CENTRE (TO THE FURTHEST NODE) FOR THE CENTRAL ATTACK SPATIAL HAZARD (FIGURE 3.35), FOR THE EUROPEAN, CHINA AND US AIR TRAFFIC NETWORKS. THE CORRESPONDING RANDOM NETWORK FOR EACH REAL WORLD AIR TRAFFIC NETWORK HAS ALSO BEEN SHOWN (THIS RANDOM NETWORK HAS THE SAME NODAL LOCATIONS, BUT A DIFFERENT ARRANGEMENT OF LINKS AS THE REAL WORLD NETWORK), ALONG WITH THE RANDOM NETWORK WITH RANDOM NODAL LOCATIONS. NOTE THAT THE RESULTS FOR THE EUROPEAN AIR TRAFFIC NETWORK ARE THE SAME AS THOSE SHOWN IN FIGURE 3.36, BUT WITH A DIFFERENT X-AXIS..... 164

FIGURE 3.57: SHOWING (A, B) THE CHANGE IN MCS AND (C, D) THE CHANGE IN APL FOR THE EUROPEAN, CHINA AND US AIR TRAFFIC NETWORKS WHEN SUBJECTED TO THE CENTRAL ATTACK SPATIAL HAZARD (FIGURE 3.35). THE PERCENTAGE CHANGE IN THE MCS AND APL HAS BEEN PLOTTED AS ALL THREE NETWORKS CONTAIN A DIFFERENT NUMBER OF NODES AND LINKS. A RANDOM NETWORK, WITH RANDOM NODAL LOCATIONS, HAS ALSO BEEN SHOWN AND IS USED AS A BENCHMARK FOR RESILIENCE..... 167

FIGURE 4.1: SHOWING THREE DIFFERENT SPATIAL NODAL LAYOUTS: (A) UNIFORM WITH DISTANCE, (B) UNIFORM WITH AREA, (C) CLUSTERED. IN THE THREE LAYOUTS, THE BLACK DOTS DEPICT THE NODES AND THE OUTER GREY CIRCLE DEFINES THE SPATIAL BOUNDARY OF THE NETWORK. ALSO SHOWING THE ASSOCIATED SPATIAL DISTRIBUTIONS FOR THE THREE NODAL LAYOUTS; (D) UNIFORM WITH DISTANCE, (E) UNIFORM WITH AREA AND (F) CLUSTERED. 173

FIGURE 4.2: THREE, OF TEN, CLUSTERED NODAL LAYOUTS GENERATED USING THE CLUSTERING ALGORITHM (CHAPTER 3.2), FOR USE IN TESTS OF HAZARD TOLERANCE. 174

FIGURE 4.3: SHOWING ALL COMBINATIONS OF NETWORK CLASS (INNER CIRCLE), NODAL LAYOUT (CENTRE CIRCLE) AND NODE INTRODUCTION ORDER (OUTER CIRCLE) USED IN THIS CHAPTER. IN THE PREVIOUS CHAPTER IT WAS ESTABLISHED THAT THE EXPONENTIAL NETWORKS, WHERE THE NODES WERE INTRODUCED RANDOMLY, WITH A CLUSTERED NODAL LAYOUT

was superior at replicating the topological and spatial characteristics of the European, China and US air traffic networks..... 175

Figure 4.4: Showing the average degree distribution for (a) exponential networks and (b) scale-free networks, with a uniform with area nodal layout and three different node introduction orders; (c) the spatial degree distribution for the same exponential networks and (d) for scale-free networks[1]..... 177

Figure 4.5: Three exponential networks with a uniform with area nodal layout, where the nodes are introduced (a) with distance, (b) proportional to distance and (c) randomly. The spatial boundary is shown as a black circle and the nodes are shown as grey-scale dots. The colour of the node indicates its degree, with black nodes having a high degree and light grey nodes a low degree..... 178

Figure 4.6: Showing three sizes of the simulated perimeter attack spatial hazard, in which the centre of the hazard is fixed on the spatial perimeter of the network and grows outwards until the whole network area is covered (i.e. from (a) to (b) to (c)). 179

Figure 4.7: Showing the results of subjecting (a, c) the exponential networks and (b, d) the scale-free networks to the 'central attack' spatial hazard. (a, b) plot the percentage of nodes and links removed, and (c, d) plot the percentage of area and links removed. Each line of results represents an average of 10 networks. It is worth noting that there is only a small scatter in the results for each of the 10 networks. 181

Figure 4.8: Showing the results of subjecting (a, c) the exponential networks and (b, d) the scale-free networks to the 'perimeter attack' spatial hazard. (a, b) plot the percentage of nodes and links removed, and (c, d) plot the percentage of area and links removed. Each line of results represents an average of 10 networks. It is worth noting that there is a small scatter in the results for each of the 10 networks. 183

Figure 4.9: Showing (a) the locations of the five additional spatial hazards (where the black dots are the nodes, the black line the spatial boundary and the grey dot the geographic centre) and (b) plotting the percentage distance of each hazard from the geographic centre of the network (the colour of the dot on the graph is the same as that shown on the network in (a) for the five additional spatial hazards). 186

Figure 4.10: Showing the results for all locations of the spatial hazards, for an average of 10 exponential networks with a uniform with area nodal layout, where nodes are introduced (a, d) with distance, (b, e) proportional with distance and (c, f) randomly. It is worth noting that there is a small scatter in the results for each of the 10 networks. 188

Figure 4.11: Showing the results for all locations of the spatial hazards, for an average of 10 scale-free networks with a uniform with area nodal layout, where nodes are introduced (a, d) with distance, (b, e) proportional with distance and (c, f) randomly. It is worth noting that there is a small scatter in the results for each of the 10 networks. 190

Figure 4.12: Showing the results for all locations of the spatial hazards, for an average of 10 exponential networks with a uniform with distance nodal layout, where nodes are introduced (a, d) with distance, (b, e) proportional with distance and (c, f) randomly. It is worth noting that there is a small scatter in the results for each of the 10 networks..... 197

FIGURE 4.13: SHOWING THE RESULTS FOR ALL LOCATIONS OF THE SPATIAL HAZARDS, FOR AN AVERAGE OF 10 SCALE-FREE NETWORKS WITH A UNIFORM WITH DISTANCE NODAL LAYOUT, WHERE NODES ARE INTRODUCED (A, D) WITH DISTANCE, (B, E) PROPORTIONAL WITH DISTANCE AND (C, F) RANDOMLY. IT IS WORTH NOTING THAT THERE IS A SMALL SCATTER IN THE RESULTS FOR EACH OF THE 10 NETWORKS. 199

FIGURE 4.14: SHOWING THE RESULTS FOR 10 EXPONENTIAL NETWORKS WITH A CLUSTERED LAYOUT, WHERE THE NODES WERE INTRODUCED RANDOMLY SUBJECTED TO THE 'CENTRAL' ATTACK. THESE RESULTS ARE AVERAGED TO PRODUCE THE 0% RESULT LINE IN FIGURE 4.15. THE AMOUNT OF SCATTER IN THE RESULTS IS DUE TO THE POSITIONS OF THE DIFFERENT CLUSTERS OF NODES. 200

FIGURE 4.15: SHOWING THE RESULTS FOR ALL LOCATIONS OF THE SPATIAL HAZARDS, FOR AN AVERAGE OF 10 EXPONENTIAL NETWORKS WITH A CLUSTERED NODAL LAYOUT, WHERE NODES ARE INTRODUCED (A, D) WITH DISTANCE, (B, E) PROPORTIONAL WITH DISTANCE AND (C, F) RANDOMLY. 203

FIGURE 4.16: SHOWING THE RESULTS FOR ALL LOCATIONS OF THE SPATIAL HAZARDS, FOR AN AVERAGE OF 10 SCALE-FREE NETWORKS WITH A CLUSTERED NODAL LAYOUT, WHERE NODES ARE INTRODUCED (A, D) WITH DISTANCE, (B, E) PROPORTIONAL WITH DISTANCE AND (C, F) RANDOMLY. 205

FIGURE 4.17: THREE OF THE SEVEN CLUSTERED LAYOUTS USED TO DEMONSTRATE THE HAZARD TOLERANCE OF GENERATED CLUSTERED NODAL LAYOUTS GENERATED WITH THE SAME SEED LOCATIONS AND RADII, BUT USING DIFFERENT C_D VALUES: (A) $C_D = 50$, (B) $C_D = 200$, (C) $C_D = 350$. 206

FIGURE 4.18: THE (A) DEGREE DISTRIBUTION, (B) SPATIAL DISTRIBUTION AND (C) SPATIAL DEGREE DISTRIBUTION FOR SEVEN RANDOM NETWORKS, WITH DIFFERENT CLUSTERED NODAL LAYOUTS. AS ALL NODES IN A RANDOM NETWORK HAVE APPROXIMATELY THE SAME DEGREE, THE DEGREE DISTRIBUTION (SHOWN IN (A)) HAS NOT BEEN PRESENTED ON A LOG SCALE. 207

FIGURE 4.19: HAZARD TOLERANCE OF SEVEN RANDOM NETWORKS WITH DIFFERENT CLUSTERING LAYOUTS, SHOWING (A, C) TOLERANCE TO CENTRAL ATTACK SPATIAL HAZARD AND (B, D) TOLERANCE TO PERIMETER SPATIAL HAZARD. 208

FIGURE 4.20: SHOWING HOW THE MAXIMUM CLUSTER SIZE (MCS) CHANGES FOR THE RANDOM NETWORKS WHEN SUBJECTED TO (A, C) CENTRAL ATTACK AND (B, D) PERIMETER ATTACK SPATIAL HAZARDS. EACH LINE SHOWN IN THE GRAPHS IS THE AVERAGE OF TEN NETWORKS. 212

FIGURE 4.21: SHOWING HOW THE SHORTEST AVERAGE PATH LENGTH (APL) CHANGES FOR THE RANDOM NETWORKS WHEN SUBJECTED TO (A, C) CENTRAL ATTACK AND (B, D) PERIMETER ATTACK SPATIAL HAZARDS. EACH LINE SHOWN IN THE GRAPHS IS THE AVERAGE OF TEN NETWORKS. 214

FIGURE 4.22: SHOWING HOW MAXIMUM CLUSTER SIZE (MCS) CHANGES WITH NODE REMOVAL FOR SCALE-FREE NETWORKS SUBJECTED TO (A) CENTRAL ATTACK AND (B) PERIMETER ATTACK SPATIAL HAZARDS. EACH LINE OF RESULTS SHOWN IS THE AVERAGE OF TEN NETWORKS. THE NETWORKS WHERE THE NODES ARE INTRODUCED WITH DISTANCE ARE SHOWN IN SHADES OF BLUE, NODES INTRODUCED PROPORTIONAL WITH DISTANCE ARE SHOWN IN SHADES OF GREEN AND NODES INTRODUCED RANDOMLY ARE SHOWN IN SHADES OF RED. THE AVERAGE RESULTS FOR THE RANDOM NETWORKS ARE SHOWN IN SHADES OF GREY. 216

FIGURE 4.23: SHOWING HOW MAXIMUM CLUSTER SIZE (MCS) CHANGES WITH NODE REMOVAL FOR EXPONENTIAL NETWORKS SUBJECTED TO (A) CENTRAL ATTACK AND (B) PERIMETER ATTACK SPATIAL HAZARDS. EACH LINE OF RESULTS SHOWN IS THE AVERAGE OF TEN NETWORKS. THE NETWORKS WHERE THE NODES ARE INTRODUCED WITH DISTANCE ARE SHOWN IN SHADES OF BLUE, NODES INTRODUCED PROPORTIONAL WITH DISTANCE ARE SHOWN IN SHADES OF GREEN

AND NODES INTRODUCED RANDOMLY ARE SHOWN IN SHADES OF RED. THE AVERAGE RESULTS FOR THE RANDOM NETWORKS ARE SHOWN IN SHADES OF GREY..... 217
FIGURE 4.24: SHOWING HOW THE SHORTEST AVERAGE PATH LENGTH (APL) CHANGES WITH NODE REMOVAL FOR SCALE-FREE NETWORKS SUBJECTED TO (A) CENTRAL ATTACK AND (B) PERIMETER ATTACK SPATIAL HAZARDS. EACH LINE OF RESULTS SHOWN IS THE AVERAGE OF TEN NETWORKS. THE NETWORKS WHERE THE NODES ARE INTRODUCED WITH DISTANCE ARE SHOWN IN SHADES OF BLUE, NODES INTRODUCED PROPORTIONAL WITH DISTANCE ARE SHOWN IN SHADES OF GREEN AND NODES INTRODUCED RANDOMLY ARE SHOWN IN SHADES OF RED. THE AVERAGE RESULTS FOR THE RANDOM NETWORKS ARE SHOWN IN SHADES OF GREY..... 219
FIGURE 4.25: SHOWING HOW THE SHORTEST AVERAGE PATH LENGTH (APL) CHANGES WITH NODE REMOVAL FOR EXPONENTIAL NETWORKS SUBJECTED TO (A) CENTRAL ATTACK AND (B) PERIMETER ATTACK SPATIAL HAZARDS. EACH LINE SHOWN IN THE GRAPHS IS THE AVERAGE OF TEN NETWORKS. THE NETWORKS WHERE THE NODES ARE INTRODUCED WITH DISTANCE ARE SHOWN IN SHADES OF BLUE, NODES INTRODUCED PROPORTIONAL WITH DISTANCE ARE SHOWN IN SHADES OF GREEN AND NODES INTRODUCED RANDOMLY ARE SHOWN IN SHADES OF RED. THE AVERAGE RESULTS FOR THE RANDOM NETWORKS ARE SHOWN IN SHADES OF GREY..... 220
FIGURE 4.26: THE DEGREE DISTRIBUTION OF SIX NETWORKS GENERATED WITH DIFFERENT NEIGHBOURHOOD VALUES. 221
FIGURE 4.27: SHOWING HOW THE SHORTEST AVERAGE PATH LENGTH (APL) CHANGES FOR SIX EXPONENTIAL NETWORKS, WITH A UNIFORM WITH AREA NODAL CONFIGURATION, WHEN SUBJECTED TO THE PERIMETER ATTACK SPATIAL HAZARD. THESE NETWORKS WERE ALL GENERATED WITH A DIFFERENT NEIGHBOURHOOD SIZE (R) WHICH IS SHOWN IN THE KEY AND THE NODES IN ALL SIX NETWORKS WERE INTRODUCED IN ORDER OF DISTANCE FROM THE GEOGRAPHIC CENTRE. 223
FIGURE 4.28: SHOWING HOW MAXIMUM CLUSTER SIZE (MCS) CHANGES WITH AREA REMOVAL FOR SCALE-FREE NETWORKS SUBJECTED TO (A) CENTRAL ATTACK AND (B) PERIMETER ATTACK SPATIAL HAZARDS. EACH LINE OF RESULTS SHOWN IS THE AVERAGE OF TEN NETWORKS. THE NETWORKS WHERE THE NODES ARE INTRODUCED WITH DISTANCE ARE SHOWN IN SHADES OF BLUE, NODES INTRODUCED PROPORTIONAL WITH DISTANCE ARE SHOWN IN SHADES OF GREEN AND NODES INTRODUCED RANDOMLY ARE SHOWN IN SHADES OF RED. THE AVERAGE RESULTS FOR THE RANDOM NETWORKS ARE SHOWN IN SHADES OF GREY. 227
FIGURE 4.29: SHOWING HOW MAXIMUM CLUSTER SIZE (MCS) CHANGES WITH AREA REMOVAL FOR EXPONENTIAL NETWORKS SUBJECTED TO (A) CENTRAL ATTACK AND (B) PERIMETER ATTACK SPATIAL HAZARDS. EACH LINE OF RESULTS SHOWN IS THE AVERAGE OF TEN NETWORKS. THE NETWORKS WHERE THE NODES ARE INTRODUCED WITH DISTANCE ARE SHOWN IN SHADES OF BLUE, NODES INTRODUCED PROPORTIONAL WITH DISTANCE ARE SHOWN IN SHADES OF GREEN AND NODES INTRODUCED RANDOMLY ARE SHOWN IN SHADES OF RED. THE AVERAGE RESULTS FOR THE RANDOM NETWORKS ARE SHOWN IN SHADES OF GREY. 228
FIGURE 4.30: SHOWING HOW THE AVERAGE PATH LENGTH (APL) CHANGES WITH AREA REMOVAL FOR SCALE-FREE NETWORKS SUBJECTED TO (A) CENTRAL ATTACK AND (B) PERIMETER ATTACK SPATIAL HAZARDS. EACH LINE OF RESULTS SHOWN IS THE AVERAGE OF TEN NETWORKS. THE NETWORKS WHERE THE NODES ARE INTRODUCED WITH DISTANCE ARE SHOWN IN SHADES OF BLUE, NODES INTRODUCED PROPORTIONAL WITH DISTANCE ARE SHOWN IN SHADES OF GREEN AND NODES INTRODUCED RANDOMLY ARE SHOWN IN SHADES OF RED. THE AVERAGE RESULTS FOR THE RANDOM NETWORKS ARE SHOWN IN SHADES OF GREY. 230
FIGURE 4.31: SHOWING HOW THE SHORTEST AVERAGE PATH LENGTH (APL) CHANGES WITH AREA REMOVAL FOR EXPONENTIAL NETWORKS SUBJECTED TO (A) CENTRAL ATTACK AND (B) PERIMETER ATTACK SPATIAL HAZARDS. EACH LINE OF RESULTS SHOWN IS THE AVERAGE OF TEN NETWORKS. THE NETWORKS WHERE THE NODES ARE INTRODUCED WITH

DISTANCE ARE SHOWN IN SHADES OF BLUE, NODES INTRODUCED PROPORTIONAL WITH DISTANCE ARE SHOWN IN SHADES OF GREEN AND NODES INTRODUCED RANDOMLY ARE SHOWN IN SHADES OF RED. THE AVERAGE RESULTS FOR THE RANDOM NETWORKS ARE SHOWN IN SHADES OF GREY..... 231

FIGURE 4.32: SHOWING THE STRATEGY USED TO REWIRE LINKS (AIR ROUTES) IN THE EVENT OF A SPATIAL HAZARD. IN ALL PARTS OF THE FIGURE A SECTION OF THE EATN IS SHOWN AND THE NODES ARE INDICATED BY DOTS AND THE LINKS BY THE CONNECTING LINES (SOLID LINES INDICATE A LINK BETWEEN TWO SHOWN NODES AND A DOTTED LINE BETWEEN TWO NODES WHERE ONE HAS BEEN OMITTED FOR CLARITY). IN (A) IT CAN BE SEEN THAT TWO AIRPORTS (RED DOTS) HAVE BEEN ENVELOPED BY A SPATIAL HAZARD (RED CIRCLE). THE ORANGE AIR ROUTE IS FAILED (AS BOTH ORIGIN AND DESTINATION AIRPORTS ARE ENVELOPED BY THE SPATIAL HAZARD) AND THE BLUE AIR ROUTES ARE 'REWIRED' TO THE CLOSEST AIRPORT AND ANY PARALLEL EDGES ARE REMOVED, THE RESULT OF THIS CAN BE SEEN IN (B). THE SAME STARTING NETWORK IS SHOWN IN (C) AND IS REWIRED IN (D) USING THE SAME 'RULES', BUT IN THIS CASE PARALLEL EDGES ARE ALLOWED TO FORM..... 239

FIGURE 4.33: THE RESULTS OF THE 'ADAPTIVE' REWIRING STRATEGY FOR THE EATN SUBJECTED TO THE CENTRAL ATTACK SPATIAL HAZARD. THE HAZARD TOLERANCE OF THE EATN WITH NO REWIRING (WHERE LINKS ARE REMOVED IF ONE (OR BOTH) OF THEIR CONNECTING AIRPORTS ARE ENVELOPED BY THE HAZARD) (BLUE LINE) IS COMPARED TO THE EATN WHEN THE LINKS HAVE BEEN REWIRED AND PARALLEL EDGES REMOVED (RED LINE) AND NOT REMOVED (GREEN LINE). THE RANDOM BENCHMARK NETWORK, WITH RANDOM NODAL LOCATIONS, AND THREE RANDOM NETWORKS WITH THE SAME NODAL CONFIGURATION AS THE EATN HAVE ALSO BEEN SHOWN (DOTTED LINES). 241

FIGURE 4.34: OBSERVING THE CHANGES IN (A, B) AVERAGE DEGREE OF THE REMAINING NODES FOR THE EATN AND TWO ADAPTIVELY REWIRED NETWORKS (ONE WITH PARALLEL EDGES, ONE WITHOUT) AND (C, D) MAXIMUM DEGREE FOR THE SAME THREE NETWORKS. THE RESULTS IN (A, C) HAVE BEEN PLOTTED WITH RESPECT TO THE PROPORTION OF NODES REMOVED AND IN (B, D) WITH RESPECT TO THE PROPORTION OF AREA REMOVED..... 242

FIGURE 4.35: OBSERVING THE CHANGES IN THE NUMBER OF LINKS REWIRED IN THE EATN FOR THE REWIRED NETWORKS WITH PARALLEL EDGES (GREEN LINE) AND WITHOUT PARALLEL EDGES REMOVED (RED LINE). THE RESULTS IN (A) ARE PLOTTED WITH RESPECT TO THE PROPORTION OF NODES REMOVED AND IN (B) WITH RESPECT TO THE PROPORTION OF AREA REMOVED..... 244

FIGURE 4.36: SHOWING THE CHANGES IN (A, B) MAXIMUM CLUSTER SIZE AND (C, D) AVERAGE PATH LENGTH FOR THE EATN, TWO REWIRED NETWORKS AND A RANDOM NETWORK SUBJECTED TO THE CENTRAL ATTACK SPATIAL HAZARD. THE RESULTS IN (A, C) ARE PLOTTED WITH RESPECT TO THE PROPORTION OF NODES REMOVED AND IN (B, D) WITH RESPECT TO THE NETWORK AREA REMOVED BY THE SPATIAL HAZARD. IT APPEARS THAT THE RESULTS FOR THE REWIRED EATN WITH NO PARALLEL EDGES (RED LINE) IS MISSING FROM THIS FIGURE, HOWEVER, IT HAS THE SAME RESULTS AS THE REWIRED EATN WITH PARALLEL EDGES (GREEN) AND APPEARS UNDER THIS LINE..... 245

FIGURE 4.37: THE (A) DEGREE DISTRIBUTION AND (B) SPATIAL DEGREE DISTRIBUTION FOR THE EATN AND FOUR NETWORKS GENERATED USING THE SAME ALGORITHM AS THE EATN BUT WITH A LIMITED MAXIMUM DEGREE (OF EITHER: 100, 75, 50 OR 20 CONNECTIONS). 247

FIGURE 4.38: SHOWING (A) THE RELATIONSHIP BETWEEN THE PROPORTION OF NODES AND LINKS REMOVED FOR THE EATN AND FOUR NETWORKS, SUBJECTED TO THE CENTRAL ATTACK SPATIAL HAZARD, WHERE THE MAXIMUM PERMITTED DEGREE DOES NOT EXCEED 100, 75, 50 OR 20. (B) PLOTTING THE SAME RESULTS, BUT WITH RESPECT TO THE PROPORTION OF AREA COVERED BY THE SPATIAL HAZARD. ALSO SHOWING THE RESULTS OF THE BENCHMARK RANDOM

network, with random nodal locations, and the random network with the same nodal configuration as the EATN (dotted lines)..... 248
Figure 4.39: Generated GIS images showing the degree of all nodes in the generated networks with a limit of (a) 50 and (b) 100, on a red (high degree) to green (low degree) scale. The location of the nodes with the maximum value of degree (red dots) is also shown for a limit of (c) 50 and (d) 100..... 250
Figure 4.40: Showing the changes in (a, d) the number of isolated nodes, (b, e) the maximum cluster size (MCS) and (c, f) the maximum degree for the EATN and four networks where the maximum degree has been limited, when the networks are subject to the central attack spatial hazard. Also showing the results of the benchmark random network, with random nodal locations (dotted lines). 252
Figure 4.41: Generated GIS images showing the location of the isolated nodes (red) and the connected airports (green) for the size of spatial hazard which results in the maximum value of isolated nodes, for the network with a maximum degree of (a) 50 and (b) 100..... 254
Figure 4.42: Showing the change average path length (APL) for the EATN and four networks where the maximum degree has been limited (as indicated), subjected to the central attack spatial hazard. The results in (a) have been plotted with respect to the proportion of nodes removed from the network and with respect to the size of the spatial hazard in (b). Also showing the results of the benchmark random network, with random nodal locations (dotted lines). 255
Figure 4.43: The results of the modified 'adaptive' rewiring strategy for the EATN subjected to the central attack spatial hazard. In this modified strategy the capacity of the nodes (when receiving additional links) has been limited, by an percentage of their original degree. Showing (a) the results in terms of the proportion of nodes and links removed and in (b) in terms of the proportion of area and links removed. Also showing the benchmark random network (with a random nodal layout) subjected to the same hazard, with no additional capacity (black dotted line)..... 257
Figure 4.44: Observing the changes in the average degree of the remaining nodes for the EATN and seven adaptively rewired networks (with different nodal capacities). The results in (a) have been plotted with respect to the proportion of nodes removed and in (b) with respect to the proportion of area removed. 259
Figure 4.45: Observing the changes in the maximum degree of the remaining nodes for the EATN and seven adaptively rewired networks (with different nodal capacities). The results in (a) have been plotted with respect to the proportion of nodes removed and in (b) with respect to the proportion of area removed. 260
Figure 4.46: Showing the changes in the maximum cluster size (MCS) for the EATN and seven adaptively rewired networks (with different nodal capacities), subjected to the central attack spatial hazard. The results in (a) have been plotted with respect to the proportion of nodes removed from the network and with respect to the size of the spatial hazard in (b). 261
Figure 4.47: Showing the changes in the shortest average path length (APL) for the EATN and seven adaptively rewired networks (with different nodal capacities), subjected to the central attack spatial hazard. The results in (a) have been plotted with respect to the proportion of nodes removed from the network and with respect to the size of the spatial hazard in (b)..... 262

FIGURE 4.48: THE RESULTS OF THE MODIFIED 'ADAPTIVE' REWIRING STRATEGY FOR THE EATN SUBJECTED TO THE PERIMETER ATTACK SPATIAL HAZARD. IN THIS MODIFIED STRATEGY THE CAPACITY OF THE NODES (WHEN RECEIVING ADDITIONAL LINKS) HAS BEEN LIMITED. SHOWING (A) THE RESULTS IN TERMS OF THE PROPORTION OF NODES AND LINKS REMOVED AND IN (B) IN TERMS OF THE PROPORTION OF AREA AND LINKS REMOVED. ALSO SHOWING THE BENCHMARK RANDOM NETWORK (WITH A RANDOM NODAL LAYOUT) SUBJECTED TO THE SAME HAZARD, WITH NO ADDITIONAL CAPACITY (BLACK DOTTED LINE). 264

FIGURE 4.49: SHOWING THE CHANGES IN THE MAXIMUM CLUSTER SIZE (MCS) FOR THE EATN AND SEVEN ADAPTIVELY REWIRED NETWORKS (WITH DIFFERENT NODAL CAPACITIES), SUBJECTED TO THE PERIMETER ATTACK SPATIAL HAZARD. THE RESULTS IN (A) HAVE BEEN PLOTTED WITH RESPECT TO THE PROPORTION OF NODES REMOVED FROM THE NETWORK AND WITH RESPECT TO THE SIZE OF THE SPATIAL HAZARD IN (B). 266

FIGURE 4.50: SHOWING THE CHANGES IN THE AVERAGE PATH LENGTH (APL) OF THE EATN AND SEVEN ADAPTIVELY REWIRED NETWORKS (WITH DIFFERENT NODAL CAPACITIES), SUBJECTED TO THE PERIMETER ATTACK SPATIAL HAZARD. THE RESULTS IN (A) HAVE BEEN PLOTTED WITH RESPECT TO THE PROPORTION OF NODES REMOVED FROM THE NETWORK AND WITH RESPECT TO THE SIZE OF THE SPATIAL HAZARD IN (B). 267

FIGURE 5.1: AN EXAMPLE NETWORK CONSISTING OF THREE NODES AND THREE LINKS, WHERE NODE 1 IS THE SUPPLY NODE AND NODES 2 AND 3 ARE THE DEMAND NODES (NODE NUMBERS ARE INDICATED BY THE BOLD NUMBERS TO THE LEFT OF EACH NODE); Q = FLOW OF SERVICE THAT THE NODE EITHER DEMANDS OR SUPPLIES; PE = POTENTIAL ENERGY OF NODE; R = RESISTANCE OF LINK (SUBSCRIPT VALUES INDICATE NODE/LINK TO WHICH THEY REFER). 272

FIGURE 5.2: SHOWING THE CORRELATION BETWEEN AVERAGE FLOW AND SHORTEST AVERAGE PATH LENGTH FOR 20 (A) SCALE-FREE, (B) EXPONENTIAL AND (C) RANDOM NETWORKS, EACH WITH 1000 NODES AND DIFFERENT NUMBER OF LINKS 277

FIGURE 5.3: CORRELATION BETWEEN BETWEENNESS CENTRALITY AND FLOW AT THE CORRESPONDING NODE FOR (A) SCALE-FREE, (B) EXPONENTIAL AND (C) RANDOM NETWORKS WITH 1000 NODES AND AROUND 5000 LINKS. THE R^2 VALUE IS GENERATED USING A BEST FIT LINEAR LINE FOR ALL NETWORKS (AS THIS IS THE LINE OF BEST FIT). 279

FIGURE 5.4: SHOWING A SAMPLE SECTION OF A NETWORK, INDICATING A SUPPLY NODE (IN RED) AND THREE DEMAND NODES (IN BLACK). THE TOP NUMBER (BLACK) INDICATES THE FLOW THROUGH THE NODE AND THE BOTTOM NUMBER (RED) IS THE AMOUNT OF SERVICE PROVISION REQUIRED BY THAT NODE (ALSO EQUAL TO ITS DEGREE). THE DOTTED LINES INDICATE CONNECTIONS TO OTHER NODES IN THE NETWORK, WHICH HAVE NOT BEEN INCLUDED FOR SIMPLICITY. THE FLOWS SHOWN ASSUME THAT THE OTHER NODES IN THE NETWORK DO NOT REQUIRE A PROPORTION OF THE FLOW; THIS IS ASSUMED IN THIS EXAMPLE FOR SIMPLICITY ONLY AND IS NOT AN ASSUMPTION OF THE FLOW MODEL ITSELF. 281

FIGURE 5.5: CORRELATION BETWEEN CLOSENESS CENTRALITY AND FLOW AT THE CORRESPONDING NODE FOR (A) SCALE-FREE, (B) EXPONENTIAL AND (C) RANDOM NETWORKS WITH 1000 NODES AND AROUND 5000 LINKS. THE R^2 VALUE IS GENERATED USING A BEST FIT LINEAR LINE FOR THE SCALE-FREE AND RANDOM NETWORKS, AND A LOGARITHMIC LINE FOR THE EXPONENTIAL NETWORKS. 282

FIGURE 5.6: CORRELATION BETWEEN DEGREE CENTRALITY AND FLOW AT THE CORRESPONDING NODE FOR (A)SCALE-FREE, (B) EXPONENTIAL AND (C) RANDOM NETWORKS WITH 1000 NODES AND AROUND 5000 LINKS. THE R^2 VALUE IS GENERATED USING A BEST FIT LINEAR LINE FOR THE SCALE-FREE AND RANDOM NETWORKS AND A POWER-LAW FOR THE EXPONENTIAL NETWORKS. 284

FIGURE 5.7: SHOWING (A) 15 NODE SAMPLE NETWORK (INDICATING NODE NUMBERS), (B) A COMPARISON OF R^2 VALUE FOR MEASURES FOR EACH POSITION OF THE SUPPLY NODE (WHERE D = DEGREE, OF = ORIGINAL FLOW, BC = BETWEENNESS CENTRALITY AND CM THE COMBINED MEASURE). 288

FIGURE 5.8: SHOWING (A) ORIGINAL FLOW AND CHANGE IN FLOW (CALCULATED USING SRSS METHOD) WITH NODE 15 AS THE SUPPLY NODE, FOR THE SAMPLE NETWORK SHOWN IN FIGURE 5.7, AND (B) ONE COMBINED MEASURE AND THE CHANGE IN FLOW (CALCULATED USING THE SRSS METHOD) WITH NODE 15 AS THE SUPPLY NODE, THE RED LINE IS THE LINEAR LINE OF BEST FIT FOR ALL DATA POINTS, AND THE BLACK LINE IS THE LINE OF BEST FIT FOR ALL DATA POINTS WITH THE OUTLIER REMOVED (CIRCLED IN RED). 289

LIST OF TABLES

TABLE 2.1: CRITICALITY SCALE FOR NATIONAL UK INFRASTRUCTURE (CABINET OFFICE 2010A)..... 20

TABLE 2.2: A SUMMARY OF THE DEFINITIONS OF THE FOUR COMPONENTS OF RESILIENCE, AS GIVEN BY CABINET OFFICE (2011B)..... 23

TABLE 2.3: THE FOUR DIMENSIONS OF RESILIENCE, ACCORDING TO O'ROURKE (2007)..... 26

TABLE 2.4: A SELECTION OF REASONABLE WORST CASE SCENARIOS FOR NATURAL HAZARDS IN THE UK, AS OUTLINED IN THE REPORT '*KEEPING THE COUNTRY RUNNING NATURAL HAZARDS AND INFRASTRUCTURE*' (CABINET OFFICE 2011B).... 34

TABLE 2.5: SHOWING THE CONCEPTUAL COMPONENTS OF FOUR DIFFERENT NETWORK MODELS. 47

TABLE 2.6: AN EXAMPLE NETWORK SHOWING HOW THE NUMBER OF LINKS, MAXIMUM CLUSTER SIZE (MCS), NUMBER OF CLUSTERS (NC) AND NUMBER OF ISOLATED NODES (NIN) CHANGES WHEN NODES ARE REMOVED FROM THE NETWORK. THIS WORK HAS BEEN MODIFIED FROM A SIMILAR EXAMPLE BY NOJIMA (2006) AND EDITED FOR CLARITY..... 62

TABLE 2.7: ONE EXAMPLE NETWORK SHOWING HOW THE NUMBER OF LINKS, AVERAGE PATH LENGTH (APL) AND DIAMETER (D) CHANGES WHEN NODES ARE REMOVED FROM THE NETWORK. 64

TABLE 2.8: THE METRICS USED BY YAZDAINI AND JEFFREY (2011) TO QUANTIFY DIFFERENT CHARACTERISTICS OF WATER DISTRIBUTION SYSTEMS..... 87

TABLE 3.1: CALCULATION OF THE NEAREST NEIGHBOUR DISTANCE..... 117

TABLE 3.2: SHOWING THE NEAREST NEIGHBOUR INDEX VALUES FOR THE ACTUAL AND PROXY WAL-MART AND TARGET DATASETS..... 124

TABLE 3.3: SHOWING THE RELEVANT FIGURES FOR THE DEGREE AND SPATIAL DEGREE DISTRIBUTIONS FOR THE GENERATED NETWORKS..... 130

TABLE 4.1: SHOWING THE APL OF THE SIX NETWORKS GENERATED WITH DIFFERENT NEIGHBOURHOOD VALUES UNDER NORMAL OPERATIONAL CONDITIONS..... 224

TABLE 4.2: THE PROPORTION OF CANCELLED AIR ROUTES FOR THE CLOSURE OF 60% OF AIRPORTS FOR SEVEN ADAPTIVELY REWIRED NETWORKS WITH DIFFERENT ADDITIONAL AIRPORT CAPACITIES..... 265

CHAPTER 1: INTRODUCTION

1.1: IDENTIFICATION OF RESEARCH GAP

Infrastructure systems, such as water, transport, communication and energy networks form the backbone of our modern communities (Institution of Civil Engineers 2009) and are crucial to the functioning of our modern society (Murray and Grubesic 2007). The reliability and integrity of these physical assets and the services they provide are vital for ensuring national security, public health and productivity (HM Treasury and Infrastructure UK 2010).

Recent natural disasters, including the earthquakes in New Zealand and Japan (2011), floods in Cumbria (2009) and the eruption of the Eyjafjallajökull volcano (2010), have highlighted not only the importance of these infrastructure systems to modern daily life but also the disproportionate effect that damage to these systems has on our communities; especially for the most vulnerable members of society, including: women and children, the aged, the infirm and the poor. The severity and lasting impact of these effects are often linked to the resilience of the infrastructure systems themselves. For example, even prior to the 2010 earthquake, the infrastructure in Haiti could be classed as among the world's worst. The resulting damage from the earthquake to the communication, transportation and electrical systems, hampered rescue and aid efforts and lead to many long term problems, including lack of sanitisation and spread of disease (Figure 1.1).

Figure 1.1: (a) (WLRN 2010) and (b) (The Telegraph 2010) showing the devastation in the aftermath of the Mw7.0 Haitian Earthquake in 2010.

However, even in more developed countries the failure to understand these complex interacting systems can lead to great suffering; for example, in the aftermath of hurricane Katrina two dozen hospitals were left without electricity, meaning that they could not operate laboratory and x-ray equipment, dialysis machines and ventilators, resulting in many potentially preventable deaths (Gray and Herbert 2006). The effects of a natural disaster are also felt economically and this economic disruption can linger for a significant period of time after the event. The estimated damage of the 2011 Tohoku earthquake and tsunami (Japan) is around $185-$309 billion (Censky 2011) and is likely to take five, or more, years to rebuild (Amandeo 2011). This estimated cost does not include the effects of power outages, caused by the nuclear crisis at the Fukushima power plant, or the subsequent loss of revenue to businesses.

It is not only large scale disasters which cause devastating impacts to our communities, the failure of a single system component coupled with the inability to understand the functioning of the system can also have devastating consequences. For example, in August 2003 North America suffered a blackout affecting 2 million people in 8 US States, with estimated economic losses between $7 and $10 billion (US dollars) (Figure 1.2) (U.S.-Canada Power System Outage Task Force 2004). This failure was caused by the loss of one power station and the failure to manage tree growth around transmission lines; ultimately it was the inability of operators to understand the vulnerability of the system which was attributed to the blackout (U.S.-Canada Power System Outage Task Force 2004).

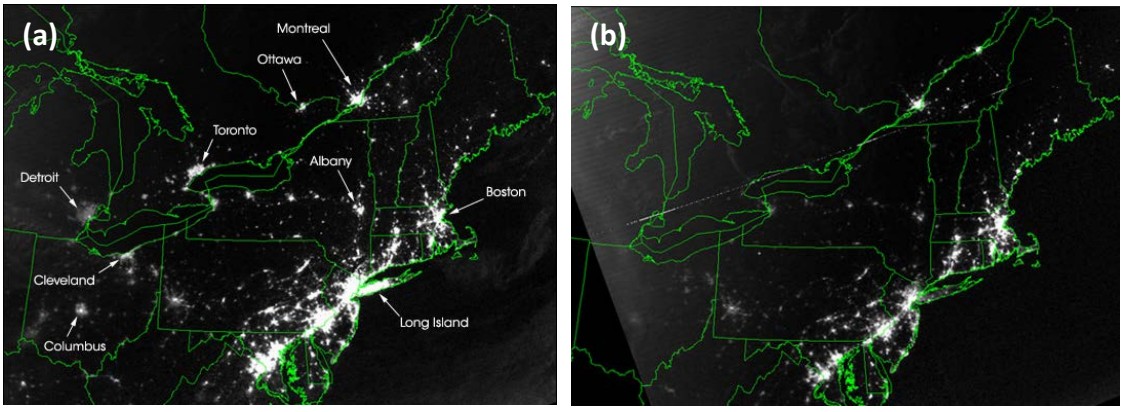


Figure 1.2: The North American Power Grid (a) before and (b) after a cascading failure, affecting 45 million people in 8 US States in August 2003 (Elvidge 2003).

Within the UK the recent floods in the summer of 2007 showed the geographically widespread nature of many natural hazards, with surface water flooding affecting many towns, villages and individual properties from Bristol to Newcastle. This event also caused damage to a number of infrastructure systems, including the closure of electricity substations (including the closure of the Castle Meads substation which left 42,000 people without power for up to 24 hours, Cabinet Office 2008c) and water treatment works (including the closure of the Mythe water treatment works causing 350,000 people to be without access to mains water supply for 17 days, OFWAT 2007) due to flooding. It was estimated that the insurance industry expected to pay out over £3 billion and economic losses to infrastructure systems was estimated at £674 million, with the water sector the worst affected (Environment Agency 2010a).

These recent events have prompted many organisations, such as the Council for Science and Technology and the Institution of Civil Engineers, to question the resilience of our infrastructure systems. In many cases, this resilience could be considered a 'by product' of Government economic investment in infrastructure, with the main priority being on the stimulation of economic growth. '*Over the centuries, the UK has had a great record of investing in world class infrastructure to underpin economic growth*' (HM Treasury and Infrastructure UK 2010); however, in recent decades the approach to infrastructure investment has changed to become uncoordinated and insufficiently targeted to support sustainable development and economic growth. This uncoordinated approach has also had a detrimental impact to the resilience of these systems, caused, in part, by a combination of aging infrastructure components and a change in the connectivity of these systems. These systems are now increasingly underpinned and operated by ICT, which has caused a shift '*from a series of unconnected structures to interconnected systems, where the failure in one part has a direct and damaging knock-on effect in others*' (Council for Science and Technology 2009).

In their 2009 report, the Institution of Civil Engineers called for a greater understanding of the threats and challenges facing our infrastructure systems; which was echoed in the 2009 report by the Council for Science and Technology who also called for '*a better understanding of the complexity and resilience of the national infrastructure*' (Council for Science and Technology 2009). They suggested that this

may be achieved through research into the modelling of infrastructure systems, from physical, economic and social perspectives. These reports, combined with the devastation caused by the 2007 UK floods, prompted the UK Government to produce the 'National Infrastructure Plan 2010' which set out the '*specific steps the Government is taking to achieve its ambition to give the UK world-leading infrastructure*' (HM Treasury and Infrastructure UK 2010) and also the founding of 'Infrastructure UK', a division of HM Treasury focused on '*coordinating the planning, prioritisation and enabling of UK infrastructure investment*' (National Audit Office 2013). Whilst, the main focus of Government investment is still within the economy, the resilience of infrastructure is receiving more attention. Further studies and reports have been commissioned, by the UK Government, including the 'Strategic Framework and Policy Statement' which sets out a process and timescale for the delivery of a Critical Infrastructure Resilience Programme (Cabinet Office 2010a). However, despite this resurgence in funding for infrastructure projects, the capacity, condition, performance and resilience of these systems is still a major concern and also forms the focus of a new study by the Institution of Civil Engineers, in the 2014 State of the Nation report, which aims to '*set out a series of recommendations to improve performance and help remove barriers*' (New Civil Engineer 2013) to deliver a higher quality infrastructure.

This attention to infrastructure resilience has also prompted studies by academic researchers, who aim to develop a deeper understanding of these systems. These studies include the Infrastructure Research Transitions Consortium (which aims to deliver research, models and decision support tools to enable analysis and planning of a robust national infrastructure system) and iSMART (which is developing assessment and adaptation strategies to ensure the future safety and resilience of geotechnical transport infrastructure). This research project also considers the resilience of infrastructure systems and aims to increase the resilience of our communities by developing methods to adapt our critical infrastructure systems so they are less vulnerable to the effects of natural hazards.

The design approach for these complex infrastructure systems is to ensure that the individual components (e.g. buildings, pipes, pumps) have sufficient robustness (i.e. a particular probability of failure) to withstand the impact of catastrophic events, such as

earthquakes and hurricanes, which is specified in the relevant design standard (e.g. Eurocodes). This robustness is usually a balance between the risk and consequences of failure (including loss of life, social and economic impacts) and the economic cost of construction. Whereas this design approach is satisfactory for a building that has a static function (e.g. to provide shelter) it can be found lacking when used to design complex interacting systems. In the event of a major disaster it is likely that some system components will have failed, but what is important is that the system as a whole is still capable of providing a baseline level of service to our communities. Therefore, it is important to ensure that the system itself is designed to have sufficient robustness to withstand the impact of a catastrophic event.

Traditionally, engineers have modelled infrastructure networks using physically-based models in an attempt to understand these systems. Depending on the sophistication of the model the outputs can be very useful in providing scenario based information; however, this modelling approach can be deficient in two ways. Firstly, the size of the problem can quickly become too large to be solved and secondly, this approach only allows a select number of scenarios to be analysed. Therefore, this approach can leave these systems and, more importantly, the communities they support vulnerable to untested events.

To solve this problem recent studies have employed network graph theory to try and understand the behaviour of these complex interacting systems and give an insight into their inherent hazard tolerance. This theory was developed to model the relationships between individuals in a social network and has also previously been applied to model the complex interactions in biological and neural networks. In this approach only the topology of the network is considered, which is modelled as a series of nodes and connecting links. Recent studies have used this approach to model infrastructure systems, representing individual components (including power stations, reservoirs and water treatment plants) as nodes and the interactions between these components (e.g. transmission lines, pipes) as links. This analysis approach reduces the computational effort required to model large infrastructure systems and also enables the fundamental properties of the system to be described. These studies have shown that potentially many infrastructure systems naturally configure to one of two specific network architectures (classes) and therefore potentially have similar

properties. That many infrastructure systems form similar underlying network architectures may seem surprising as a power grid seems vastly different to an air traffic network, but in fact they share many similar characteristics. Both of these networks can be categorised as 'exponential networks', whilst other infrastructure networks have been shown to belong to the 'scale-free' network class. These classes of network are subtly different, but both comprise a small number of highly connected components and a large number of weakly connected components. Classifying a network not only allows the underlying network architecture to be described, but also enables an insight into the hazard tolerance of the system. For example, the World-Wide-Web and the Internet have been shown to belong to the 'scale-free' network class and therefore have been shown to be resilient to random failures and vulnerable to targeted attack (e.g. a terrorist attack) (Albert et al. 2000). This is because a random hazard has a small chance of removing one of the few the highly connected (and important) nodes, whereas a targeted attack will often remove these connected nodes seeking to cause maximum disruption to the functioning of the network.

However, this hazard tolerance assessment is based purely on topological models and does not account for spatial hazards, which are those most likely to disrupt infrastructure systems (e.g. flooding, hurricanes). For the majority of previously analysed infrastructure systems space has little effect on the physical configuration of the network; for example, the physical routers and servers, which comprise the Internet, each require only a room, or even a small space within a room. Even the largest hubs require little physical space and little or no planning permission. The World-Wide-Web requires even less space. Web pages and the hyperlinks that connect them are virtual entities whose physical size amounts to only a few nanometres on a hard disc drive. However, other infrastructure systems, such as electrical transmission systems or transportation networks, require large amounts of space and are usually subject to strict planning regulations. A small number of studies have considered the spatial configuration of these infrastructure systems, but these studies have not assessed the hazard tolerance of these systems to determine their resilience to spatial hazards.

1.2: AIM OF RESEARCH

The aim this project is to improve the resilience of our communities by developing techniques that can identify fragile system architectures, recognize vulnerable areas within these systems and establish methods that can help to protect them from hazard. The project will use a network graph theory approach to analyse infrastructure systems and quantify the impact that damage to these systems can have.

1.3: OBJECTIVES FOR THE RESEARCH

This PhD project will be delivered through the completion of five objectives and will answer six research questions:

1. **Review existing network analysis / reliability / damage models that have been used to analyse infrastructure systems**

   Method: This objective focuses on a review of current literature to identify models used to analyse infrastructure systems, including physically-based models (modelling the flow of services in the systems) and hazard/damage models (simulating disaster scenarios). This objective will also review the literature regarding the more recent analysis of infrastructure systems using the application of network graph theory.

   Output: A literature review detailing the traditional and new methods / models used to analyse infrastructure systems.

   Research Questions:

   i. What are the potential threats to the infrastructure systems?

   ii. What classifies a network as resilient or vulnerable to a hazard scenario?

2. **Collection of real world infrastructure data set(s), which will be catalogued into classes to enable their underlying properties to be described and synthetic analogies for these real world system(s) to be formed**

Method: It has already been discussed that many real world networks potentially form specific network architectures (i.e. classes of network). Understanding the rules that result in these network classes facilitates the ability to generate synthetic networks that can be used as proxies for real world infrastructure systems. These artificial networks display all the characteristics of their real world counterparts and so can be used to generate results for a wider range of systems (e.g. different size systems, generic systems that there is no obtainable data for, future systems that do not yet exist, and whole infrastructure groups) compared to using data for a relatively small number of real world systems. These synthetic networks can also be used to determine if a hazard tolerance displayed by a real world network is unique to that system, or is characteristic of its network class. One suitable real world example will be identified and data regarding this system will be obtained and used as a basis for forming the synthetic networks. Data regarding the spatial location of components in the real world network will also be gathered and replicated in the synthetic networks.

For many infrastructure networks it is their ability to transfer service around the network that is considered to be important. Therefore, to enable the flow of service around infrastructure networks to be analysed, this objective will also employ a simple physically-based flow model to simulate the physical processes in infrastructure systems, which govern the flow of service around the systems.

Output: Generation of synthetic networks that can serve as proxies for real-world infrastructure systems, accounting for both the network architecture (class) of the system and its spatial locations and also the development of a flow model.

Research Questions:

iii. How does the inclusion of a spatial component affect the algorithm used to generate the synthetic networks, if at all?

3. **Simulation of 'disasters' to the real and synthetic infrastructure systems (enabling the quantification of resilience)**

   Method: To quantify the inherent resilience of each class of network (and to identify fragile network architectures) to different types of disasters, hazard and damage models will be developed and applied to the real and synthetic infrastructure systems. The deterioration of the systems will be monitored using network theory measures and the resilience of the network quantified using these measures. To enable the identification of specific nodes and/or links that cause a disproportionate effect when removed from the system, the network models will be combined with the reduced complexity flow model (developed in Objective 2) and physically-based measures will be compared with measures from graph theory. The comparison between these two sets of measures should establish vulnerability markers (defined as nodes and/or links that when removed from the network have the greatest impact, e.g. those nodes whose removal causes the most disruption to the flow of service).

   Output: Quantification of the resilience of the synthetic and real infrastructure systems and the identification of fragile network architectures and specific vulnerable nodes and/or links in these systems.

   Research Questions:

   iv. Does the inclusion of a spatial component into the analysis alter the hazard tolerance of the network class, compared to using a purely topological model?

4. **Evaluate methods to reduce the vulnerability of networks to disasters**

   Method: Quantifying the resilience of the real and synthetic infrastructure networks (Objective 3) will identify the inherent tolerance to hazard to each type of disaster considered (e.g. random hazard, spatial hazard and targeted attack). To identify the reasoning behind any vulnerability displayed by these networks, a range of synthetic networks with inherently robust network

architectures (to different hazards) and different spatial locations of components will be formed. These networks will be subjected to the same hazards and their resilience quantified using the same network measures as previously used. Comparison between this range of synthetic networks and those analysed in Objective 3 should explain the reason for any vulnerabilities shown. From these results methods to increase the resilience of the real world network will be formed and evaluated. Possible methods could include either permanently or adaptively 'rewiring' the network in the event of a hazard and solutions that change as little of the network structure as possible are preferred, as they are more likely to be economically viable.

Output: Identification of inherently robust classes and spatial configurations of systems and methods to modify inherently vulnerable real-world networks to increase their resilience.

Research Questions:

v. What is the best measure for identifying specific vulnerable nodes and/or links in a network?

vi. What is the best method at reducing any inherent vulnerability in a real world infrastructure system?

5. Recommendations to crisis managers and infrastructure planners

Method/Output: The findings of this project will be summarised and will aim to inform both crisis managers (how they can best cope with damaged infrastructure in the aftermath of a disaster) and infrastructure planners (showing the best methods to modify their systems so they are better prepared for disasters). The summary will detail which network classes are inherently resilient / vulnerable to different types of disasters. For those that are inherently vulnerable methods to increase their resilience will be indicated.

1.4: SCOPE OF RESEARCH

To keep this work to a manageable size, a small number of limitations have been placed on the network models.

i. This research does not consider the interdependency between infrastructure systems. Many studies recognise that there is some level of interdependency between infrastructure systems, for instance, to operate normally the transportation network requires electricity from the power grid (for traffic lights, trains, etc.). However, this interdependency is not yet fully understood and/or mapped. To include this element into the network model would not only add another layer of complexity, but would also require many assumptions to be made. Due to the lack of interdependent models of interacting infrastructure systems it is not clear how many connections there are between two interconnected infrastructure networks, if the highly connected nodes in each system form the interconnected nodes, or how the flow of service in both systems is affected by their shared connections, among other questions. To answer these questions assumptions would need to be made, many of which may be unrealistic and could affect the validity of the network model. For this reason, interdependency has not been considered in this research.

ii. The network graph theory models analysed and generated in this thesis do not include parallel edges (parallel links) and/or self-loops (as illustrated in Figure 1.3). Parallel edges occur when a pair of nodes are connected by more than one link and self-loops are edges that connect a node to itself. The inclusion of these into a network constitutes a weighted network model, which could have different analysis results to those that are un-weighted. These additional links are not included in traditional network generation algorithms and so are not included in this thesis. However, an exception to this exclusion of parallel edges is made when strategies to increase the resilience of the European air traffic network are developed; the reasons for this inclusion are discussed in Chapter 4.8.

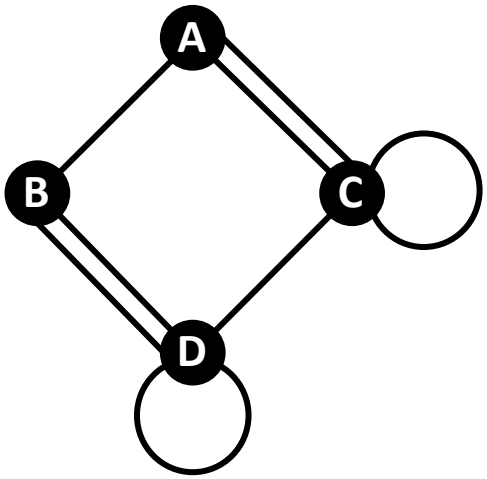


Figure 1.3: An illustration of parallel edges/links (between nodes A-C and B-D) and self-loops (nodes C and D).

iii. This research does not analyse weighted network models. Network models can be weighted by using parallel edges (outside the scope) or by assigning a weight to each link (for example, representing the resistance of a pipe in a water distribution network). This weighting can be easily incorporated into the hazard tolerance analysis (having been successfully achieved in previous studies), however, this component has not been included into a network generation algorithm (to the authors' knowledge) and any analysis of weighted networks is therefore restricted to real world systems only. For this reason, all of the networks used in this thesis are un-weighted.

iv. This research will only consider four of the nine national infrastructure sectors, as defined by the UK Government (Cabinet Office 2011a); namely the communications, water, energy and transport sectors (and their associated sub-sectors), excluding, the emergency services, government, health, financial services and food national infrastructure sectors.

1.5: STRUCTURE OF THESIS

Chapter 2: This chapter introduces and defines the terms 'infrastructure' and 'resilience', shows how real world infrastructure systems can be categorised and identifies the main threats to these systems, according to Governments and academic researchers. The chapter also discusses how infrastructure networks are currently analysed and the problems associated with using these methods to improve the resilience of an infrastructure system. The recent advances in network graph theory aimed at solving this problem are presented, including the network theory concepts of 'classes', 'network measures' and 'hazard tolerance'.

Chapter 3: This chapter uses the European air traffic network and the Eyjafjallajökull volcanic event to show that this real world spatial network has the same topological hazard tolerance as its network class, but is vulnerable to random spatial hazards (contradicting this theory). To determine whether this vulnerability is unique to this network or is inherent of its class, a network generation algorithm is developed and used to generate proxy networks. These synthetic networks are then subjected to a simulated Eyjafjallajökull event, as well as other spatially coherent hazards, showing that they too are vulnerable to spatial hazards. The hazard tolerance of two other real world air traffic networks (China and US), and their synthetic counterparts, are also assessed.

Chapter 4: This chapter assesses the hazard tolerance of a range of spatial networks with different topological and spatial characteristics, to determine which combinations of these characteristics are resilient / vulnerable to spatial hazard. Due to the lack of complete and detailed datasets for real world infrastructure systems, a range of synthetic networks with different topologies and spatial properties are formed to simulate the differing characteristics of real world systems. The most resilient / vulnerable of these combinations to different locations and sizes of spatial hazard are initially identified by quantifying the proportion of disrupted connections for a given proportion of components or area removed and then by assessing their change in connectivity and performance for an increasing hazard size. These results of this analysis are then used to inform solutions to increase the resilience of the European air traffic network when subjected to spatial hazard.

Chapter 5: This chapter focuses on the impact that the removal of a single node can have to the functioning of the remaining network and develops methods to identify individual nodes that have a disproportionate effect to the remaining network when removed. A reduced complexity flow model is initially developed and used to show the applicability of using network metrics to analyse physically based systems. A sample network is used to assess the predictive skill of using network theory metrics, traditional physically based measures and combinations of these to identify nodes that can have a disproportionate effect to the network when removed.

Chapter 6: This chapter summarises and draws conclusions from the main findings of the research presented in this thesis and provides suggestions for further research.

CHAPTER 2: INFRASTRUCTURE NETWORKS, RESILIENCE AND GRAPH THEORY ANALYSIS

The previous chapter discussed the vital role that infrastructure systems play in underpinning the social and economic growth and productivity of our modern communities. It was also discussed that these systems can either aid or hinder the recovery of our communities in the aftermath of a disaster and for this reason increasing the resilience of these systems is of paramount importance. The problems, and complexities, associated with using current analysis techniques (physically-based models) for this task was outlined and it was discussed that some studies are turning to a network graph theory analysis approach to describe the fundamental properties of these systems. In this chapter, the concept of what constitutes an 'infrastructure system' and what is meant by the term 'resilience' are discussed. From this the main threats to infrastructure systems are identified and their potential impacts / consequences to our communities discussed. This chapter also outlines how infrastructure networks are currently analysed and introduces the newly applied analysis approach using network graph theory. A brief overview of the main elements of network graph theory is given along with a summary of applications to previous real world networks.

2.1: TYPES OF INFRASTRUCTURE NETWORKS

To better protect our communities from the effects of disasters though the use of our infrastructure systems the concept of 'infrastructure' and what constitutes as an 'infrastructure system' must be initially defined. This should be a relatively simple process, the Oxford English Dictionary defines 'infrastructure' as:

> *'The basic physical and organisational structures and facilities (e.g. buildings, roads, power supplies) needed for the operation of a society or enterprise.'* (Oxford Dictionaries 2012)

However, many governments (and other policy makers) often shy away from providing a clear definition of what is actually meant by the term 'infrastructure' (New Zealand

Government 2010). In the case of many countries, there does not appear to be an agreed or accepted definition. This could be due to fear of restricting the scope of the definition, leaving out vital systems, or could raise questions about why other systems have been included. This fear of inclusion / exclusion of certain systems may seem trivial, but could have many important future repercussions in terms of future policies and government funding. For many governments the definition of the term 'infrastructure' also depends upon the context in which it is being used; for example in the US the definition of 'infrastructure' has been '*evolutionary and often ambiguous*' (U.S. Congressional Reseach Service 2004). In a 1983 report by the US Congressional Budget Office, the term 'infrastructure' was defined as:

> *'facilities with the common characteristics of capital intensiveness and high public investment at all levels of government. They are, moreover, directly critical to activity in the nation's economy.'* (U.S. Congressional Budget Office 1983)

In this report, it was also noted that the term 'infrastructure' could be '*applied broadly to include such facilities as schools, hospitals, and prisons, and it often includes industrial capacity as well*' (U.S. Congressional Budget Office 1983). However, in a later report by the same office this definition was narrowed to exclude:

> *'some facilities often thought of as infrastructure – such as public housing, government buildings, private rail service, and schools – and some environmental facilities (such as hazardous or toxic waste sites) where the initial onus of responsibility is on private individuals.'* (U.S. Congressional Budget Office 1988)

In a later document, stating Public Law, the US Government characterised 'infrastructure' as:

> '*facilities with high fixed costs, long economic lives, strong links to economic development, and a tradition of public sector involvement.*' (U.S. Government 1984)

According to the US Government, the services that 'infrastructure' provide '*form the underpinnings of the nation's defence, a strong economy, and our health and safety*'

(U.S. Government 1984). This Public Law was one of the last significant documents to consider the definition of 'infrastructure'. Since this time US policy makers have instead preferred to address the needs of individual infrastructure sectors, thereby sidestepping the need to define the collaborative term (U.S. Congressional Reseach Service 2004).

Although, different governments (and even different departments within the same organisation) tend to have a different definition of the term 'infrastructure' a common theme exists: 'facilities that provide a service'. Many governments also acknowledge that infrastructure and economic prosperity are strongly linked (New Zealand Government 2010) and that infrastructure systems form the backbone of our modern communities. It can be deduced that, essentially, the term 'infrastructure' refers to the systems that provide our communities (both at the national and global levels) with the resources they need to sustain life and enable growth, by delivering a flow of services from areas of generation or storage (e.g. power stations) to areas of demand (e.g. communities).

Owing to the lack of an accepted definition for the term 'infrastructure' there is also a 'grey area' surrounding what systems should be classed as or constitute 'infrastructure'. In the early definitions of 'infrastructure' facilities such as 'highways, public transit systems, wastewater treatment works, water resources, air traffic control and airports' were included (U.S. Congressional Budget Office 1983). However, later definitions focus instead on defining several broad areas, into which smaller systems can be placed, rather than defining, and naming, each individual system. In one such study, O'Rourke (2007) classes infrastructure systems into one of six principal systems: electric power, gas and liquid fuels, telecommunications, transportation, waste disposal and water supply. Whilst, the UK Government defines nine areas as national infrastructure, Figure 2.1.

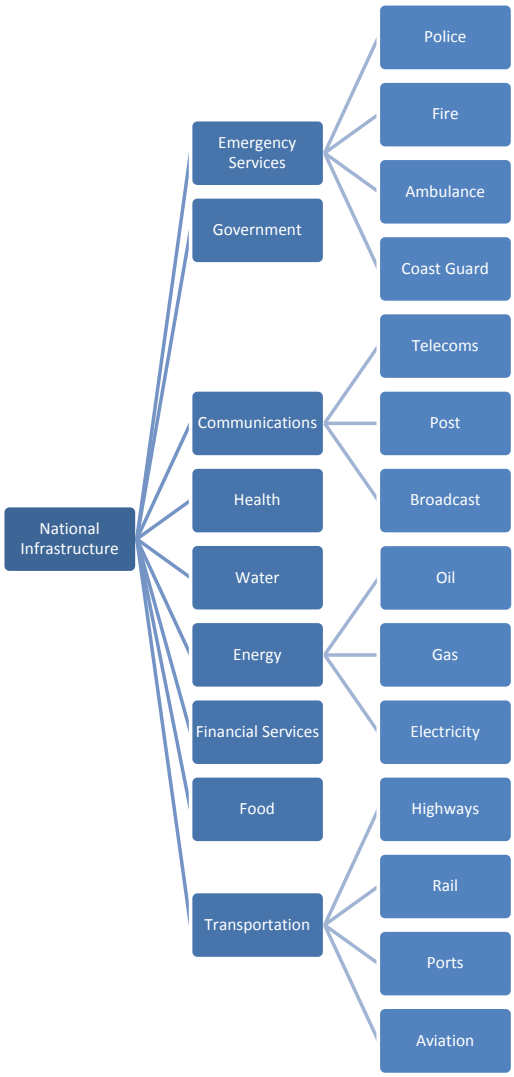


Figure 2.1: The nine national infrastructure sectors and associated sub-sectors as defined by the UK Government (Cabinet Office 2011a).

In recent years, the focus has moved from defining the term 'infrastructure' and what constitutes as an 'infrastructure system' to defining and categorising what is 'critical infrastructure'. Whilst there is still no universally accepted and used definition of this term, many individual governments have recently formed their own clear definition. These definitions tend to focus on the idea that these 'critical' systems as those that would lead to severe economic and/or social consequences, or even loss of life, if they were damaged or destroyed. The term 'critical infrastructure' has been defined by the UK, Australian and US Governments and the EU as:

> UK – *'Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life.'* (Cabinet Office 2010a)

> Australia – *'Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.'* (Australian Government 2010)
>
> US – *'Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have debilitating impact on the security, national economic security, national health or safety, or any combination of those matters.'* (DCSINT 2006)
>
> EU – *'Critical Infrastructure consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments.'* (Cabinet Office 2010a)

The UK Government acknowledges that these definitions are '*important to ensure clarity and consistency when considering whether infrastructure is critical*' (Cabinet Office 2010a). To define whether an infrastructure system, or component of a system, can be classed as 'critical' the UK Government has developed a Criticality Scale (Table 2.1). This scale is used to categorise infrastructure according to the impact of its loss, on a national scale, accounting for: economic impact, impact on life and impact on essential services. To be classed as 'critical' the system must fall into CAT 3 or above. However, there does not appear to be a publically available document listing the criticality of each component within the nine defined national infrastructure areas (Figure 2.1). Therefore, it is still unclear as to the exact systems the UK Government defines as 'critical infrastructure'.

Table 2.1: Criticality Scale for national UK infrastructure (Cabinet Office 2010a).

Criticality Scale	Description
CAT 5	This is infrastructure the loss of which would have a catastrophic impact on the UK. These assets will be of unique national importance whose loss would have national long-term effects and may impact across a number of sections. Relatively few are expected to meet the Cat 5 criteria.
CAT 4	Infrastructure of the highest importance to the sectors should fall within this category. The impact of loss of these assets on essential services would be severe and many impact provision of essential services across the UK or to millions of citizens.
CAT 3	Infrastructure of substantial importance to the sectors and the delivery of essential services, the loss of which could affect a large geographic region or many hundreds of thousands of people.
CAT 2	Infrastructure whose loss would have a significant impact on the delivery of essential services leading to loss, or disruption, of service to tens of thousands of people or affecting whole counties or equivalents.
CAT 1	Infrastructure whose loss could cause moderate disruption to service delivery, most likely on a localised basis and affecting thousands of citizens.
CAT 0	Infrastructure the impact of the loss of which would be minor (on national scale).

This thesis acknowledges that there is no universally accepted definition of the term 'infrastructure' or classification of an 'infrastructure system'. However, as this thesis is produced in the UK the definition of the terms 'infrastructure' and 'critical infrastructure' from the UK Government and the classification of the nine national infrastructure sectors, and subsectors, are adopted.

2.2: DEFINITIONS OF RESILIENCE

It has previously been discussed that the severity and lasting impact that the effects of disasters have on our communities are often linked to the resilience of the underpinning infrastructure systems. Therefore, to ensure that these systems are resilient, and can protect our communities, the term 'resilience' and what makes a system resilient must first be identified. In a similar manner to the term 'infrastructure' the term 'resilience' is also seemingly difficult to define and the definition often depends upon the context in which it is being used. The Oxford English Dictionary defines 'resilience' as:

> '*The ability of a substance or object to spring back into shape'* or *'the capacity to recover quickly from difficulties.'* (Oxford Dictionaries 2012)

Whilst, previous studies in ecology, systems and information engineering and risk management have defined 'resilience' as:

> Ecology – '*Measures of the persistence of systems and of their abilities to absorb change and disturbance and still maintain the same relationships between populations or state variables.*' (Holling 1973)
>
> Systems and information engineering – '*The ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks.*' (Haimes 2009)
>
> Risk management – '*The uncertainty about and severity of consequences of the activity given the occurrence of any types of events.*' (Aven 2011)

These definitions all differ, however, in a similar manner to the term 'infrastructure' there is a common theme connecting all definitions. With regards to infrastructure systems, the Australian Government does not have a universally used definition of 'resilience' (Rogers 2011) and the US Government has only short definition of the term:

> '*The ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions.*' (Homeland Security Advisory Council 2011)

The UK Government has the most detailed definition of the term which was formed as part of its plans to increase the resilience of national infrastructure systems (shown in

Figure 2.1). These plans are a direct result of the disruption caused by the summer 2007 floods, which caused 13 deaths, flooded 44,660 homes and cost the UK economy over £4 billion (BBC 2008; Environment Agency 2010a). After this flood event a detailed report was commissioned, the Pitt Review (2008), which called for '*a more systematic approach to building resilience in critical infrastructure*' (Cabinet Office 2011a) and highlighted the need for:

- *Improved understanding of the level of vulnerability to risk to which infrastructure and hence wider society is exposed;*
- *More consistent emergency planning for failures;*
- *Improved sharing of information at a local level for emergency response planning.*

In the Pitt Review the term 'resilience' was defined as:

> '*The ability of a system or organisation to withstand and recover from adversity.*' (Cabinet Office 2008c)

In response to the recommendations in the Pitt Review, the UK Government published the consultation document '*Strategic Framework and Policy Statement*' in 2010 (Cabinet Office 2010a) which set out the process and timescale for a Critical Infrastructure Resilience Programme. This report adopted the definition of the term 'resilience' from the Pitt Review and emphasised that in the Government's view resilience encompasses activity to prevent, protect and prepare for natural hazards. Responses to this consultation document were obtained from all nine areas of the national infrastructure (Figure 2.1) and all areas highlighted the need for a clearer definition of the term 'resilience' (Cabinet Office 2010b). From these responses the Government produced a further document for consultation defining 'resilience' in greater detail (Cabinet Office 2011a), to which responses were again gathered and a final report produced: '*Keeping the Country Running*' (Cabinet Office 2011b). In this report the UK Government identifies four components needed to build resilience into infrastructure (shown in Figure 2.2 and defined in Table 2.2).

Figure 2.2: The four components of infrastructure resilience, according to Cabinet Office (2011b).

Table 2.2: A summary of the definitions of the four components of resilience, as given by Cabinet Office (2011b).

Resistance	**Reliability**
The Resistance element of resilience is focused on providing protection. The objective is to prevent damage or disruption by providing the strength or protection to resist the hazard or its primary impact.	The Reliability component is concerned with ensuring that the infrastructure components are inherently designed to operate under a range of conditions and hence mitigate damage or loss from an event.
Redundancy	**Response & Recovery**
The Redundancy element is concerned with the design and capacity of the network or system. The availability of backup installations or spare capacity will enable operations to be switched or diverted to alternative parts of the network in the event of disruptions to ensure continuity of services.	The Response and Recovery element aims to enable a fast and effective response to and recovery from disruptive events. The effectiveness of this element is determined by the thoroughness of efforts to plan, prepare and exercise in advance of events.

From these definitions it can be deduced, that in the view of the UK Government, for an infrastructure system to be resilient it must have increased strength to resist the primary impact of the hazard (resistance), to have some ability to maintain function in a reduced capacity (reliability), have increased or backup capacity (redundancy) and be quickly repaired back to normal operation (response and recovery). It can also be stated that the lack of one of these four elements could result in the decrease of the resilience of the system as a whole. For example, if the components of a system lacked the resistance (strength) to resist the primary impact of the hazard and even though there was an effective management plan in place (response and recovery) there would be an increased recovery time, due to the increased initial damage to system components. Likewise, if a system lacked redundancy (capacity) the flow of service to communities could be restricted, or even interrupted, if system components were slightly damaged and flow along them could not be redistributed.

The definition of 'resilience' may not have received much attention from individual Governments, but it has been debated by many academic researchers. The most notable are the studies by Bruneau et al. (2003) and O'Rourke (2007) who base their definition upon that of Comfort (1999):

> '*The capacity to adapt existing resources and skills to new situations and operating conditions.*' (Comfort 1999)

Bruneau et al. (2003) state that resilience can be understood:

> '*As the ability of the system to reduce the chance of shock, to absorb a shock if it occurs (abrupt reduction of performance) and to recover quickly after a shock (re-establish normal performance).*' (Bruneau et al. 2003)

Unlike the UK Government, these studies also express their idea of resilience graphically (Figure 2.3), capturing the initial damage to the system (the loss of quality of the infrastructure of a community from 100% to 50% at t_0) and the time taken to restore the infrastructure (from t_0 to t_1). It can also be seen from this graphical view that the resilience of a system is directly affected by the initial damage to the system and also the time taken to restore functionality to the system. However, less apparent, in the figure, is the impact of redundancy to the resilience of the system; although, it

could be deduced that this is implied and accounted for in the measure of the quality of infrastructure (y-axis).

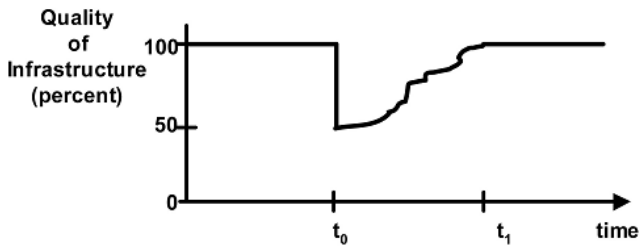


Figure 2.3: A conceptual definition of the resilience of an infrastructure system (Bruneau et al. 2003).

These studies also quantify the idea of resilience by using formulae to measure the size of the expected degradation in quality over time (from initial impact, at t_0, to full recovery, at t_1) as shown by Equation 2.1. Using this equation the resilience of different infrastructure systems can be quantified and compared.

$$R = \int_{t_0}^{t_1} [100 - Q(t)]\, dt \qquad 2.1$$

In a similar manner to the UK Government, Bruneau et al. (2003) also defined four elements of resilience, which were later refined by O'Rourke (2007) and are shown in Table 2.3. Although these definitions seem similar to those of the UK Government there are subtle differences. Both parties agree that the infrastructure system must include redundancy and that the system must also have sufficient strength to withstand the impacts of hazard, but each give this component a different name (resistance / robustness). The UK Government's element of response and recovery splits the idea behind O'Rourke's rapidity into two distinct areas, where recovery is concerned with pre-event planning and response the time taken to restore service after the event. The idea of pre-planning is not explicitly stated in the elements used by O'Rourke, although it is implied in the idea of rapidity (as the speed with which disruption can be overcome can only be improved through better planning). Also, the idea of early response by the emergency services is not explicitly stated by the UK Government and forms part of the idea of resourcefulness by O'Rourke. The two parties also differ in the concept of reliability, which encompasses the idea that infrastructure components should be designed to operate under a range of conditions

and is specifically stated by the UK Government and is again only implied by O'Rourke in the resourcefulness element.

Table 2.3: The four dimensions of resilience, according to O'Rourke (2007).

Robustness	**Redundancy**
The inherent strength or resistance in a system to withstand external demands without degradation or loss of functionality.	System properties that allow for alternate options, choice and substitutions under stress.
Resourcefulness	**Rapidity**
The capacity to mobilise needed resources and services in emergencies.	The speed with which disruption can be overcome and safety, series and financial stability restored.

Many studies have used these four elements of resilience (Table 2.3) and the quantifying equation (Equation 2.1) of Bruneau et al. (2003) and O'Rourke (2007) to assess and quantify the resilience of systems. These studies include: comparing seismic retrofit strategies in water distribution systems (Chang and Shinozuka 2004), seismic resilience assessment for acute care facilities (Bruneau and Reinhorn 2007) and the assessment of the resilience of networked infrastructure (Reed et al. 2009). One study, by Ouyang et al. (2012), expanded upon the graphical representation of resilience (Figure 2.3) to visually show three distinct stages of resilience (Figure 2.4).

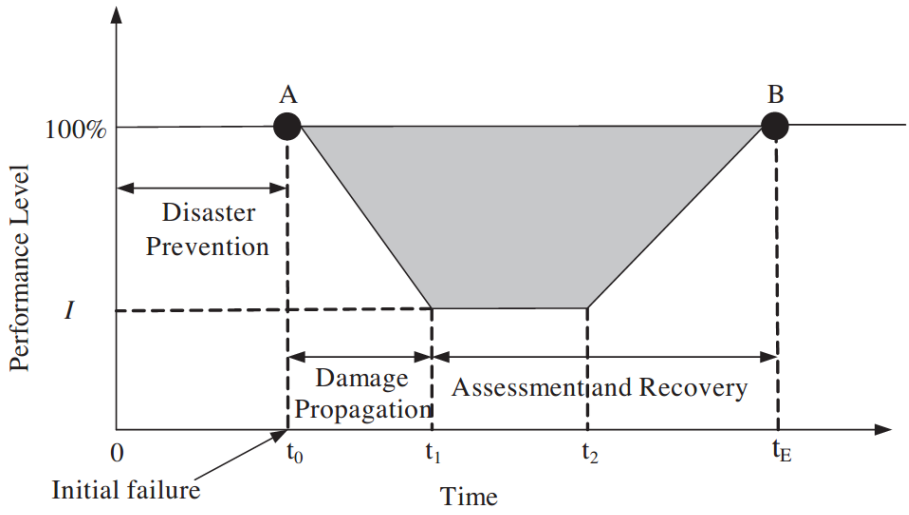


Figure 2.4: The typical performance response curve of an infrastructure system following the occurrence of a hazard, according to Ouyang et al. (2012).

Unlike the figure developed by Bruneau et al. (2003) and O'Rourke (2007), this figure incorporates an assessment of the damage to infrastructure before recovery can take place. This inclusion is logical as it will take time to assess the damage to the system before a plan for recovery can implemented. However, it is unclear whether the figure used by Bruneau et al. (2003) and O'Rourke (2007) accounts for temporary infrastructure measures, as their figure described the quality of infrastructure. For example, if the power supply to a community is disrupted the emergency plans could include the provision of generators to provide temporary power, subsequently causing the quality of the infrastructure to increase (as there is now provision of some power, although it may be restricted). In their study Ouyang et al. (2012) also state that many infrastructure systems are constantly evolving and that the resilience of the system will change depending on the time interval between 0 and t_0 (in Figure 2.4). Due to the recent publication of this study, there have currently been no other published studies which have adopted the model of Ouyang et al. (2012) and used it to assess the resilience of infrastructure systems, other than the authors themselves (Ouyang and Duenas-Osorio 2012). Therefore, it is unclear whether this method is more accurate, or has been adopted by other researchers, in place of the model of Bruneau et al. (2003).

Whilst many studies have used the models of Bruneau et al. (2003) and O'Rourke (2007) to quantify the resilience of infrastructure systems, to the authors' knowledge there does not currently exist a study which has used this method to inform decisions

on how to increase the resilience of an infrastructure system. These methods are useful at giving an indication of where the vulnerabilities may lie within the management of an infrastructure system (e.g. is the speed of recovery hampering the resilience of the system?) and are also useful to provide a quantification of resilience that can be used to compare different infrastructure systems. However, it is unclear whether this information could be used to provide information to minimise the impact to the quality of infrastructure (Figure 2.3) or the drop in performance level (Figure 2.4).

To conclude, many definitions of the term 'resilience' have been presented and debated; in a similar manner to the term 'infrastructure', the definition of the term 'resilience' used in this thesis will be the same as that stated by the UK Government. It has also been established that to be 'resilient' an infrastructure system must have sufficient strength to resist the initial impact of the hazard (resistance) and have additional capacity to reroute flow if necessary (redundancy). There is some debate regarding the other elements of resilience; however, it can be concluded that an effective management plan is needed to ensure a speedy recovery (rapidity / response) and that this plan must include details regarding the mobilisation of resources (resourcefulness). Additionally, it can be argued that to be resilient an infrastructure system must be capable of operating under a range of conditions (adaptable / reliable). It has also been established that the failure of one of these elements could prove to be detrimental to the long term functioning of the system (making for a longer recovery time).

2.3: IDENTIFICATION OF MAIN THREATS TO INFRASTRUCTURE

In 2008 the UK Government published the first National Risk Register (NRR) (Cabinet Office 2008a), fulfilling the commitment made in the National Security Strategy (Cabinet Office 2008b). This document is the public version of a classified assessment of national risks documented in the National Risk Assessment (NRA). The NRR proved to be the first step in providing advice on how people and businesses can prepare for civil emergencies. This document was updated in 2012, and again in 2013, to include the Government's current assessment of the likelihood and potential impacts of a

range of different civil emergency risks that may directly affect the UK (Cabinet Office 2012a; Cabinet Office 2013). The NRR takes its definition of the term 'civil emergency' from the Civil Contingencies Act 2004, which describes a civil emergency as:

- '*an event or situation which threatens serious damage to human welfare in a place in the United Kingdom,*
- *an event or situation which threatens serious damage to the environment of a place in the United Kingdom,*
- *war, or terrorism, which threatens serious damage to the security of the United Kingdom*' (Great Britian 2004).

This definition was used to identify a list of possible risks threatening the UK, though consultation with experts from government departments and wider fields. For each of these identified risks a reasonable worst case is chosen, which represents a realistic expectation of the risk when the highly implausible scenarios are excluded. A selection of risks and their 'reasonable worst case' scenarios are given in Table 2.4. The severity of the identified risk is dependent upon the likelihood of it happening over the next 5 years and the consequences / impacts that people will feel if it does happen. Therefore, the highest classified risks are those with a high probability of occurring and with a high impact if they do happen. In the NRA there is a list of 80 types of scenario that meet the definition of the term 'civil emergency' and a further 40 scenarios that have been placed on a reserve list, as they may occur in the long term future. It is worth noting that the NRA and NRR only consider risks that are likely to affect the UK directly (i.e. events occurring overseas are not included, unless they will directly affect the UK).

The NRA and NRR use two scales to quantify the likelihood of a civil emergency, depending on the risk in question. For the majority of naturally and accidentally occurring hazards, historical analysis and numerical modelling are used to form estimates of likelihood. These estimates are then combined with expert judgement to place the hazard the scale shown in Figure 2.5(b). The likelihood of terrorist, or other malicious attacks, is assessed based upon the willingness of individuals or groups to carry out attacks; the scale of these risks is shown in Figure 2.5(a). The impact of a civil emergency is assessed based on the number of fatalities, illness or injury caused levels

of social disruption, economic harm and psychological impact resulting from the emergency, which are all given a score from 0 to 5 (5 being high impact) and the overall relative impact of the emergency is given as the mean of these five scores. Figure 2.5 shows the relative likelihood and impact of 24 civil emergencies as given in the NRR (Cabinet Office 2013). From these matrices (Figure 2.5) the UK Government has identified the mains risks to be: pandemic influenza, coastal flooding, catastrophic terrorist attacks and severe effusive (gas-rich) volcanic eruptions abroad. These matrices are also summarised graphically in the report '*Keeping the Country Running*' (Figure 2.6).

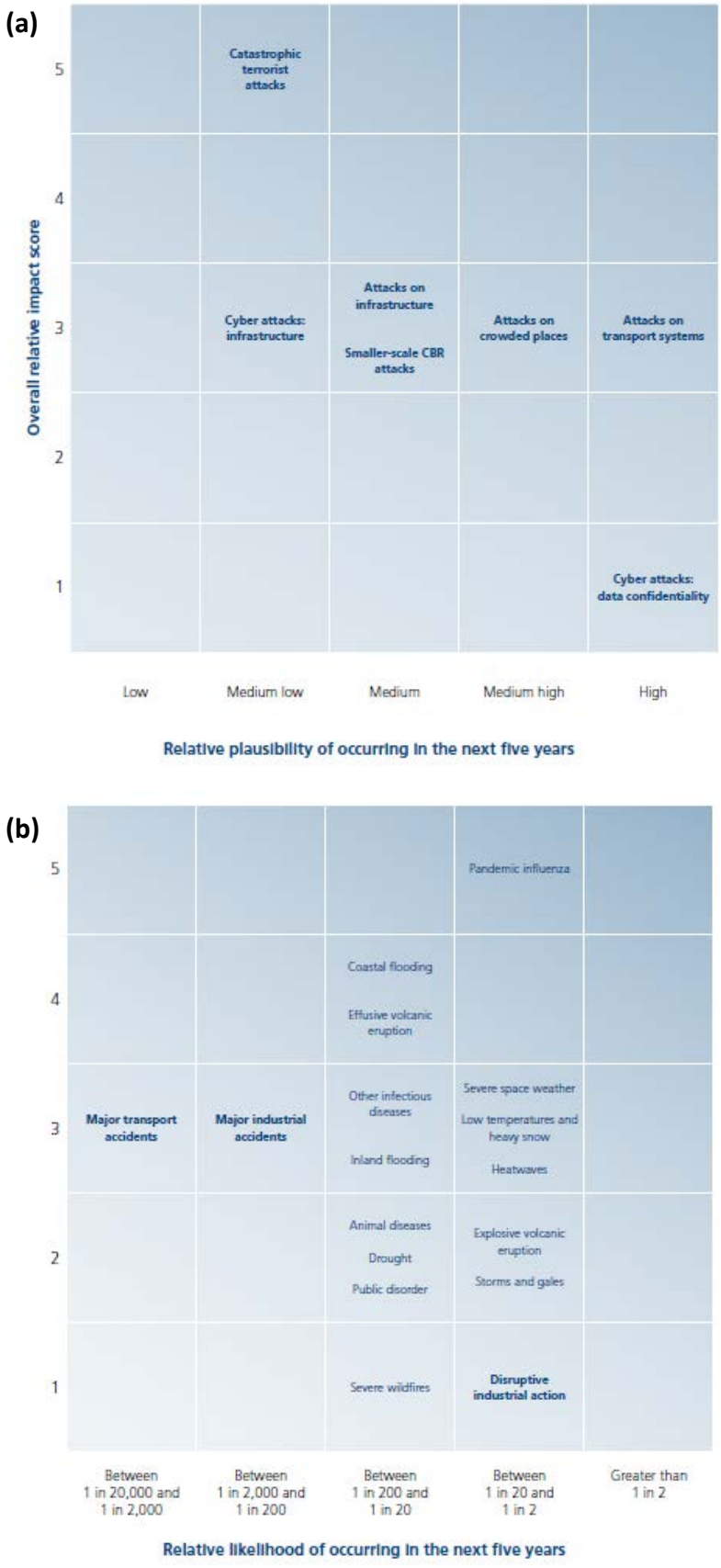


Figure 2.5: Civil emergencies as identified in the National Risk Register (2013), showing (a) risks of terrorist and other malicious attacks and (b) risks of natural hazards and major accidents. It is worth noting that the two scales for relative likelihood shown in (a) and (b) are not directly comparable with each other.

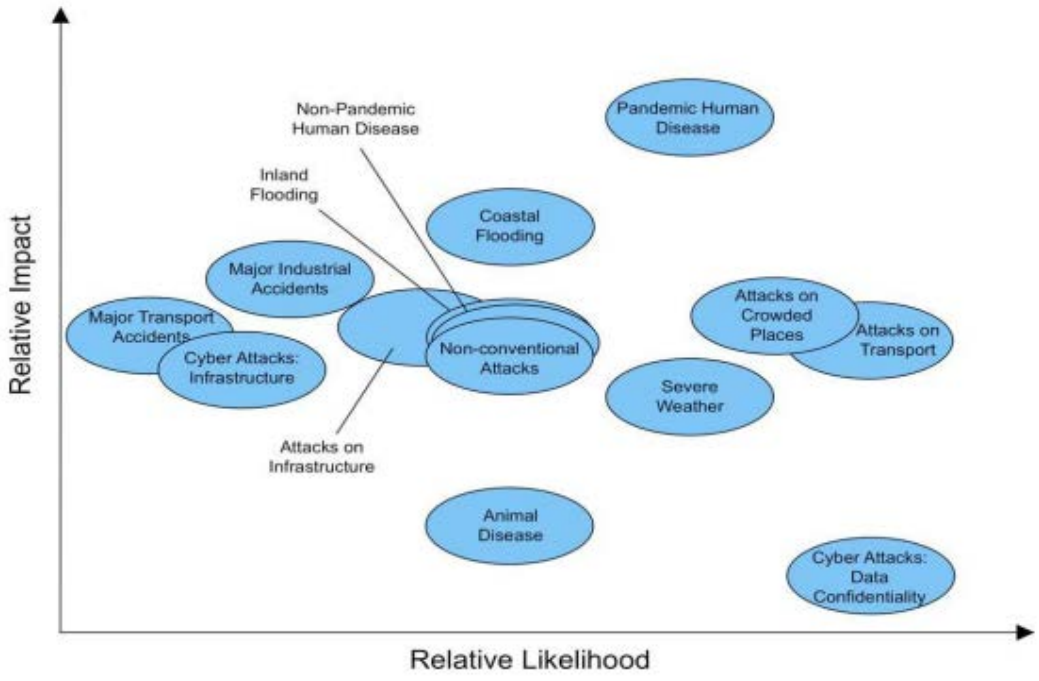


Figure 2.6: An illustration of the high consequence risk facing the UK (Cabinet Office 2011b).

From this graphical interpretation (shown in Figure 2.6), it is interesting to note that both *inland flooding* and *attacks on transport systems* have the same relative impacts, but that *attacks on transport* has a higher relative likelihood of occurrence. The assessment of *inland flooding* is based on the events of summer 2007 (in which 48,000 households and 7,300 businesses were flooded) and the November 2009 floods in Cumbria (notably causing the collapse of six bridges and isolating communities). The associated effects of these floods, to primary transport routes, electricity supplies and telecommunications, amongst others, has also been taken into account in this assessment. However, the assessment does not appear to consider the more recent, and devastating, events of the flooding in 2012, lasting in some places from April to June; although, the NRR does acknowledge that '*the frequency of flooding is increasing*' (Cabinet Office 2013). Whereas, the NRR highlights that the assessment of attacks on *transport systems* is influenced by the attacks to the London transport system on 7th July 2005 and the 1988 Lockerbie bombing. These events occur less frequently than the devastating inland flooding and should therefore mean that this risk has a lower probability of occurring. However, the relative likelihood of these attacks seems to be skewed by events in other countries, including: the attacks to Moscow's underground system in 2004 and the attacks on the World Trade Centres and the Pentagon in 2001. In contrast to the assessment of the relative likelihood of *inland flooding*, which can be

quantified using return periods, the attacks on transportation systems are more difficult to define and rely on an assessment of probable human behaviour by a group of experts. Therefore, the question could be raised as to how accurate the assessment of risks presented in Figure 2.6 is. Although attacks on transport can have devastating and in many cases fatal consequences, studying the reports of flooding in the past few years reveals that these events occur more frequently than attacks on transport and should therefore have a higher relative likelihood. This potential discrepancy highlights the difficulties in ranking, and prioritising, the risks faced by the UK.

Focusing on natural hazards, the report '*Keeping the Country Running*' details the potential hazards to the UK and outlines their probable effects to national infrastructure, Table 2.4 gives a typical summary for a selection of these hazards. The 'reasonable worst case' scenario and other potential effects of the natural hazard are also listed in this document. It is also worth noting that many of these hazards have the potential to affect many systems and that the failure of one system may impact upon others (interdependency). The interdependency of these systems is acknowledged, however, the analysis of this relies on the formation of interdependent networks, which is outside the scope of this thesis.

Table 2.4: A selection of reasonable worst case scenarios for natural hazards in the UK, as outlined in the report '*Keeping the Country Running Natural Hazards and Infrastructure*' (Cabinet Office 2011b).

Scenario	Reasonable Worst Case Scenario	Other Related Effects	Potential Impacts on Infrastructure
Inland Flooding	A single massive inland event or multiple concurrent regional events following a sustained period of heavy rainfall extending over two weeks (perhaps combined with snow melt or intense summer rainfall leading to widespread surface water flooding). The event would include major fluvial flooding affecting a large, single urban area. This is broadly regarded as a 0.5% annual probability flood event.	• Storms and gales • Snow • Land Instability (including offshore and submarine) • Heavy rainfall	• Loss of primary transport routes • Lack of staff availability • Impaired site access • Loss of power supplies • Loss or contamination of water supplies • Closure of local businesses increased demand for emergency power and water supplies • Increased demand for health and emergency services
Windstorm: Storm / Gales	Storm force winds affecting most of a region for at least 6 hours. Mean speeds in excess of 70mph with gusts in excess of 85mph. Short term disruption to infrastructure including power, transport networks, homes and businesses.	• Flooding • Land instability • Heavy rainfall • Wildfire	• Loss of power • Loss telecoms • Blocked road and train routes and flight disruption
Volcanic Ash	Volcanic ash incursions for up to 25 days. The UK mainland and potentially other parts of Europe could be affected for up to 10 of these days. A single period of closure within the 3 month eruptive episode may last up to 12 consecutive days, depending on meteorological conditions.	None	Sporadic and temporary closures of significant parts of UK airspace

A similar version of the graphical analysis produced by the UK Government (Figure 2.6) is used by other countries to prioritise risk; for example, the New Zealand Government uses this approach to assess specific natural hazard risks to infrastructure systems (Figure 2.7). However, their analysis is more detailed, and sophisticated, using the size of the 'bubbles' to reflect the range of potential consequences a hazard may have (for example, the consequence of a terrorist attack ranges from minor to major) and also to differentiate between the relative likelihoods of hazards located in different geographic areas. Using this approach they make the distinction that as each natural hazard has its own distinctive risk, regulation to mitigate these risks should not group all hazards together, but should consider each risk individually.

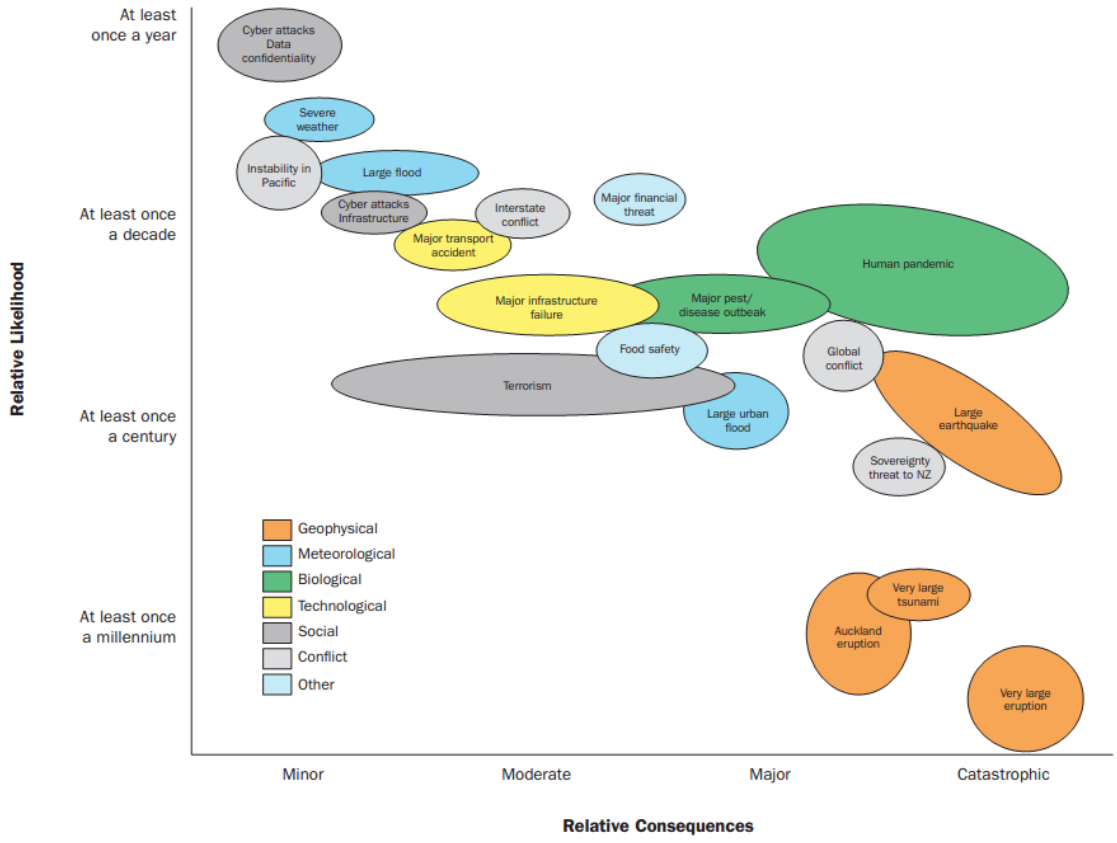


Figure 2.7: National risks to infrastructure in New Zealand (The Institution of Professional Engineers New Zealand 2012).

With regard to the specific threats to UK infrastructure the NRR is used, in combination with the document *'Keeping the Country Running'* to form resilience plans for each of the nine national infrastructure sectors (Figure 2.1). Publically available versions of these plans have been published annually since 2010 in the '*Sector Resilience Plans*' (Cabinet Office 2010c; Cabinet Office 2011c; Cabinet Office 2012b). The Plans include

the assessment of existing resilience within infrastructure systems and plans to build resilience and are continually updated to account for the changing risks facing infrastructure. The majority of these plans seem to focus on the assessment and evaluation of current infrastructure to cope with the effects of the potential hazards outlined in the NRR. The publically available version of these plans does not include details regarding strategies to increase the resilience of current infrastructure systems. However, these Plans do not include information regarding the specific impact that these hazards pose to infrastructure systems (e.g. which individual infrastructure components are most at risk). This is addressed in the following sub-section, which focuses on the main threats that natural hazards pose to infrastructure systems within UK and uses previous hazards to identify the potential impacts of future threats to infrastructure.

2.3.1: SUMMARY OF THE MAIN THREATS TO INFRASTRUCTURE SYSTEMS AND THEIR POTENTIAL IMPACTS

The majority of the natural hazards threatening UK infrastructure today can be broadly placed into one of two categories, those caused by weather related impacts and those resulting from geotechnical conditions. As such, this sub-section has been split into three further sub-sections, one for each of these main areas of risk and one further section other detailing all other risks. It is worth noting that some of these risks can be placed into two categories, for example coastal erosion is caused by weather related impacts but the severity of these impacts is linked to the rock/soil structure (geotechnical). These risks have been placed into the category which is deemed to have the most influence over the likelihood and impact of the risk. It is also worth considering that many of the natural hazard risks outlined in this section can cause other natural hazard risks. For example, flooding can occur due to a period of heavy rainfall, but can also be caused by severe storms and gales and the melting of an extensive snowfall which are both natural risks themselves, and pose their own threat to UK national infrastructure (Cabinet Office 2011b).

2.3.1.1: WEATHER RELATED RISKS

Flooding has been identified as the greatest risk to the UK, both currently and in future climate change exacerbated scenarios (Institution of Civil Engineers 2009). The effects that this hazard can have to our communities are illustrated in many past events, including the flooding across England in summer 2007. This event was caused by a period of extreme rainfall (the wettest since rainfall records began in 1766) and resulted in the flooding of over 55,000 homes and businesses (Cabinet Office 2008c; Environment Agency 2007). Flooding can also have devastating effects to our infrastructure systems; for example, the summer 2007 event caused damage to energy infrastructure systems through the closure of electricity substations which were affected by floodwaters (including the closure of the Castle Meads substation which left 42,000 people without power for up to 24 hours (Cabinet Office 2008c)). Water infrastructure was also badly affected, with the closure of water treatment works due to flooding (including the closure of the Mythe water treatment works which caused 350,000 people to be without access to mains water supply for 17 days (OFWAT 2007)). This event also directly impacted transport infrastructure, forcing the closure of roads and railways (due to flooding). Other recent notable flood events in the UK include the flooding in Cumbria in November 2009 (which notably '*cut in half*' (Met Office 2012) communities through severe damage to bridges and also caused disruption to energy and water infrastructure (The Guardian 2010)) and the summer 2012 floods (which included a flash flood event in Newcastle, where a month's rainfall fell in 2 hours, causing major disruption to transport infrastructure). In a recent report, the Environment Agency highlighted that there were '*significant risks to important national infrastructure*' (Environment Agency 2009) as a result of flooding; with over 55% of water and sewage pumping station/treatment works, 20% of railways, 10% of major roads, 14% of electricity and 28% of gas infrastructure located in areas at risk from flooding (Figure 2.8).

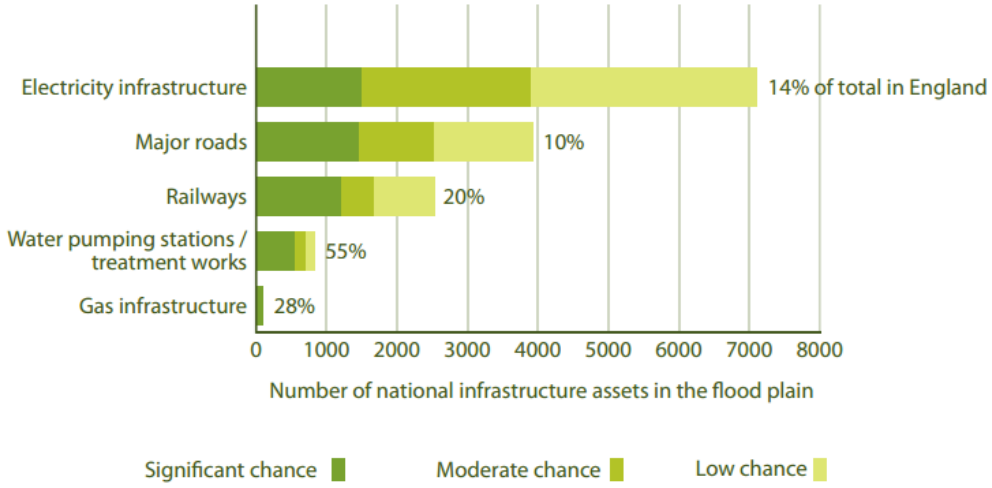


Figure 2.8: The proportion of national infrastructure assets located in flood risk areas (Environment Agency 2009).

Windstorms and gales are the *'most common cause of damage and disruption in the* UK' (Met Office 2013) and they have the potential to affect widespread areas. The average cost of damage to the UK each year is estimated to be at least £300 million (Met Office 2013). One of the most notable past windstorm events, to affect the UK, occurred on 16 October 1987. This storm affected southern England and was poorly forecast with unusually high wind speeds and estimated losses of around £1.4 billion (Risk Management Solutions 2007). The storm brought down around 15 million trees, which caused damage to power lines and disrupted power supply and telephone communications to Gatwick airport as well as thousands of homes (Risk Management Solutions 2007). Transport infrastructure was also badly affected, as debris closing many roads and railways, with Kent, Surrey and Sussex the worst affected counties. Windstorms have the potential to affect a wide range of infrastructure systems, with perhaps the energy sector the most vulnerable to damage caused by falling trees severing power cables. The majority of distribution faults to the UK power grid, resulting from weather-related effects, occur due to windstorms and gales (McColl et al 2013).

Severe winter weather (consisting of low temperatures, heavy snowfall and ice storms) also has the potential to affect infrastructure systems, with heavy snowfall causing the most disruption to UK infrastructure in recent years. For example, the winter of 2009-10 was '*the most severe in the UK for over 30 years*' (Met Office 2013) with a mean UK temperature of 1.5°C for the whole winter. Significant snowfalls were recorded from

mid-December until the end of February and were the most widespread of a winter for 30 years. This snowfall caused '*extensive disruption*' to the UK's transport infrastructure (Transport Committee 2011), with Heathrow airport closed between 18th and 20th December after 7cm of snow fell within one hour (Heathrow Winter Resilience Enquiry 2011). Heavy snowfall is most likely to directly affect energy infrastructure (through damage to power lines), communications infrastructure (due to damage to telephone masts) and transport infrastructure (due to closed roads and rail links and disruption to airport operations). Ice storms also have the potential to disrupt energy infrastructure, with power lines and transmission towers particularly susceptible to damage (Figure 2.9). During these storms ice can accumulate on power lines, initially causing them to loose efficiency (due to sagging, Figure 2.9(a)) and can eventually snap the power cables leading to a total loss of power. These storms can also cause total failure of transmission towers (Figure 2.9(b)), which can result in a lengthy repair time and a high cost of repair. A notable example of this type of failure is the January 2008 Ice Storm which damaged 1196km of transmission lines and 4017 transmission towers in China, causing transmission systems in some areas to become '*completely dysfunctional*' (Yang et al. 2013).

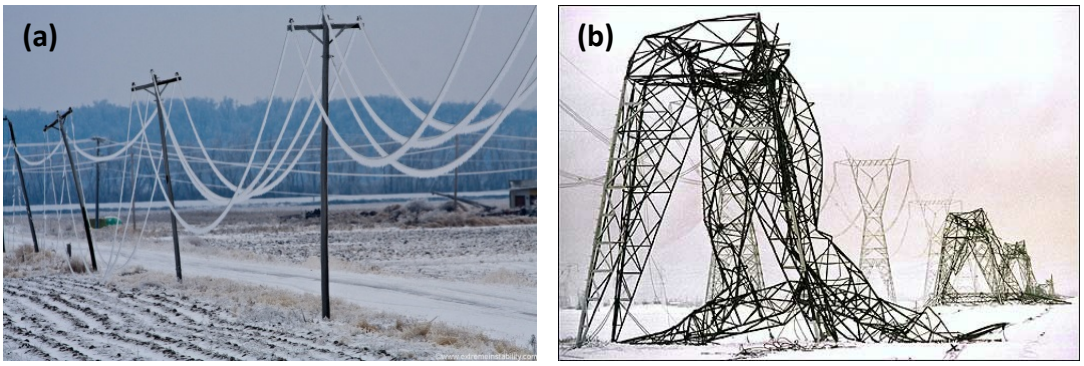


Figure 2.9: Damage to (a) power lines (Hollingshead 2007) and (b) transmission towers due to ice storms (Canadian Energy Issues).

Heatwaves are another form of extreme weather event that has the potential to affect infrastructure systems within the UK. This type of risk can put a strain on our infrastructure systems and cause a disruption to service prevision, with energy infrastructure particularly susceptible to disruption. In the event of a heatwave it is likely that customers will operate an increased number of air conditioners, which can dramatically increase the demand for power. This has the potential to lead to demand outstripping supply resulting in power blackouts. This problem can also be

exacerbated by the drop in efficiency from some power grid components; for example, extreme heat can cause power lines to sag, resulting in a drop in their performance, and can also cause transformers to become less efficient. Heatwaves also have the potential to directly affect transport infrastructure, through the deterioration of road and runway services (Cabinet Office 2013) which can lead to lengthy transport delays. Water infrastructure can also be directly affected by this risk, as heatwaves can occur during periods of drought where there is often a reduction in the water supply available. Coupled with the increase in customer water usage, due to the high temperatures, this can put a strain on the available resources.

Droughts can also put a strain on infrastructure systems, with the water sector the most affected. The most recent drought in the UK occurred in 2010-12, where some parts of the south-east and eastern England recorded the lowest 18 month rainfall for at least 100 years. Within this severe dry spell water companies ran water saving campaigns and managed to restrict the imposed water saving measures to domestic customers only (i.e. there was no impact to industry or agriculture) (Cabinet Office 2013).

2.3.1.2: GROUND CONDITION RISKS

Coastal erosion is defined as '*the removal of material from the coast by wave action, tidal currents and/or the activities of man, typically causing a landward retreat of the coastline*' (British Geological Survey 2012a). In England and Wales, it has been estimated that of the 6,251km coastline, 3,327km (53%) are cliffs subject to instability and erosion (Environment Agency 2010b). Figure 2.10 shows the distribution of these erodible cliffs in England; from this figure it can be seen that there are only a few areas of the English coastline that are not vulnerable to this type of risk. Whilst, coastal erosion is a major issue for those living in these communities and can leave local councils facing multi-million pound repair bills (for example the village of Hallsands (Devon) collapsed into the sea during a storm in January 1917, destroying all but two homes), the overall threat to our infrastructure systems remains small. However, some major infrastructure components must be located close to the coast and therefore have the potential to be affected by this threat. This mainly affects energy

infrastructure, as nuclear power stations must be located close to an area of guaranteed continuous water supply and gas terminals which import fuel from other countries. There are some reports of coastal erosion threatening these components, such as the Bacton Gas Terminal (Dickson et al. 2006)); however, this risk is known, can be predicted to some degree and can be mitigated through the use of coastal defences.

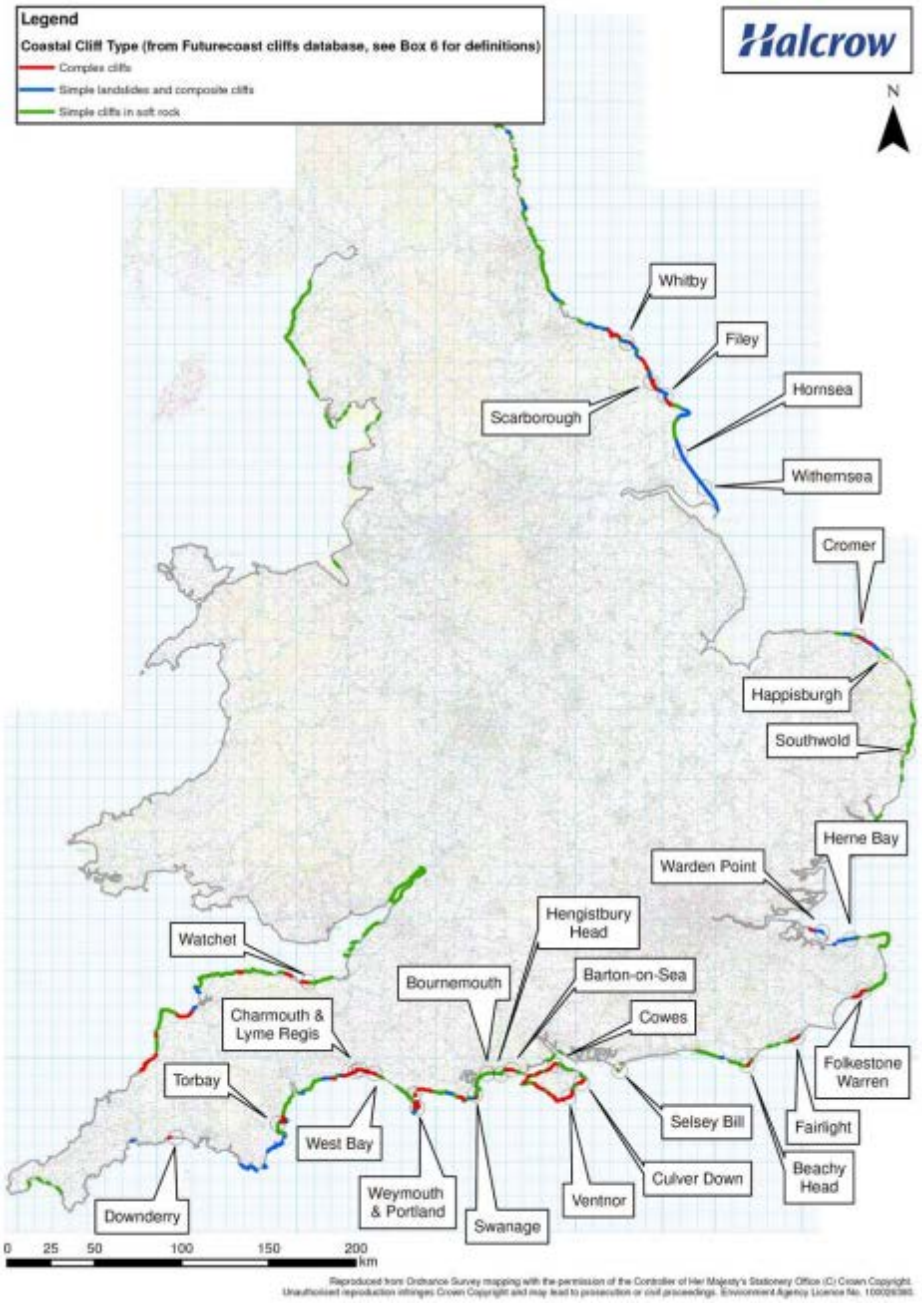


Figure 2.10: The distribution of erodible cliffs in England (Environment Agency 2010b).

Landslides mainly affect transportation infrastructure, with a significant proportion of slope failures occurring on man-made railway embankments, potentially leading to train delays and cancellations for extended periods of time. Road infrastructure can

also be affected, for example, a landslide in Rothbury (Northumberland) in December 2012 forced the closure of a road which has still not reopened, due to continuing ground movement in the area (Northumberland Gazette 2013). However, landslides also have the potential to affect other infrastructure sectors, by causing damage to electricity pylons (energy infrastructure) and uncovering, or damaging, buried pipelines (energy and water infrastructure). All of these effects could lead to significant disruption to the levels of service provided by these systems to our communities, which have the potential to propagate to areas unaffected by the initial landslide.

2.3.1.3: OTHER RISKS

In 2011 the UK recognised, for the first time, extreme space weather events as rare but potentially high impact hazards (Royal Academy of Engineering 2013). Space weather has the potential to directly, or indirectly, affect the majority of our infrastructure in the UK (Figure 2.11). The majority of these effects are related to the operations of satellites and the power grid; though due to the interdependency of infrastructure systems the loss of the power grid could affect the supply of clean water, communications and transport, for example (Lloyd's 2010). Space weather can cause the failure of power grids, due to geomagnetically induced currents which overloading parts of the system (Wik et al. 2009). To date, space weather has not greatly affect the UK, but has had a significant impact to the power grids in other nations; notably, causing the entire province of Quebec (Canada) to suffer an electrical blackout affecting 6 million people until power was restored 9 hours later (NASA 2009).

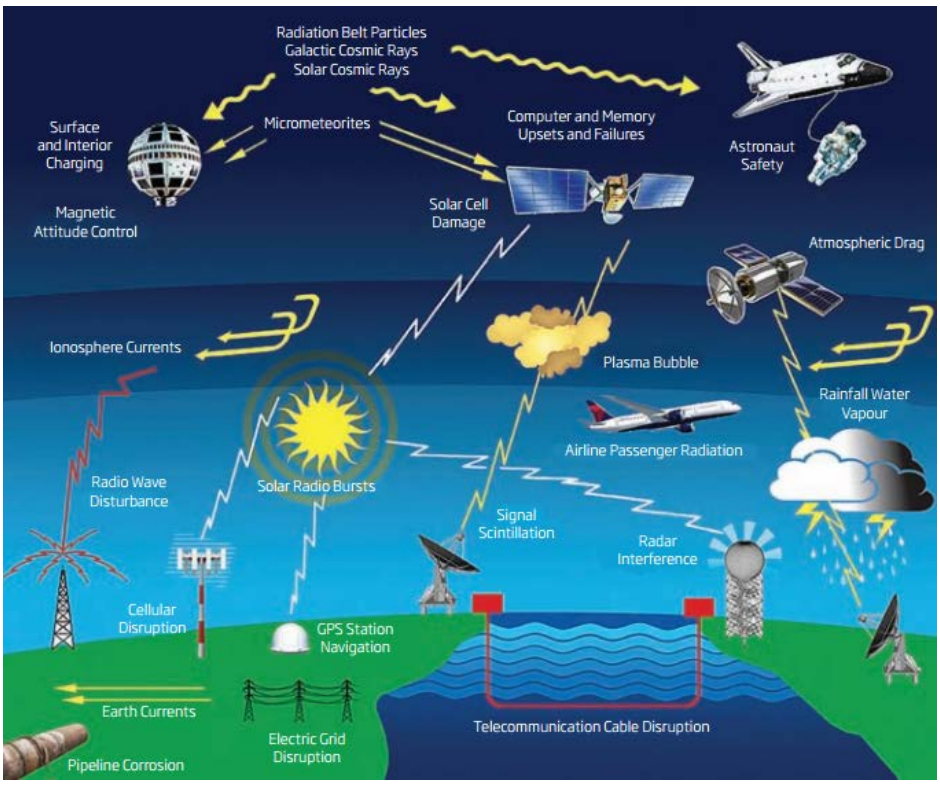


Figure 2.11: The potential impacts of space weather (Royal Academy of Engineering 2013).

Volcanic eruptions also pose a threat to UK infrastructure, even though there are no active volcanoes within the UK. This threat was highlighted in the 2010 eruption of the Eyjafjallajökull volcano in Iceland which caused disruption to air transportation infrastructure within the UK through the closure of European airspace (Brooker 2010). This volcanic eruption was classified as an 'explosive eruption' and is one of two types of eruption that have the potential to affect the UK (Cabinet Office 2013):

- *effusive* – these eruptions are not violent and include the outpouring of lava from vents in the volcano and can emit large volumes of gases and aerosols into the atmosphere for months or even years;
- *explosive* – are characterised by a violent, explosive eruption which usually emits a large ash cloud.

These eruptions could affect the UK through the emission of volcanic ash and aerosols. At high altitude the effects are generally limited to aircraft, potentially causing engine failure and high concentrations could also pose health risks to air passengers. However, if present at ground level the impacts could directly affect human health, contaminate water supplies and affect electricity infrastructure (British Geological Survey 2012b).

Earthquakes also pose a small risk to UK infrastructure, as the UK is located in an area low seismicity, where moderate earthquakes are rare, but can occur. The BGS monitors the earthquake activity in the UK and has recorded 20 significant earthquakes (Magnitude 4.0 or greater) between June 1970 and February 2008 (British Geological Survey 2013a). This included the Magnitude 5.2 event on 27 February 2008 which was felt across large parts of the country, but caused only minimal damage to structures. The BGS has assessed the risk of an earthquake in the UK for a 2,500 year return period (Figure 2.12). From this data, it can be established that in the UK earthquakes have the potential to cause some damage to structures and cause disruption to services, but are unlikely to have a major impact to our infrastructure systems.

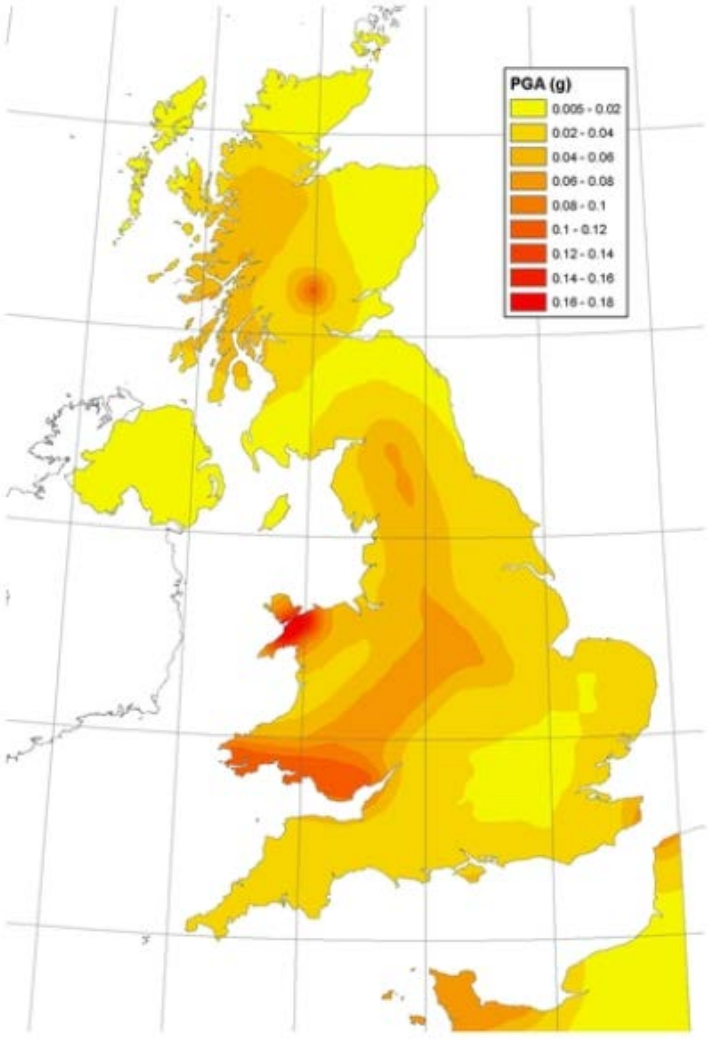


Figure 2.12: Hazard map for a 2,500 year return period seismic event in the UK (British Geological Survey 2013b).

The 'Boxing Day' earthquake in 2004, which initiated a devastating tsunami, has led to many governments assessing the likelihood, and potential impacts, of similar events occurring in other parts of the world. This earthquake occurred off the west coast of northern Sumatra (Indonesia) and measured M_W9.3, making it the second biggest earthquake ever recorded. The resulting tsunami caused loss of life in 11 countries, with an estimated total death toll of more than 230,000 (Synolakis 2005). This event also had a devastating impact to infrastructure systems, breaking water and sewage pipes, contaminating water and food sources. This damage led to disruption to the water and electricity systems, which hampered rescue efforts in immediate aftermath of the disaster and caused longer term problems with disease (World Health Organisation 2005). Whilst events on this scale are rare there is historical and geological evidence that tsunamis have affected the UK in the past (DEFRA 2005), and as such there is a potential for this risk to pose a threat to our infrastructure systems in the future. These events are likely to be triggered by earthquakes in other countries and underwater landslides, with the possible impacts of these tsunamis varies from very low (with a consequence of probability of less than 0.1%) to very high (with a consequence of probability greater than 90%) (DEFRA 2005). Therefore, it can be concluded that tsunamis pose a threat to UK infrastructure, although the potential damage could be minimal (e.g. a temporary loss of service due to slight damage to individual infrastructure components) or devastating (e.g. complete loss of infrastructure within the impact area).

From all of the above natural hazards, whether weather related or caused by ground conditions, etc., it can be seen that they have the potential to affect large geographic areas of the UK. However, it is also important to note that these hazards tend to be spatially coherent; for example, it is unlikely that several isolated areas, or dispersed counties, of the UK will be affected by a windstorm event (e.g. the counties of Devon and Cumbria), it is more likely that adjoining counties will be affected (e.g. Devon and Cornwall).

2.4: REVIEW OF CURRENT ANALYSIS OF INFRASTRUCTURE SYSTEMS

It has already been established that the UK Government has identified nine categories of national infrastructure, into which each individual system can be placed (Figure 2.1) (with the scope of this thesis limiting this to four categories: communications, water, energy and transportation) and it has also been established that infrastructure systems serve our communities by facilitating a flow of service from areas where it is stored or generated (e.g. power stations) to areas of demand (e.g. communities).

This flow of service is governed by 'rules' which can differ between infrastructure systems. For example, the flow of service around many communications networks is governed by 'logistical' rules (including the postal system). However, many other systems are governed by more complex 'physically based' rules and are traditionally analysed using physically based models (sometimes referred to as deterministic, comprehensive or process-based models). These models attempt to represent the physical processes displayed by these real world systems (for example modelling the flow of water around a water distribution system or the flow of electricity around a power grid). In the case of a water system these models can contain representations of surface runoff, channel flow and evapotranspiration.

A detailed explanation of these models is outside the scope of this thesis; the reader is directed to Sallam and Malik (2011), Alexander and Sadiku (2009) and Pansini (2005) for a detailed explanation of power grids, Osiadacz (1987) for gas pipeline networks and Novak et al. (2010) for water distribution systems. However, a conceptual overview of the main components in four 'physically based' systems is given in Table 2.5.

Table 2.5: Showing the conceptual components of four different network models.

Network	Flow	Driver	Resistance	Earth	Thermodynamic Constraint	Eqn. to Solve
Simple Spring Model	Force	External Forces	Spring Stiffness	Support Reactions	Compatibility of Nodal Displacements	F = kd
Water Distribution System	Fluid	Pressure Head	Pipe Friction	Reservoir	Head Loss	$HL = kQ^2$
Power Grid	Electricity	Potential Difference	Impedance	Generator	Voltage Drop	V = IR
Transport	Vehicles	Destination	Vehicle Density	Origin	Travel Time	-

These physically based models are useful at providing scenario based information; for example, many studies have used hydraulic models to analyse the flow of contaminants around a water distribution system. In one such study, Grayman (2006) introduced a contaminate into the water distribution system, shown in Figure 2.13, from the river source and analysed how this contaminate propagated through the system over time. This physically based model can give detailed information regarding the concentration of this contaminate at different points in the system for a range of time periods (Figure 2.14 shows an example of this).

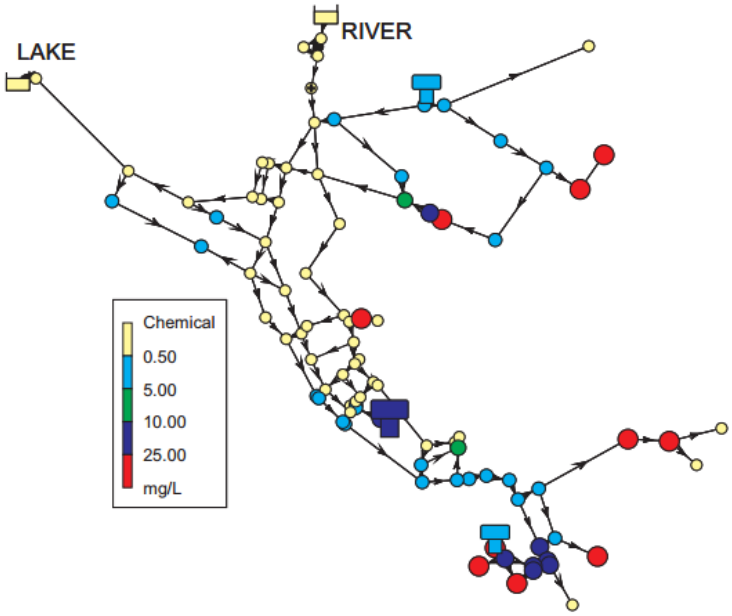


Figure 2.13: A hydraulic network showing the concentration of a chemical 15 hours after it was injected into the system at the river source (Grayman 2006).

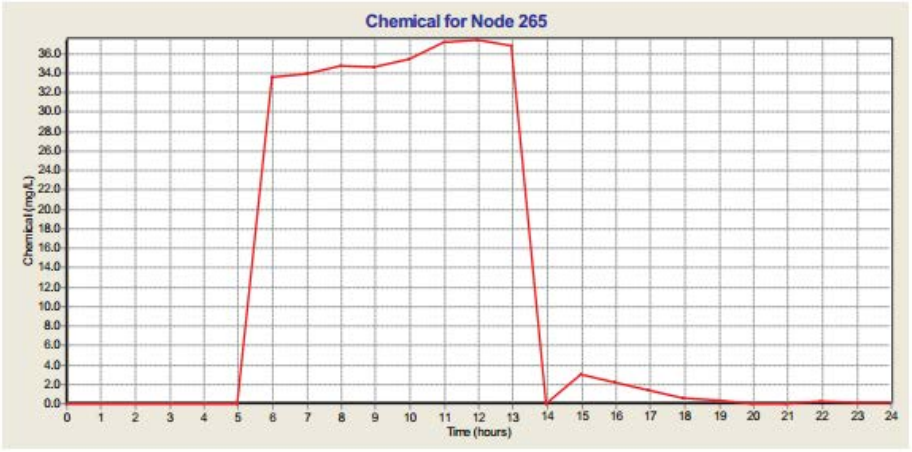


Figure 2.14: The temporal variation of the chemical used to contaminate the hydraulic network shown in at node 265 (located in the centre of the system) (Grayman 2006).

With regard to resilience, these models can also be used to analyse the potential reduction in water supply to customers due to a burst water main, for example. However due to their complexity, physically based models can become too large to be solved and can only provide information regarding the resilience of the system for chosen scenarios, potentially leaving our communities vulnerable to unforeseen events. These models are also lacking when used to identify critical components in the system. For example, if an electrical distribution system consists of 1,000 transmission towers and an assessment is needed to determine the impact of the removal of 10 of these towers at random then the analysis is fairly straightforward. However, if the analysis

asked which of these 10 transmission towers, if removed from the system, would cause the most customers to lose power, the analysis becomes much more complicated (the number of possible combinations/simulations to be analysed is 2.63e23). Therefore, to solve this problem and to provide confidence that the system will be able to provide at least a baseline level of service to untested scenarios another analysis approach is needed.

2.5: NETWORK GRAPH THEORY

Network graph theory has previously been used to model the complex interactions between components in social systems (Amaral et al. 2000; Newman et al. 2002; Arenas et al. 2003), neural networks (Sporns 2002; Stam and Reijneveld 2007; Bullmore and Sporns 2009), biological networks (Rual et al. 2005) and in computer science (Valverde and Solé 2003). During these studies many advances in this field have been made, the most notable of which include the discovery of different network classes and the identification of the hazard tolerance of these classes. This sub-chapter aims to give an overview of these notable discoveries as well as their recent application to model the complex interactions in infrastructure systems.

Network graph theory can find its roots in Euler's solution of the Konigsberg bridge problem, in 1735 (Newman 2003; Glendinning 2012). The problem asked whether it was possible to tour the town, crossing each bridge only once (Figure 2.15(a)). Previous mathematicians, using only trial and error methods, showed that this was clearly very difficult; however, it was not until 1735 when it was proved to be impossible by Euler. His solution imagined each of the four 'islands' as a point (or vertex), connected using links (or edges) to model the bridges, thereby removing the geographical distraction (Figure 2.15(b)). To cross each bridge only once, there must be nodes with both an odd and even number of connected links present in the network. However, in this example there are only nodes with an odd number of links, making (and proving) the problem impossible to solve.

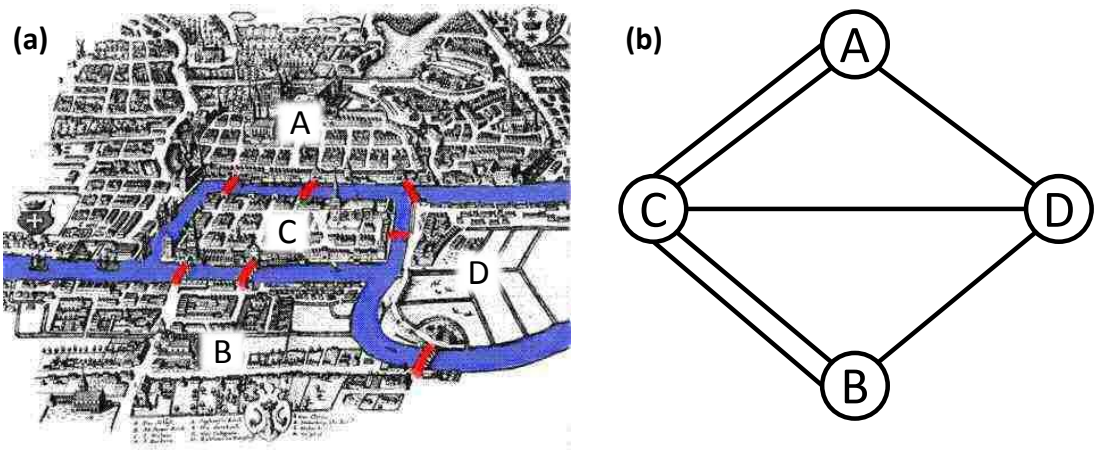


Figure 2.15: (a) A map representing the Konigsberg Bridge Problem (Paoletti 2013) and (b) a graphical representation of the problem, where the letters have been used in each image to indicate corresponding 'islands'.

Another notable problem solved by applying network graph theory is the four colour problem (Thomas 1998). This problem dates back to 1852 and arose when Francis Guthrie noticed that four colours were sufficient to colour the map of the counties of England, whilst ensuring that adjacent regions (those that share a boundary and not just a point) were different colours. Guthrie then wondered if any map can be coloured using only four colours. There were many unsuccessful 'proofs' to the problem and was not until graph theory was used to solve the problem, using the states of the US (Figure 2.16(a)), that a successful proof was formed. This approach represented the capital of each state (or an arbitrary point inside that state) and joined the capitals of every pair of neighbouring states (Figure 2.16(b)). This makes it fairly straightforward to assign each capital a colour or number (from 1 to 4) ensuring that connected capitals do not share the same colour / number.

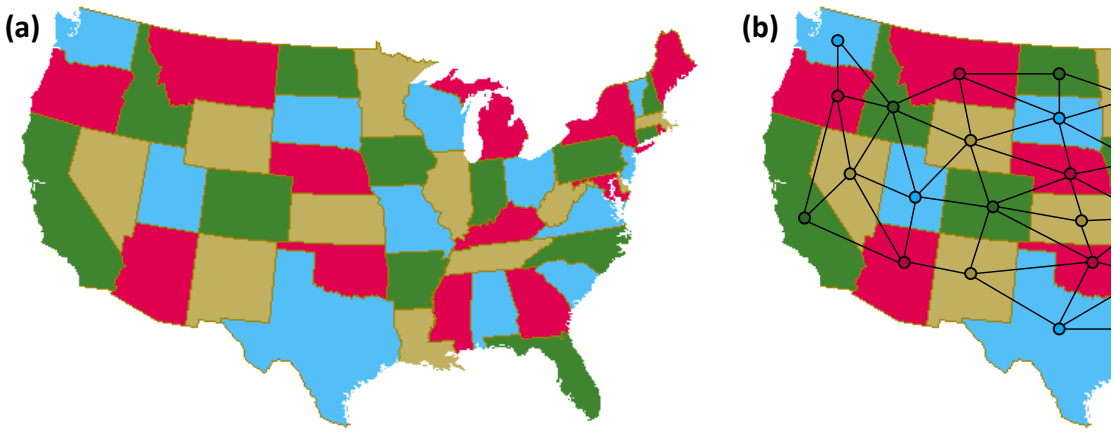


Figure 2.16: Showing (a) the Four Colour Theorem (Robertson et al. 2007) and (b) the network used to construct the proof of the solution.

The theory and application of network graph theory has '*experienced a tremendous growth in the last decade*' (Zanin and Lillo 2013) and is seemingly driven by a realisation that certain parts of networks are important. Therefore, the primary research focus has been on understanding why the connections between components establish themselves resulting in complex systems with specific architectures (or network classes).

2.5.1: TYPES OF NETWORK CLASSES AND NETWORK MODELLING

The first network model developed was the random graph model (Erdos and Renyi 1960) and has since been followed by the small-world network (Watts and Strogatz 1998), the scale-free network (Barabasi and Albert 1999) and most recently the exponential network (Liu and Tang 2005). Each of these network models has different evolutionary rules for attaching links between pairs of nodes, resulting in networks with different architectures (i.e. different arrangements of the links between nodes in the network). The development of these different network models has been fundamentally driven by the desire to form a better understanding of real world networks (e.g. the Internet, social networks). It could be considered that the major contribution of network theory, to the analysis of real world networks, is its ability to describe generic properties of a network and in so doing give an indication of the behaviour of seemingly different systems. Today, many real world networks can be classified into one of these four main network classes.

Each class of network can be differentiated by its degree distribution (for example Figure 2.17(b)). It is this distribution that allows for the distinction between different classes of network and also defines the inherent hazard tolerance of the network. Figure 2.17(a) shows part of a scale-free network, and indicates the degree of each node, which is equal to the number of links attached to it (for example, if a node has 3 links attached to it, then it has a degree of 3). The degree distribution of the network, P(k), gives the cumulative probability that a selected node has k or greater links. P(k) is calculated by summing the number of nodes with k = 1, 2, … links divided by the total number of nodes in the network. The degree distribution for the scale-free network (partly shown in Figure 2.17(a)) is shown in Figure 2.17(b).

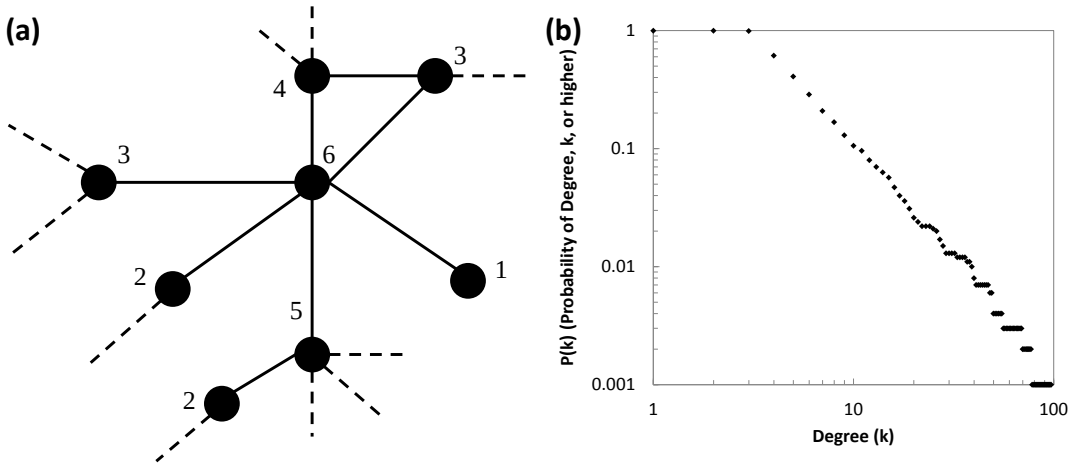


Figure 2.17: Showing (a) part of a larger 100 node scale-free network (generated using Network Workbench (NWB Team 2006)) and (b) the degree distribution for the same network (which forms a straight line on a log-log graph). The black dots in (a) represent the nodes and the black lines the connections between the nodes shown. The dashed lines represent links to nodes that have not been shown for clarity and the number beside each node indicates its degree (i.e. 2 indicates that a node has two links attached to it). The degree distribution for this network has been obtained using the method outlined in the text.

The first developed network model was the Erdos and Renyi random graph model (Erdos and Renyi 1960), which is arguably the simplest graph possible (Albert and Barabasi 2002). This class of network has been shown to be a poor representation of most real world network architectures (Newman 2003); however, random graphs are useful and are normally used as a baseline for comparison with more structured networks (Lewis 2009). An example of this can be found in tests for network robustness presented in Batagelj and Brandes (2005). Figure 2.18 shows a sample random network and its associated degree distribution. It can be seen from this distribution that all nodes in random networks tend to be attached to the same number of links (i.e. a homogeneous network), which can be confirmed visually by inspecting the network (Figure 2.18 (a)).

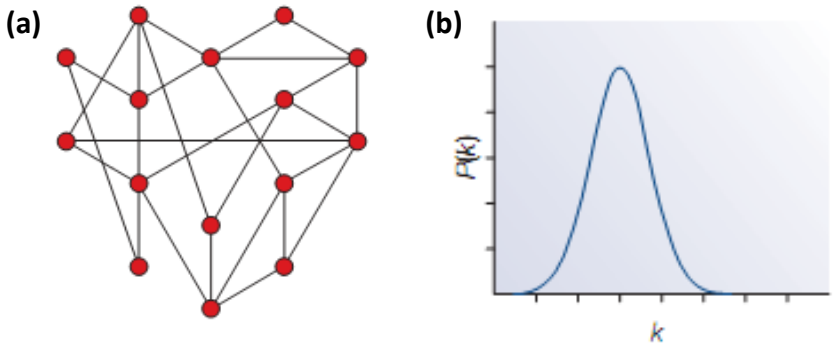


Figure 2.18: (a) A sample random network and (b) its degree distribution, where P(k) in this figure is not cumulative (Barabasi and Oltvai 2004).

To more accurately model real world systems and to acknowledge that real world networks '*are neither completely ordered nor completely random, but rather exhibit important properties of both'* (Watts 2004) Watts and Strogatz modified the random graph model by using the concept of 'six degrees of freedom' (Milgram 1967) forming 'small-world' networks (Watts and Strogatz 1998). The main characteristic of small-world networks is that the majority of nodal pairs are not directly connected, but can be reached via very few links. The degree distribution is very similar to that of a random network (Figure 2.18(b)) (Barthelemy 2011). In recent years, the small-world network has been considered to be more of a network characteristic rather than a network class in its own right, and is characterised by a high clustering coefficient and a short average path length (Latora and Marchiori 2002). Many networks have been shown to belong to one of the other three network classes but possess these small-world characteristics (da Rocha 2009).

Both the random graph model and the small-world network are characterised by a Poisson degree distribution (Network Workbench 2009). However, Barabasi and Albert discovered that real world networks (including, the Internet (Albert et al. 2000) and the World-Wide-Web (Barabasi and Albert 1999; Barabasi et al. 2000)) tend to form a power law degree distribution. Networks that follow this power law are more commonly known as scale-free networks. These scale-free networks include a small number of highly connected nodes (nodes with a high degree) and a large number of poorly connected nodes (nodes with a small degree). This can be seen visually in the sample network shown in Figure 2.19(a) and by the associated degree distribution in Figure 2.19(b).

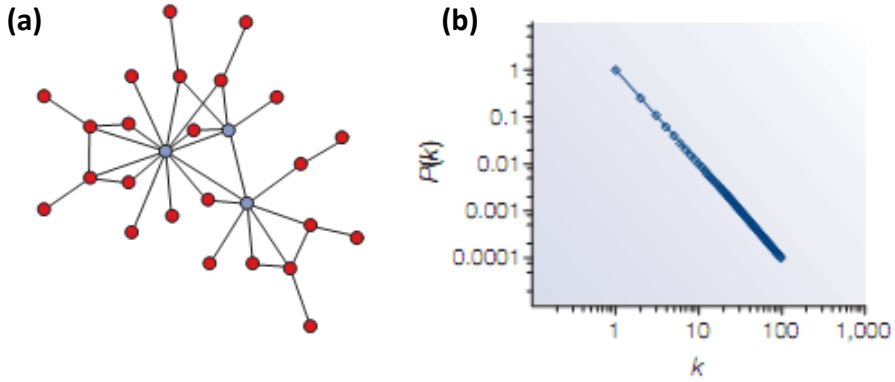


Figure 2.19: (a) A sample scale-free network and (b) its degree distribution, where P(k) in this figure is cumulative. It can be seen from the degree distribution in (b) that a scale-free network forms a straight line on a log-log graph (Barabasi and Oltvai 2004).

Other real world networks, such as power grids, have been found to have an exponential degree distribution (i.e. their degree distribution forms a straight line when plotted on a log-linear scale) and so can be classed as exponential networks (Liu and Tang 2005). The origins of exponential networks are unclear and no one individual (or group) appears to be cited with their discovery; however, they have been used in many studies of real world networks including those by, Albert et al. (2004), Amaral et al. (2000) and Bompard et al. (2011). The degree distribution for a real world exponential network (the North American Power Grid) is shown in Figure 2.20.

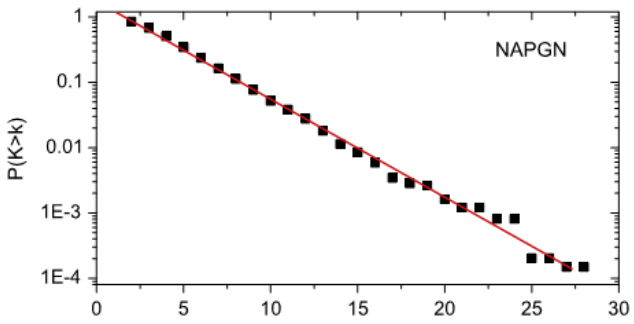


Figure 2.20: Degree distribution for the North American Power Grid, a real world exponential network (Deng et al. 2011). Note that for an exponential network this distribution forms a straight line when plotted on a log-linear scale.

2.5.2: NETWORK GENERATION ALGORITHMS

Each of these different network classes has a different set of 'rules' that govern the formation of links between pairs of nodes in the network. It is these 'rules' that determine the overall structure of the network, which can be seen in the degree

distribution. This section outlines the network generation algorithms used to form the network classes introduced in the previous sub-section.

2.5.2.1: RANDOM NETWORKS

The network generation algorithm for random networks is possibly the simplest of all the network models. The network starts with the total number of nodes and each pair of nodes is considered in turn and a connection (link) is made between them based upon the value of linking probability, L (the higher this value the more likely it is that a link will be generated) (Erdos and Renyi 1960). If the linking probability is equal to 1, then the network will be fully 'saturated' (i.e. all nodal pairs will be connected and the network will include the maximum possible number of links) and if this value is equal to 0 then no links will be formed between nodal pairs. It is possible to have isolated nodes in the network (nodes that are not connected to any others in the network) using this network generation algorithm; this usually occurs when the value of linking probability is close to 0. Figure 2.21 shows five random networks (generated using Network Workbench (NWB Team 2006)) which were all generated with a different value of linking probability. From this figure it can be seen visually that the higher the linking probability the higher the number of nodes in the network. Two isolated nodes, resulting from a low value of linking probability, can also be seen in the network generated with a linking probability equal to 0.1.

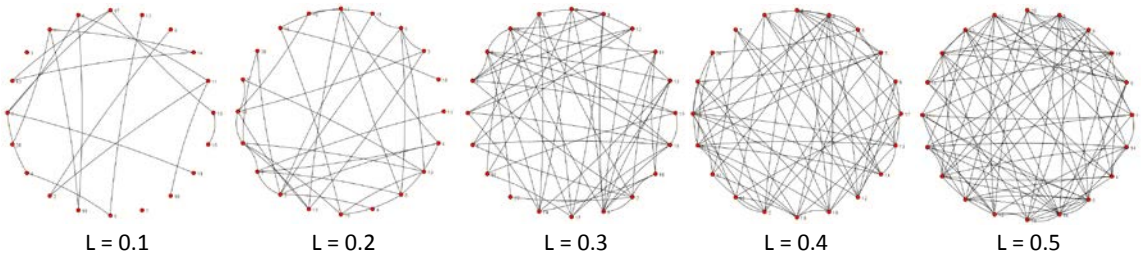


Figure 2.21: Five random networks, generated using Network Workbench (NWB Team 2006), with different values of linking probability (L).

2.5.2.2: SMALL-WORLD NETWORKS

In a similar manner to the random network model, the generation algorithm for small-world networks starts with the total number of nodes in the network; although, these nodes are connected (via links) to a given number of initial neighbours. It is the number of initial neighbours which determines the total number of links in the network (as no new links are added as the network is formed). For example, for a network with 20 nodes and a number of initial neighbours as 2, there will be 40 links in the network (as each node starts with two links to its initial neighbours). These initial links are then 'rewired' using a rewiring probability, the higher the value of this probability the higher the number of links that are rewired. Figure 2.22 shows the effects of the rewiring probability, p. For p = 0 no links are rewired and the resulting network is regular in structure and for p = 1 all links are rewired, resulting in a random network.

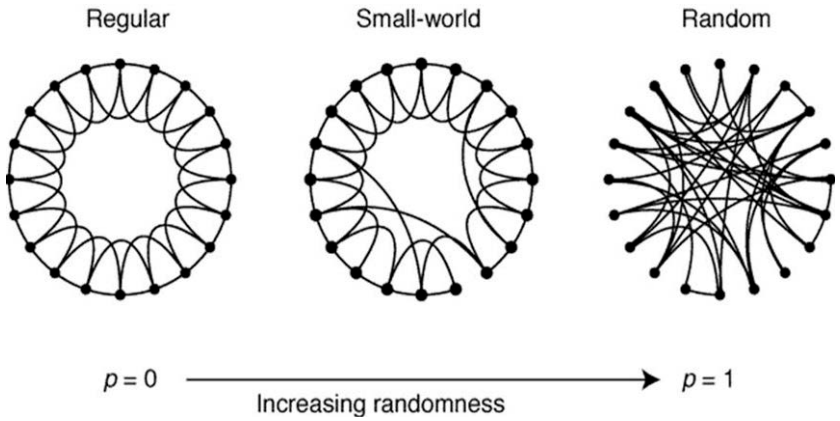


Figure 2.22: Showing the effects of the rewiring probability (p) in the small-world generation algorithm (Watts and Strogatz 1998).

2.5.2.3: SCALE-FREE NETWORKS

The generation algorithm for the Barabasi and Albert (1999) scale-free network is significantly different to that of the random and small-world networks and is based upon the ideas of *growth* and *preferential attachment* (Boccaletti et al. 2006). These networks are formed by starting with an initial number of isolated nodes, m_0 (usually a small percentage of the total number of nodes in the network). New nodes are then added to the network at each 'timestep' (i.e. 'growing' the network) until the total number of nodes in the network is reached. These added nodes have between 1 and

m_0 links attached to them and attach to the existing nodes in the network based upon the idea of *preferential attachment*. The probability of attaching to each existing node is calculated based upon its degree, where the nodes with a high degree are more likely to 'attract' a link from the new node (i.e. the rich get richer). It is this 'preferential attachment' rule which results in a few high degree nodes and many small degree nodes in the network. Figure 2.23 shows this idea of preferentially attachment using part of a scale-free network, previously shown in Figure 2.17(a). In this figure, the introduced node at the current 'timestep' is shown in red and it is assumed that this node will only introduce one link to the network.

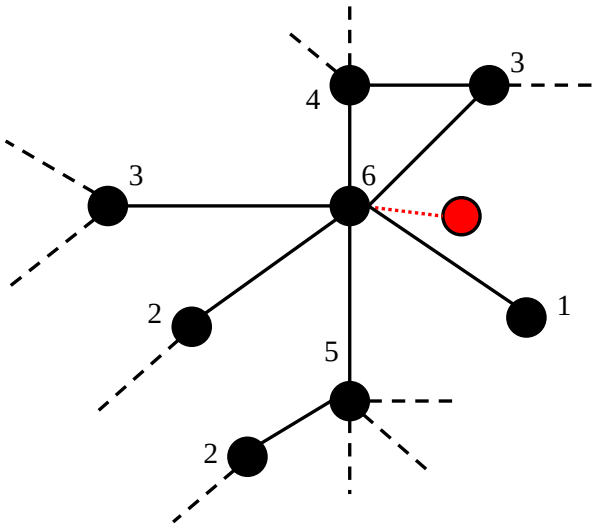


Figure 2.23: Demonstrating the idea of *preferential attachment* using the section of the scale-free network shown in Figure 2.17(a). The black dots show the nodes that already form part of the network and the red dot shows the new node that has been added at this 'timetep'. This new node is likely to preferentially attach to the node with the highest degree in the network (the node with a degree of 6). This is shown by the presence of a new link (red dashed line). It is worth noting that this node is assumed to only introduce one new link to the network.

One implication from this network generation algorithm is that nodes that are introduced early in the process have more chance to attract links from introduced nodes and therefore tend to be those that have a higher degree when the network is fully formed (i.e. it has finished 'growing'). However, for many real world networks shown to have a scale-free topology this is not the case. For example, in the case of the World-Wide-Web many newly introduced nodes, such as Google, Facebook and Twitter, have a very high degree. To accommodate this phenomenon, Barabasi introduced the idea of *fitness* to the network generation algorithm (Barabasi 2013). The *fitness* is used to alter the probability of attachment of a selection of nodes that are introduced to the network (Cohen and Havlin 2010). Therefore, the probability Π_i

that the node introduced at the current 'timestep' connects one of its links to a node which is already present in the network not only depends upon its degree, but also on the fitness of the node, such that (Bianconi and Barabasi 2001a; Bianconi and Barabasi 2001b):

$$\Pi_i = \frac{\eta_i k_i}{\sum_l \eta_l k_l} \qquad 2.2$$

Where, *k* is the degree of a node, η is its fitness and the subscripts *i* and *l* refer to a node already present in the network and all nodes in the network, respectively.

Incorporating this idea into the network model explains the presence of some highly connected nodes that are introduced to the network at a later 'timestep'. The growth of nodes over time is now controlled by the fitness component and this provides the competition in networks (the nodes with a higher value of fitness will tend to 'win out' and become very highly connected (Barabasi 2013)).

2.5.2.4: EXPONENTIAL NETWORKS

This network class is not as well documented as the other three classes and few network generation algorithms exist for forming exponential networks, none of which have been validated by forming proxies for real world networks. However, Liu and Tang (2005) propose a model based upon the Barabasi-Albert scale-free network (including the ideas of *growth* and *preferential attachment*). In their model, the network starts with a small number of fully connected nodes (m_0). At each 'timestep' a new node is introduced to the network with a number of links between 1 and m_0 (which continues until all nodes have been added to the network). The idea of preferential attachment is still used to connect to existing nodes to the network; however, this is modified so that the probability of attachment is not based upon the degree of the existing node but is instead based on the degree of the connected nodes (to this node). Meaning that a node with a low degree can still 'attract' links from new nodes if it is connected to existing high degree nodes.

2.5.3: HAZARD TOLERANCE OF NETWORK ARCHITECTURES AND FAILURE MODES

The hazard tolerance of these network classes has been well documented in previous tests of network resilience. It is the different arrangement of links (nodal connectivity) in each network class that determines the hazard tolerance. There are two main topological 'attack strategies' which are used in these resilience tests to determine the order in which nodes (and their connecting links) are removed from the network: *random node failure* and *targeted attack*. The random node failure attack strategy removes nodes at random from the network, whilst the targeted attack strategy removes nodes based on their degree (highest to lowest). It is worth noting that both of these hazard strategies use binary damage models (i.e. nodes cannot operate at a reduced capacity). The majority of studies quantify the hazard tolerance of a network by quantifying the proportion of links removed for a given proportion of nodes removed (Albert et al. 2000).

Previous studies have shown that the random network shows the same hazard tolerance to both of these attack strategies. This is due to the homogeneous nature of the network (i.e. all of the nodes have approximately the same degree); therefore each node has approximately the same impact to the network when removed (Albert et al. 2000; Magnien et al. 2011). For this reason, random networks are often used as a benchmark for resilience in tests of network robustness to determine if a more structured network is resilient or vulnerable to the applied hazard (Lewis 2009). This benchmark random network is generated with an equal number of nodes and links as the more structured test network and is subjected to the same hazard. The results for both networks are then compared by plotting the proportion of nodes and the proportion of links removed. If the test network has a smaller proportion of removed links for the same proportion of removed nodes the network is classed as resilient (to the applied hazard) and if a higher percentage of links is removed the network is classed as vulnerable (to the applied hazard).

In contrast to random networks, scale-free networks show a different hazard tolerance to these two topological attack strategies, due to the different connectivity of nodes (or arrangement of links) in the network. They have been shown to be resilient to random hazard and vulnerable to targeted attack (Albert et al. 2000; Barabasi and Bonabeau 2003). This is due to the inhomogeneous nature of scale-free networks,

meaning that they consist of a few high degree nodes and many smaller degree nodes (Figure 2.19). The random failure attack strategy has a high chance of removing one of the many small degree nodes from the network; whereas the targeted attack strategy will remove the higher degree nodes first, seeking to cause the maximum disruption to the network. Figure 2.24 shows a scale-free network subjected to the random hazard and targeted attack strategies (Barabasi and Bonabeau 2003). From this figure it can be seen visually that the random node failure attack strategy removes fewer links than the targeted attack strategy.

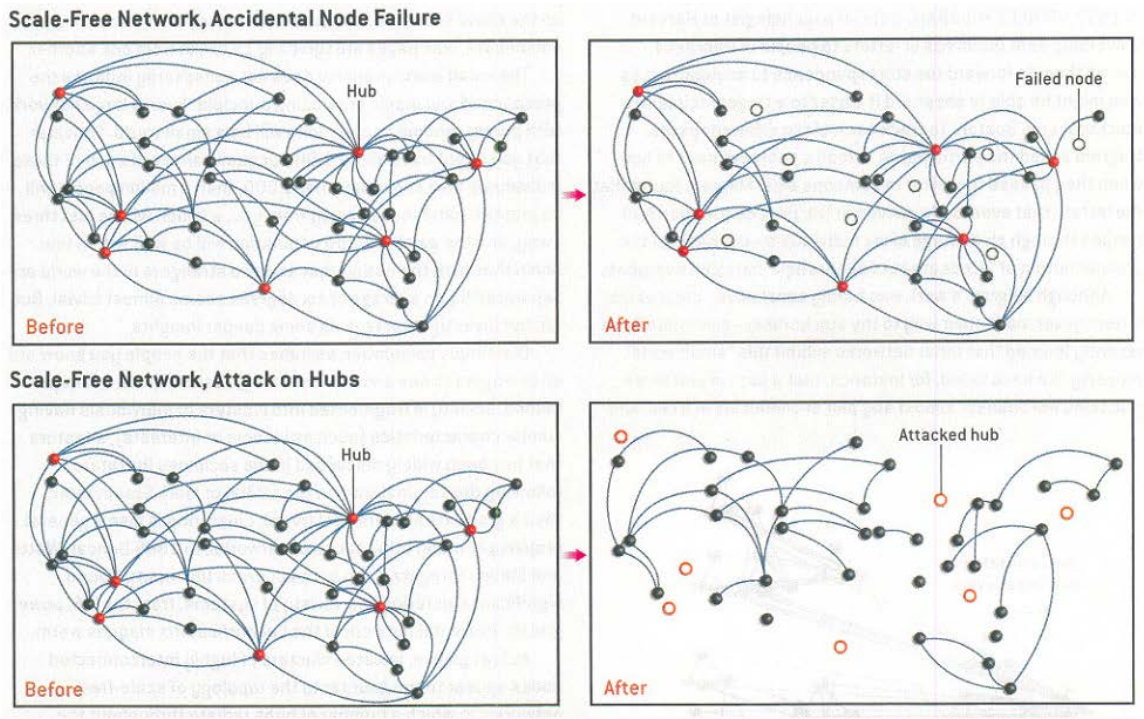


Figure 2.24: Showing a scale-free network (representing the US air traffic network) subjected to the random node failure and targeted attack strategies (Barabasi and Bonabeau 2003).

Exponential networks show similar resilience as the scale-free networks to these two attack strategies (Rosas-Casals et al. 2006). As such, this network class is resilient to random hazard (due to the large number of low degree nodes) and vulnerable to targeted attack (as this attack will focus on the removal of the few highly connected nodes).

2.5.4: NETWORK MEASURES

The hazard tolerance of networks is usually determined by quantifying the proportion of nodes and links removed by an attack strategy; however, other network measures can also be used to quantify change in connectivity and/or performance or to identify 'important' nodes in networks.

2.5.4.1: CONNECTIVITY MEASURES

There are numerous graph theory measures that can be used to describe, and quantify, the connectivity of a network as it becomes degraded and breaks into smaller clusters (where a cluster is a group of nodes connected via links) when subjected to hazards. The most commonly used connectivity measures are the maximum cluster size (MCS), number of clusters (NC) and the number of isolated nodes (NIN).

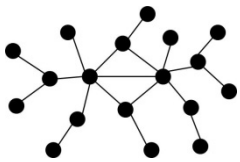
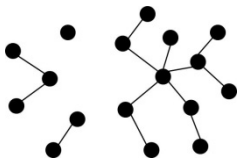
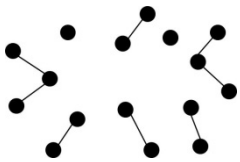
The MCS of a network is defined as the total number of nodes in the largest cluster of the network (Nojima 2006) and for a network that is not fragmented this value is equal to the total number of nodes in the network. For a fragmented system this measure gives an indication of how many nodes can still be reached via links within the largest remaining component.

The NC can be used to quantify the number of clusters, which contain two or more connected nodes, in a fragmented network (Nojima 2006). For a fully connected network (i.e. one that is not fragmented) this value is equal to 1. For an infrastructure system, this measure states how many clusters the network has broken into and can be used to give an indication of the repair time, and resources, needed to fully connect the fragmented system (for example, the time taken to connect a small NC is likely to be shorter than the time taken to connect a large NC).

The NIN is used to quantify the number of isolated nodes (i.e. nodes that do not have any connections to other nodes in the network), but does not include the number of nodes that have been removed from the network by the attack strategy (Nojima 2006). For a fragmented infrastructure system, this measure gives an indication how many components have become entirely unconnected from the rest of the system and, if demand components, will receive no supply of resource.

A sample network has been created to show how these three measures changes when two nodes are removed (Table 2.6). It can be seen that the MCS decreases as nodes are removed from the network, indicating that the size of the largest component in the network becomes smaller and that it is no longer possible to reach every node in the network from any other node. Whilst, the NIN and NC both indicate that the network has fragmented and give an indication of exactly how fragmented the network has become (the larger these values the more 'fragments' the network has broken in and therefore the more difficult it may be to reconnect the network).

Table 2.6: An example network showing how the number of links, maximum cluster size (MCS), number of clusters (NC) and number of isolated nodes (NIN) changes when nodes are removed from the network. This work has been modified from a similar example by Nojima (2006) and edited for clarity.

			
Number of nodes removed	0	1	2
Number of links	19	13	8
Maximum Cluster Size (MCS)	18	11	3
Number of Clusters (NC)	1	3	6
Number of Isolated Nodes (NIN)	0	1	2

These measures are used in many tests of network resilience to quantify the fragmentation of a network when it is subjected to an applied hazard (for example see: Nojima (2006) and Albert et al. (2000)) and could be applied to infrastructure networks to indicate how they fragment, if at all, when subjected to hazard. However, they cannot be used to quantify the proportion of communities without service (e.g. these measures cannot identify which clusters contain supply components), nor can they be used to give an indication of the efficiency of the fragmented system.

2.5.4.2: PERFORMANCE MEASURES

There are many graph theory measures that can be used to quantify different aspects of network performance, of these measures there are two that are commonly used: shortest average path length (APL) and diameter (D).

The shortest APL of a network captures the concept of efficiency in a network (Boccaletti et al. 2006) and is defined as the average number of steps along the shortest path between all pairs of nodes a network (Barthelemy 2011). The higher the value of APL the more inefficient the network (as on average there are more links between each pair of nodes). If the network is fragmented then this value is calculated using the largest connected component (i.e. the largest cluster). The equation used to calculate the APL is (Boccaletti et al. 2006):

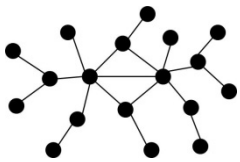
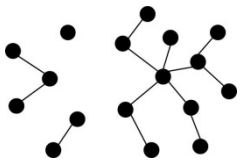
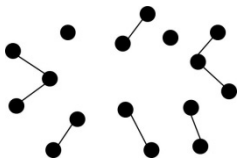
$$L = \frac{1}{N(N-1)} \sum_{i,j \epsilon N, i \neq 1} d_{ij} \qquad 2.3$$

Where, *L* is the shortest APL of the network, *N* is the total number of nodes and d_{ij} is the shortest path between node *i* and node *j*.

D is the maximum shortest path length in the network (Newman 2003) and '*characterises the ability of two nodes to communicate with each other*' (Albert et al. 2000). Similarly to the APL, if the network is fragmented, then this value is calculated using the largest connected component (Nojima 2006).

In a similar manner to the connectivity measures, the change in APL and D has been calculated for the same sample network (with the same two nodes removed) (Table 2.7). From this table, it can be seen that both the APL and D decrease as the network is degraded, this is because the network has broken into clusters and therefore both of these measures are no longer valid measures of efficiency (Nojima 2006). This indicates the problem with using these measures, particularly without using them in conjunction with connectivity measures (to establish whether the network has fragmented). In a larger network is it likely that these values will initially increase, indicating that the network is becoming increasingly inefficient, before dramatically decreasing, indicating a 'tipping point'.

Table 2.7: One example network showing how the number of links, average path length (APL) and diameter (D) changes when nodes are removed from the network.

			
Number of nodes removed	0	1	2
Number of links	19	13	8
Average Path Length (APL)	2.95	2.42	1.20
Diameter (D)	6	4	2

In a similar manner to the connectivity measures, these measures have previously been used in tests of network resilience (see Nojima (2006)). In terms of an infrastructure system these measures could be used to give an insight into the efficiency of the system (its ability to transfer service from areas of supply to areas of demand) and how this efficiency may change when the network is subjected to hazard.

2.5.4.3: IMPORTANCE MEASURES

Many studies consider the highest degree node to be the most 'important' to the network (Bagler 2008), that is the node that plays a large role in the complex interactions and communication between other nodes in the network (Cadini et al. 2009). However, other studies have tried to develop more sophisticated measures of establishing the importance of nodes, rather than just using degree. The most widely used of these measures are centrality measures: betweenness and closeness centrality. Unlike the previous connectivity and performance measures, in which the outputs concern the whole network, these importance measures give an output for each node (or a component if applied to an infrastructure system).

The betweenness centrality of a node (Equation 2.4) is the proportion of all shortest average path lengths between pairs of other nodes that include this node (Freeman 1979; de Nooy et al. 2005) and is based on the concept that central nodes are included on the shortest average path length of pairs of other nodes (de Nooy et al. 2005).

$$C_i^B = \frac{1}{(N-1)(N-2)} \sum_{j,k \epsilon G, j \neq k \neq i} \frac{n_{jk}(i)}{n_{jk}} \quad 2.4$$

Where, n_{jk} is the number of shortest paths between *j* and *k*, and $n_{jk}(i)$ is the number of shortest paths between *j* and *k* that contain node *i* (Crucitti et al. 2006).

The closeness centrality (Equation 2.5) is defined as the mean shortest path between that node and all other nodes reachable from it (nodes that tend to have a small shortest path length between other nodes in the network have a higher value of closeness) (Freeman 1979; de Nooy et al. 2005) and comprises the idea of speed of communication between pairs of nodes in a network (de Nooy et al. 2005; Cadini et al. 2009).

$$C_i^C = \frac{N-1}{\sum_{j \epsilon G, j \neq i} d_{ij}} \quad 2.5$$

Where, d_{ij} is the shortest path length between *i* and *j* (Crucitti et al. 2006).

These measures were developed for the analysis of social networks, to identify the important figure in a group of people or organisation, for example, studies using these measures include: Everett and Borgatti (1999) and Rothenberg et al. (1995). However, they have recently been applied to infrastructure systems, to show that nodes with a high degree do not necessarily have a high value of centrality (and are not necessarily 'important' to the network) and vice versa.

In one such study, Guida and Maria (2007) compared the degree of a node with its betweenness centrality, for the Italian air traffic network and a random network, with the same number of nodes and links (Figure 2.25). They found that in the air traffic network (black squares) nodes with a high degree tended to have a high value of betweenness centrality, but that there were several nodes that did not conform to this arrangement. These nodes (airports) tended to have a value of betweenness centrality lower than other nodes with the same value of degree. This is in contrast to the random network (grey circles) where there is a clear correlation between these two measures. Another study by Guimera et al. (2005) confirmed this variable relationship between the betweenness centrality and degree of a node in an air traffic network, using the worldwide air traffic network as an example Figure 2.26(a). In their study, Guimera et al. (2005) used nodes to represent cities that included one, or more,

airports and formed a connection between them if they were connected by at least one direct flight. This is in contrast to Guida and Maria (2007) who used nodes to represent individual airports and links to represent their connecting air routes.

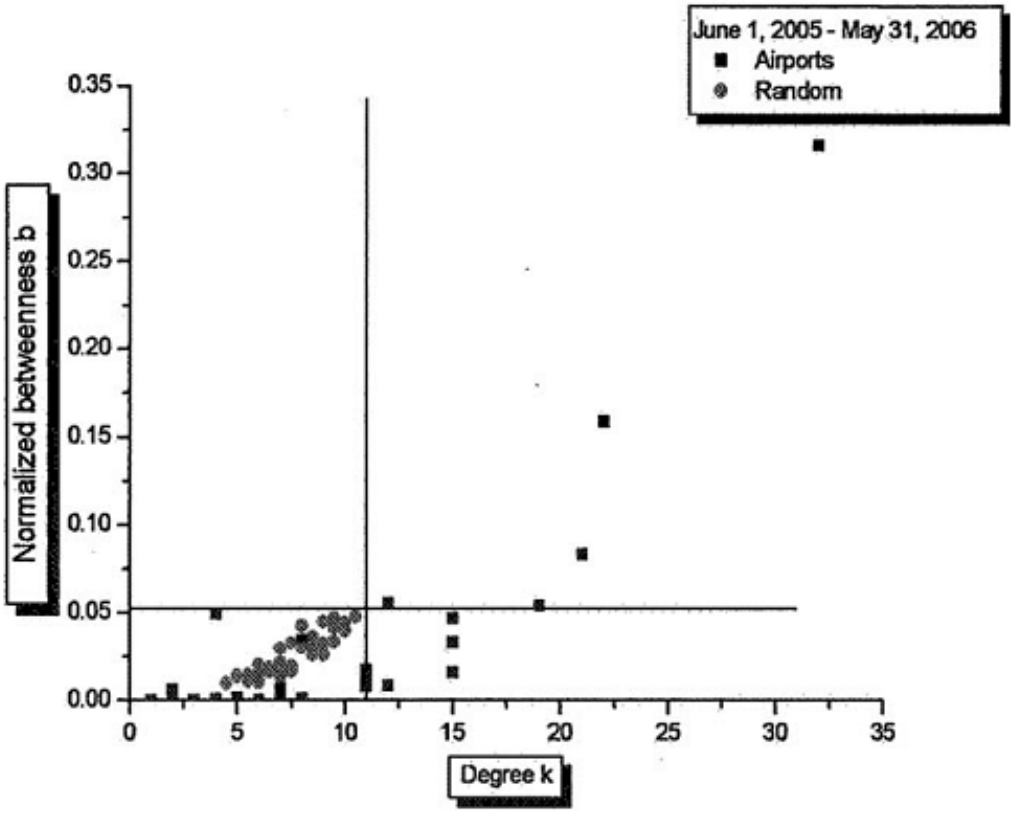


Figure 2.25: Plotting the normalised betweeness and degree of a node for the Italian air traffic network (black squares) and a random network (grey circles) (Guida and Maria 2007).

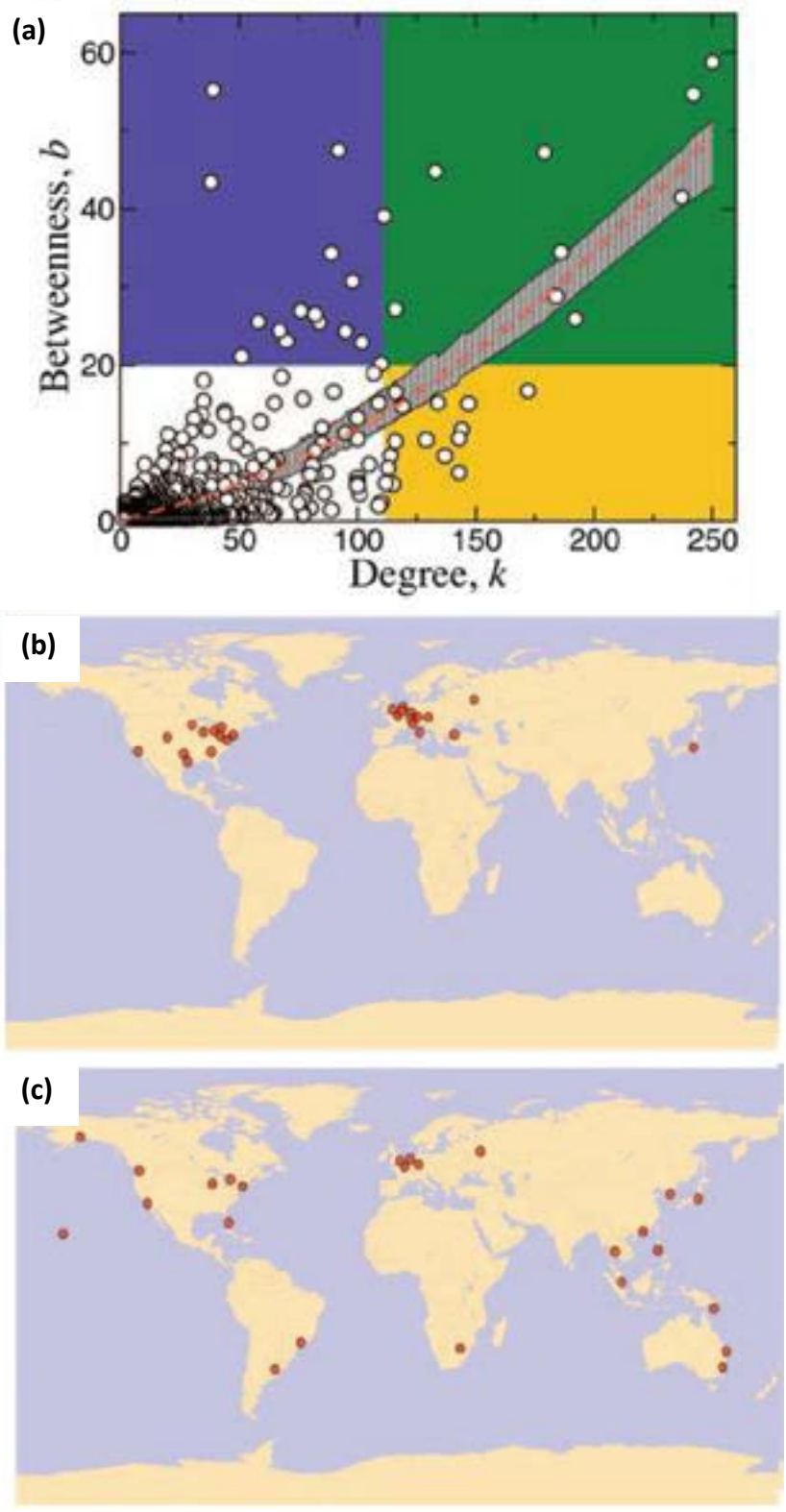


Figure 2.26: (a) Plotting the betweenness centrality of a node with its degree (circles) for the worldwide air traffic network. This figure also shows the relationship for a random network, where 95% of the data falls inside the grey region. Also showing the location of 25 cities that have the highest (b) degree and (c) betweenness centrality (Guimera et al. 2005).

In Figure 2.26(a) the blue region of the graph contains the 25 most central cities (those with the highest value of betweenness centrality) and the yellow region contains the 25 most connected cities (i.e. those with the largest degree). The green and white regions are formed by finding the intersection of the blue and yellow regions. Guimera et al. (2005) found that, surprisingly, there are only a few cities with large betweenness and degree (green region). This is a contrast with the random network (grey region) which shows a distinct relationship between these two parameters (similar to the results achieve by Guida and Maria (2007), Figure 2.25). Guimera et al. (2005) also plotted the geographic location of the 25 most central and connected cities (Figure 2.26(b, c)). These plots show that the most highly connected cities are located around Europe and the USA, whereas there appears to be an even spread of central cities, with a slight cluster around central Europe. This location of highly connected cities within two small geographic areas could be due to the regulation of flights in countries, passenger demand or due to political constraints, however, the authors of the paper do not give any clear reasons for this distribution.

To demonstrate how a node can have a high betweenness centrality and a low degree a sample network has been created (Figure 2.27). In this network, it can be seen that the red node is on a large number of shortest paths between pairs of other nodes (and is also critical in transferring flow between the input and output nodes) and has a small degree (it is only connected to two other nodes). This high betweenness and low degree is shown by the airport in Hawaii and is an example of how space can impact the characteristics of the network, as this airport was used to refuel aircraft en route from US to Asia/Australia before the advent of long range aircraft.

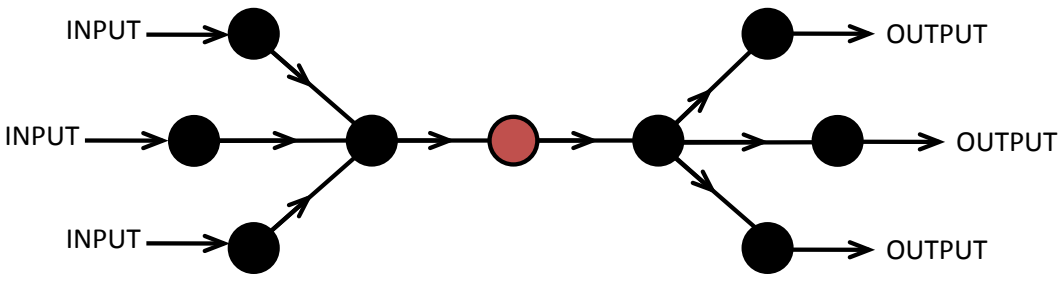


Figure 2.27: An example of how a node can have a high value of betweenness centrality and a low degree. In this example, the red node will have a high betweenness centrality, as it is one the shortest path of many other nodes in the network, and a low degree, as it only has two connecting nodes.

Therefore, it can be concluded that in air traffic networks there are some nodes which may act as a 'transfer' node for flights from one region to another. This appears to be more common on a larger scale (i.e. between countries) rather than on a smaller scale (i.e. in one country) and could be crucial when considering the hazard tolerance of these networks (as the removal of these 'transfer' nodes could result in the network breaking into clusters quickly).

This relationship (between node degree and betweenness centrality) has also been considered in other types of infrastructure network, including electrical distribution systems (Figure 2.28). These studies have also found that there does not appear to be a direct relationship between the degree of a node and its betweenness centrality value. Therefore, it can be concluded that in many real world networks, there are nodes which do not have a high value of degree, and could be dismissed as 'unimportant' but may have a high value of centrality and could therefore be critical to the functioning of the network.

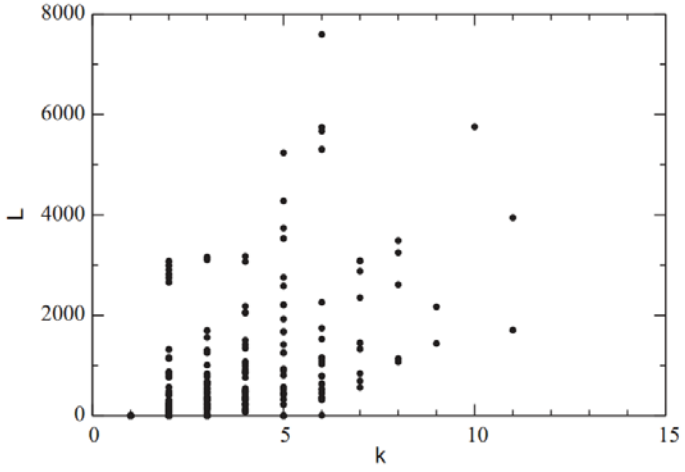


Figure 2.28: Plotting the degree of a node (k) with its betweenness (L) for the Italian electrical distribution network (Crucitti et al. 2004b).

Centrality measures have also been used to rank the importance of components in an infrastructure system (Cadini et al. 2009); again finding that nodes with a high degree do not necessarily have a high betweenness centrality and vice versa. However, the majority of previous research has either focused on the relationship between degree and centrality or has ranked the critical components (using the measures) but has not used this information to determine whether removing nodes based on their value of degree or centrality has the most devastating effect to the network (in terms of a

targeted attack). It is therefore unclear as to whether centrality measures are more sophisticated and accurate measures of determining critical nodes in a real world network.

To summarise, there are various measures in network theory that can be used to either give an indication of how the properties of a network change when subjected to hazard or to indicate which components are likely to be important to the functioning of a network. However, these measures can be deficient; for example, the MCS, which is the number of nodes in the largest cluster, gives an indication of how fragmented the network has become by a hazard, but does not indicate how inefficient this network has become. To achieve this, performance measures, such as the APL, must be applied. However, this measure is deficient in that it can show an increase in the efficiency of a network which has been 'damaged' by hazard. Therefore, to consider the degradation of the network when subjected to hazard, both of these measures must be used in combination. Whilst, other measures indicate the importance of a node to the functioning of a network, their validity has not been tested by removing these nodes to gauge their impact to the remaining network.

2.6: PREVIOUS APPLICATIONS OF GRAPH THEORY TO SOCIAL AND OTHER NETWORKS

Social networks were among the first real world networks to be analysed using network graph theory and indeed many measures and network classes were developed for the analysis of these networks. In these models nodes are used to model a person, or group of people, and the links used to connect the people who are acquaintances, work colleagues, friends, for example. This research began in the mid-1930s but was limited by the technical tools available to analyse these networks. As the sophistication of these technical tools increased so did the size and complexity of the networks analysed (Carrington et al. 2005). The studies in this area tend to be data-orientated and involve the investigation of a real world network to determine its structure and the centrality or influence of the various connected parties (Newman et al. 2002). The studies in this area have included the analysis of collaborations between scientists (Newman et al. 2002), musicians (Costa et al. 2011) and actors (Amaral et al. 2000), to name but a few. These studies have many important implications for the

understanding of real world systems; for example in the analysis of actor networks it was found that the '*distribution of actors' degrees is highly skewed*' (Newman et al. 2002), where a small number of actors have a disproportionately large numbers of ties. It has been shown, through simulations and analysis, that this skewness may impact on the way in which communities operate in terms of the way information flows around the network and the robustness of the network when these highly connected actors are removed.

Since the early application of network graph theory to social networks, many other real world networks have been analysed using this method. These studies have included the analysis of biomolecular systems in medicine (Lee et al. 2008), food webs in ecological systems (Dunne et al. 2002) and the study of interactions in the brain in neuroscience (Sporns 2002). In these studies, the network models are constructed, formed of nodes and links, and are analysed to determine the characteristics of the network. This normally includes an initial assessment of the network by defining its network class (gaining an insight into the connectivity and hazard tolerance of the network), before applying network metrics to identify the most important nodes in the network or the efficiency of the system (either under normal operational conditions or in the event of a hazard scenario). For example, in their study Lee et al. (2008) applied network theory to systematically map links between diseases, finding that this approach can help to uncover some critical disease comorbidities and can explain their metabolic origin. They concluded that this approach offers an *"increasingly potent tool to explore and understand the interplay between cellular networks and human diseases*" (Lee et al. 2008). Sporns (2002) also successfully applied network theory to the analysis of brain interactions, concluding that "*network analysis may be the key to understanding and harnessing the remarkable computational and informational power of the brain*". In recent years, the analysis of real world networks has turned to consider the potential applying network graph theory to characterise and analyse infrastructure systems.

2.7: APPLICATION OF GRAPH THEORY TO INFRASTRUCTURE NETWORKS

Network graph theory has previously been used to analyse a wide range of infrastructure systems, including: highway networks (Jenelius et al. 2006; Boas et al. 2009), subway networks (Latora and Marchiori 2002), railways (Sen et al. 2003), gas networks (Carvalho et al. 2009) and water distribution systems (Yazdani and Jeffrey 2012). However, the research in this area has tended to focus on the breadth of systems that can be studied rather than the depth in which these systems can be analysed. For example, the vast majority of studies only classify the topological characteristics of these systems (e.g. identify the degree distribution of the system) and do not assess their hazard tolerance. As a result of the breadth of research in this area there are few studies which expand upon previously published work, with the majority of studies preferring to study a 'new' system.

This sub-section will present and discuss previous research relating to the four national infrastructure sectors included in the scope of this thesis (due to the breadth of research in this area it is not possible to give an overview of all types of analysed infrastructure systems).

2.7.1: COMMUNICATION NETWORKS

The World-Wide Web and the Internet were two of the first studied real world infrastructure systems using network graph theory. The World-Wide Web was first studied by Albert et al. (1999) who reported the network to exhibit their recently discovered scale-free degree distribution (Barabasi and Albert 1999). This network classification was later confirmed by Pastor-Satorras et al. (2001), who furthered the original study to consider how the Internet changed with time.

Since the classification of the Internet, a few studies have sought to confirm whether its hazard tolerance is the same as that shown by its network class (to random and targeted topological hazards). The hazard tolerance of the Internet is speculated in a study by Tu (2000) and actually proved by Cohen et al. (2000). Cohen et al. (2000) subjected a network model of the Internet to a series of random attacks (removing nodes randomly) and found that the network showed a surprising level of resilience to

this attack strategy, characteristic of scale-free networks. In a later study, Cohen et al. (2001) subjected the same network to a targeted attack (removing nodes in order of degree, highest to lowest) and found that the network showed an increased vulnerability to this attack strategy (compared to the random attack strategy), again characteristic of scale-free networks. One further study by Albert et al. (2000) also considered the hazard tolerance of the Internet and the World-Wide Web, but furthered the studies of Cohen et al. (2000) and Cohen et al. (2001) by comparing this hazard tolerance to generated scale-free and random networks. All four networks were subjected to a topological random and targeted attack and their resilience to these hazards quantified by applying network measures.

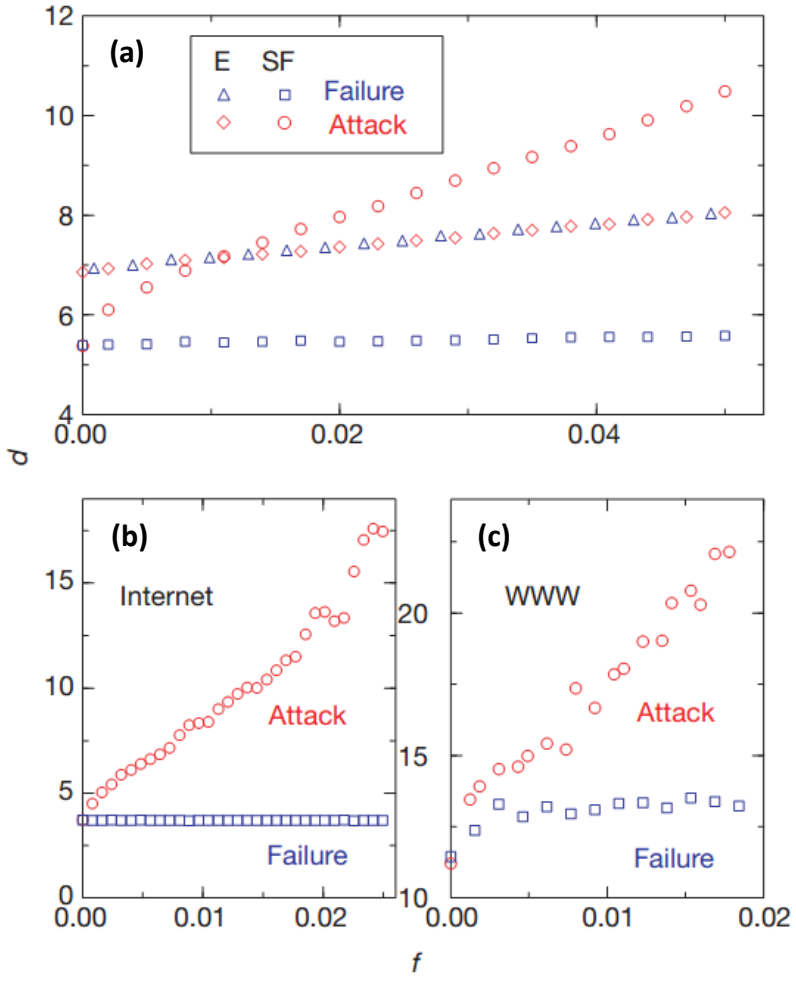


Figure 2.29: The changes in the diameter, d, of the network as a function of the fraction (f) of the removed nodes, for networks subjected to a targeted and random failure attack strategies. (a) Shows a comparison between a random network and a scale-free network, generated using the network generation algorithms of Erdos and Renyi (1960) and Barabasi and Albert (1999). Also showing the changes to the diameter of the (b) Internet and (c) World-Wide-Web (Albert et al. 2000).

In their study, Albert et al. (2000) initially compared the diameter of the scale-free network to the random benchmark network, for a given fraction of nodes removed, to determine if the scale-free network was resilient or vulnerable to the applied hazard (Figure 2.29(a)). From these results, it can be seen that the scale-free network becomes less efficient more quickly to the targeted attack strategy than the random attack strategy (as indicated by the higher value of diameter); whereas, the random network shows the same response to both attack strategies. The results for the Internet and the World-Wide Web have been shown in Figure 2.29(b, c) and show that these scale-free networks have a similar hazard tolerance as the synthetic scale-free network shown in Figure 2.29(a). Albert et al. (2000) also plotted the fraction of removed nodes against the relative size of the largest cluster in the network and the average size of the isolated clusters for all four of these networks. This comparison again showed that the random network showed the same hazard tolerance to both attack strategies and that the scale-free network showed an increased vulnerability to the targeted attack strategy. Both the Internet and the World-Wide Web showed the same level of resilience to these attack strategies as the scale-free network, further confirming that they show the hazard tolerance which is characteristic of their network class.

2.7.2: ELECTRICAL DISTRIBUTION NETWORKS (POWER GRIDS)

In a graph theory model of an electrical distribution system nodes are used to represent a combination of generators and distribution substations and links are used to represent the transmission lines connecting these nodes (Crucitti et al. 2004b). It could be assumed that nodes would also be used to represent transmission towers; however, many studies model these systems over a wide geographic region (most commonly over a whole country) and therefore do not model these systems in such high detail (Albert et al. 2004; Sole et al. 2008).

Almost all electrical distribution networks have been shown to follow an exponential degree distribution; including the Italian network (Crucitti et al. 2004b), North American (Albert et al. 2004; Kinney et al. 2005), Western USA (Holmgren 2006), Nordic (Holmgren 2006) and European (Holmgren 2006) networks. Therefore, these

networks comprise a small number of high degree nodes and a large number of smaller degree nodes. Two examples of an electrical distribution network have been shown in Figure 2.30 (for the UK and Italy) along with their associated degree distributions.

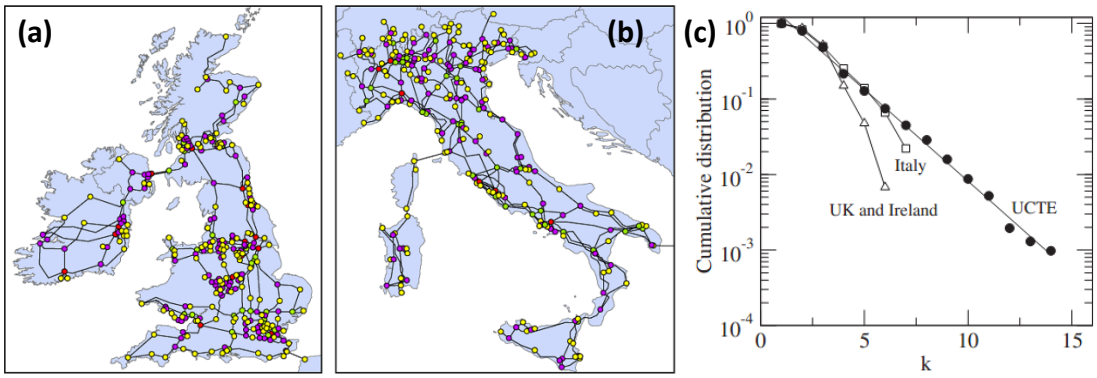


Figure 2.30: The electrical distribution network for (a) the United Kingdom and (b) Italy and (c) the degree distribution for both of these networks and the European power grid (UCTE) (Rosas-Casals et al. 2006).

In the analysis of electrical distribution systems, many studies incorporate an element of flow into the network model. This is achieved either by coupling the model with a physically-based model or by forming an estimate of the flow by using the betweenness centrality network measure (Equation 2.2). The reasoning behind the use of this graph theory metric is that flow will tend to travel along the most direct path (i.e. the path of least resistance) and the betweenness centrality measure is concerned with the most direct path between two nodes and therefore many studies reason that this measure can be used as a proxy for a more complex and computationally demanding physically-based model (Albert et al. 2004; Baldick et al. 2009).

Similar to other network models, the hazard tolerance of electrical distribution systems has been assessed in many studies using the random and targeted topological attack strategies. However, many of these studies also consider the 'flow' element in the system and additionally consider 'cascading failures'. A cascading failure is caused by a redistribution of load when a single, or group, of nodes, or links, are removed from a network (Crucitti et al. 2004a). An example of a cascading failure can be seen in Figure 2.31; in this example it can be seen that the removal of a single node can cause

the failure of many others in the network and, in this case, can lead to the system being unable to supply the required level of service.

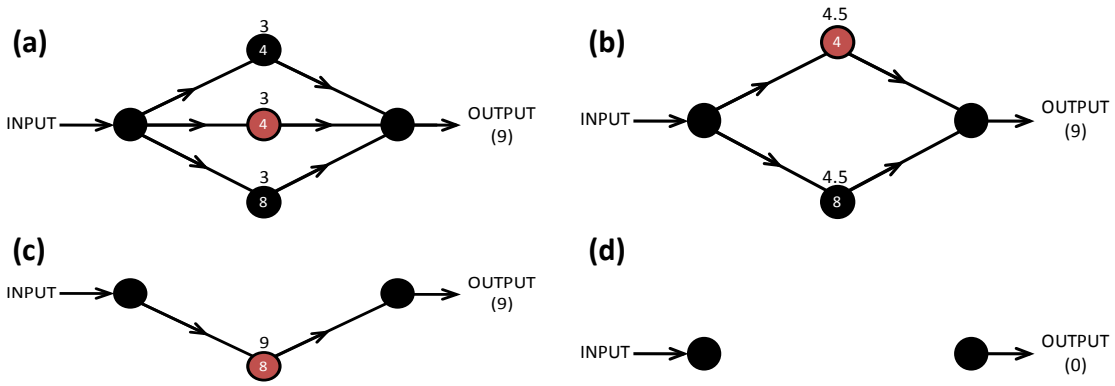


Figure 2.31: Showing a cascading failure in a sample network, which has one generator node, one demand node and three distributor nodes. In this sample network it is assumed that each node and link has the same resistance and that each link has infinite capacity. (a) Shows the original network, where the direction of flow is indicated by the arrows (on the links), the capacity of each distributor node is shown in white on the node and the flow through each node is shown in black above the node. To initiate a cascading failure the middle distributor node is removed (shown in red in (a)). The removal of this node causes the flow to be redistributed throughout the network (b). This redistribution of flow causes one of the other distributor nodes to fail, as the amount of flow trying to pass through the node is greater than its capacity. The failure of this node results in the network shown in (c) and the resulting redistribution of flow causes the remaining distributor node to be overcapacity and fail. It is worth noting that in this example only the capacity of the nodes was considered. It is likely that in many real world networks the links will also have a fixed level of capacity which, if exceeded, would cause them to fail.

A study by Albert et al. (2004) showed how damaging a cascading failure to an electrical distribution network can be, using the North American power grid as an example. In their study, the network model consisted of 14,099 nodes (representing 1633 power plants, providing a service, 2179 distributing substations, requiring a service, and 10287 transmission substations, distributing the service) and 19,657 links (representing transmission lines); the flow (or load) through each node was calculated using the betweenness centrality of the node. To assess the hazard tolerance of their network model, Albert et al. (2004) subjected the network to four different attack strategies, removing transmission nodes: randomly (random), in decreasing order of degree (degree-based) or load (load-based) and to simulate a cascading failure they removed the 10 nodes with the highest load and then recalculated the load and removed the 10 nodes with the next highest load, until all nodes were removed (cascading failure). The results of this analysis are shown in Figure 2.32 and are presented in terms of the percentage of connectivity loss (C_L) and the fraction of transmission nodes removed (f_t).

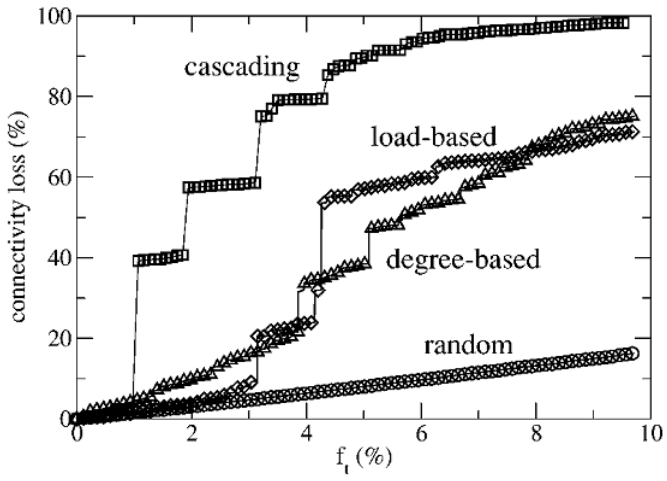


Figure 2.32: Connectivity loss in the North American power grid due to the removal of nodes, using one of four different algorithms: randomly (circles), in decreasing order of the node degree (triangles) or load (diamonds), and by recalculating the load every ten steps and removing the ten nodes with the highest load (squares).

Albert et al. (2004) define the 'damage' to the network caused by the removal of nodes using their measure of C_L (connectivity loss), given in Equation 2.6, rather than using a more 'traditional' graph theory metric. In this equation, N_g refers to the generators and N^i_g to the distribution substations and *i* is used to refer to a specific substation. Essentially, C_L measures the '*decrease of the ability of the distribution substations to receive power from the generators*' (Albert et al. 2004) and is expressed as a percentage.

$$C_L = 1 - \langle \frac{N_g^i}{N_g} \rangle_i \qquad 2.6$$

From the results of the analysis (Figure 2.32), it can be seen that the cascading failure is the most damaging to the network, as it causes the highest connectivity loss for the same fraction of transmission substations removed as the other three attack strategies. It can also be seen that the network shows the most resilience to the random attack strategy, which can be expected when considering its exponential network class. It can be determined from these results that this network is more vulnerable to a cascading failure than to a degree based attack (to which this network should be most vulnerable to when considering the degree distribution of this network). This is because of the inclusion of a flow component into the analysis and the redistribution of this flow when nodes are removed from the network causing additional nodes to fail as they become overcapacity.

There are numerous other studies which assess the hazard tolerance of electrical distribution networks by initiating cascading failures and in a similar manner to Albert et al. (2004) they find that this attack strategy is the most damaging to this type of infrastructure system (Baldick et al. 2009; Chang and Wu 2011).

2.7.3: TRANSPORT NETWORKS

The graph theory analysis approach has been applied to many different types of transport network, including: road networks, railways, subway systems and other forms of public transport network. For example, a study by Tu et al. (2013) identified *'the most vital elements of a [road] network for supporting transportation planning and management activities'*. They proposed a new index system to identify vital elements within a road network, based on the vulnerability index of Bulteau and Rubino (1997), which ranks the vulnerability of links between nodal pairs based on the topological structure of a network. They then applied this index system to rank the vulnerability of links in the Shanghai freeway network (Figure 2.33), finding that the link between nodes 8 and 9 was the most vulnerable (although this is not a direct link, but is via node 7). However, they did not remove this link to verify if it caused the most disruption to the remaining network. Tu et al. (2013) then considered new routes that could be added to the network to reduce this vulnerability (shown as dashed lines in Figure 2.33). After rerunning the index system, they found that the link between nodes 19 and 26 to be the most superior at reducing the vulnerability of the network. Tu et al. (2013) concluded that this method could be used by decision makers to compare different planning scenarios to reduce the vulnerability of road networks.

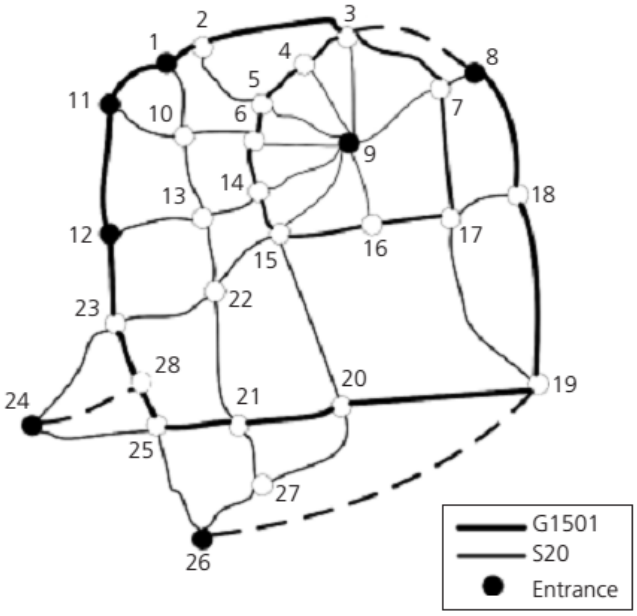


Figure 2.33: Showing the freeway network of Shanghai, consisting of 27 nodes and 49 links, where node 9 represents the centroid of Shanghai central city (Tu et al. 2013).

In a similar manner, Mathe et al. (2013) applied network theory to the analysis of Romania's railway network to determine the impact (in terms of journey time) that a new planned connection would make to travel around the network. To construct their model, Mathe et al. (2013) represented individual stations as nodes and the train links that connected them as links (Figure 2.34). They initially calculated the length of the journey from each station to all other stations in the network, finding that the total length of the network was 525,560km and also ranked the ease of access from each station to the rest of the network (finding that the Copsa Mica station had the greatest accessibility to all other stations). Mathe et al. (2013) then reanalysed the network including the new planned connection (between Targu Mures and Sighisoara) and found that the total distance necessary to travel through the entire network was shortened by 24,848km (a decrease of 4.7%). They also analysed how this planned line would affect the ease of access for each station in the network; for example, they calculated that the railway distance between Tirgu Mures and Brasov would decrease by 101km (an improvement of 79%). Mathe et al. (2013) concluded that this analysis could be used by planners to determine the impact that proposed connections would have to the functioning of the existing network.

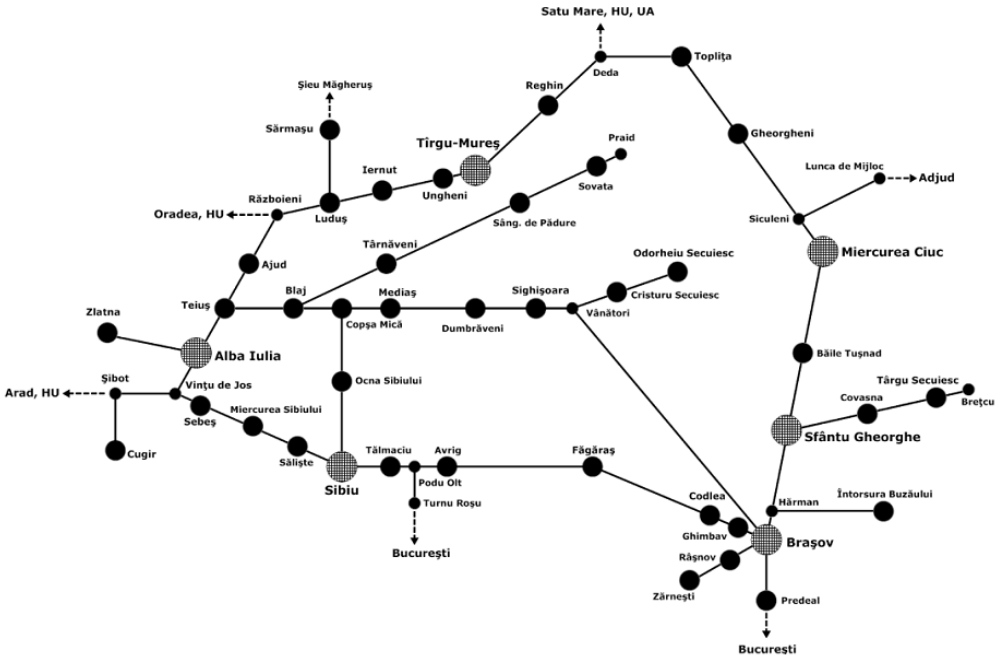


Figure 2.34: An image of the Romanian railway network (Mathe et al 2013).

However, within the infrastructure sector it is the analysis of air traffic networks which receives the most attention (in terms of the classification of network topology and analysis of characteristics). In these network models, nodes tend to be used to represent individual airports and links are used to show the presence of air routes. In some studies, the links are given a weighting to show the number of flights or passengers along a particular air route, for example, however, these studies will not be presented in this section as weighted networks are outside the scope of this research. Whereas, other studies consider a directed network, where the direction of a flight is included (determined by the origin and destination airports). Air traffic networks have also been studied on a variety of different scales, including country (Han et al. 2008; Zhang et al. 2010) and worldwide scales (Guimera and Amaral 2004). However, less considered is the hazard tolerance of these networks.

There has been much discussion as to the exact network class into which air traffic networks can be placed, with one study being devoted to this problem (Li et al. 2006). It has generally been concluded that air traffic networks possess a truncated scale-free distribution or a scale-free network with an exponential 'tail', including the Indian and Brazilian air traffic networks (shown in Figure 2.35). This type of infrastructure system does not fall wholly into one network class, but takes attributes from both the

exponential and scale-free network classes. They possess a small number of high degree nodes ('hub' airports) and a large number of smaller degree nodes.

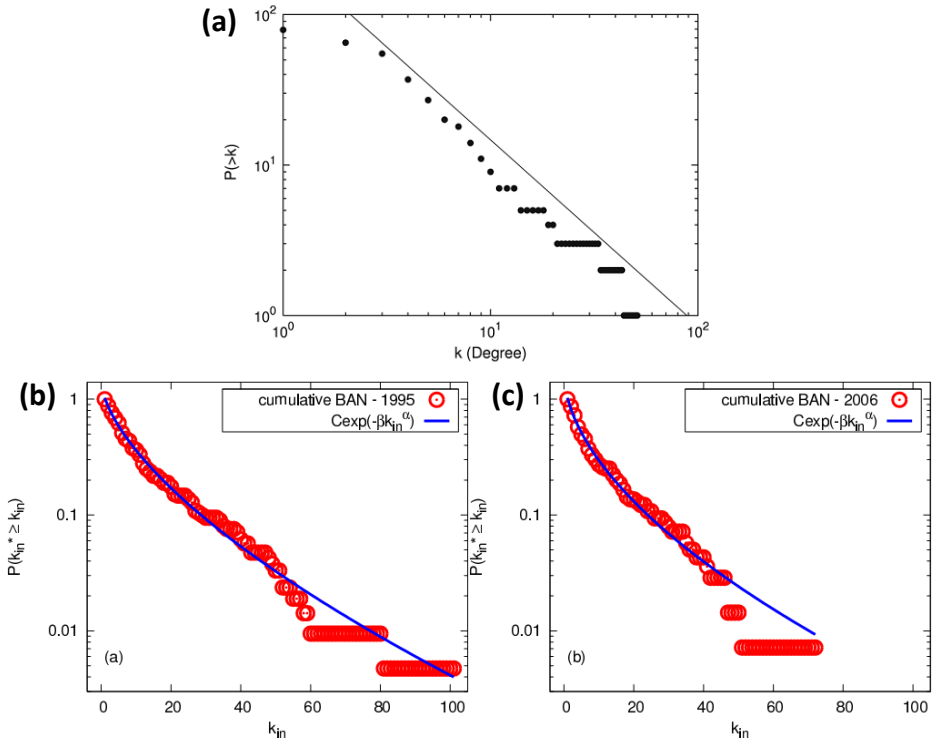


Figure 2.35: Showing degree distributions for the (a) Indian air traffic network, containing 79 nodes and 442 links (Bagler 2008) and the Brazilian air traffic network in (b) 1995 and (c) 2006 (da Rocha 2009). It is worth noting that these studies only consider the presence of an air route between two nodes in the network (i.e. intercontinental flights are not considered) and the networks are not weighted or directed.

Both of these studies considered the presence of an air route, irrespective of the season (as more flights can be expected in the summer to popular holiday destinations) and the day of the week. Whereas, Han et al. (2008) plotted the degree distribution of the Austrian air traffic network for different days during the week (Figure 2.36). This study classified a link as an individual flight rather than the presence of an air route between two airports and also considered the direction of flights in the network; therefore, altering the degree of each node to consider whether the flight was 'incoming' or 'outgoing'. The resulting degree distributions are very similar, and little differences can be observed between them. The incoming and outgoing flights for one particular day (Monday) are also plotted, enabling a direct comparison between these two variables to be made (Figure 2.36(c)). From this figure, it can also be seen that there is little change in the degree distribution obtained for the incoming and outgoing flights. However, due to the presentation of the distributions it is not possible to tell, visually, if the network forms a scale-free, exponential or truncated scale-free

distribution, this information is also lacking in the study literature. The classification of this network is also hampered due to the small network size, compared to other studies, consisting of only 134 airports and 9560 flights (for the whole week). Although, it can be determined from this study that the day of the week or the direction of flights does not noticeably alter the degree distribution and therefore the fundamental topological characteristics of the network.

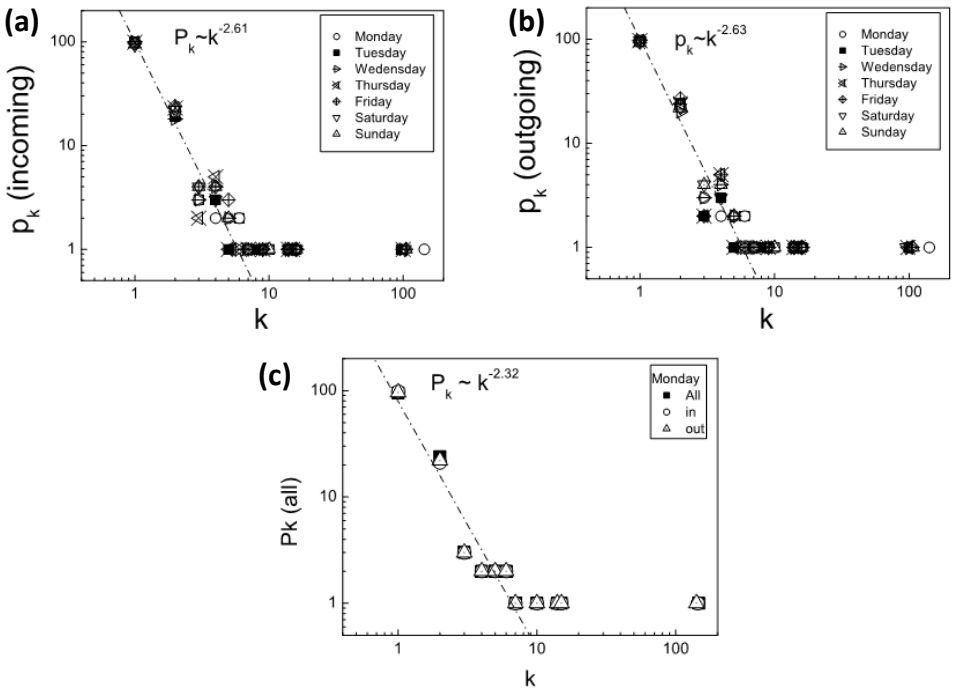


Figure 2.36: Degree distributions for each day of the week for the Austrian air traffic network, showing (a) all incoming flights, (b) all outgoing flights and (c) all flights on Monday (Han et al. 2008).

This work by Han et al. (2008) was taken a stage further by Zanin and Lillo (2013), who considered how the mean degree of each node (airport) changed depending on the day of the week. It is worth noting that this study did not separate flights from each airport into incoming and outgoing (i.e. it did not consider a directional network). In their study Zanin and Lillo (2013) found that the mean degree of an airport does change depending on the day of the week, being highest on a Monday and lowest on a Saturday. Although, it is worth noting that the change was only around 0.43 (approximating from the graph, Figure 2.37). The study also considered the Chinese air traffic network (Figure 2.37), finding that the spread in the mean degree of airports was greater for this network (with a change of approximately 2.3). Therefore, this analysis does confirm that the day of the week affects the topology of an air traffic

network; however, these changes are not consistent between networks and only result in small differences between the maximum and minimum mean degrees.

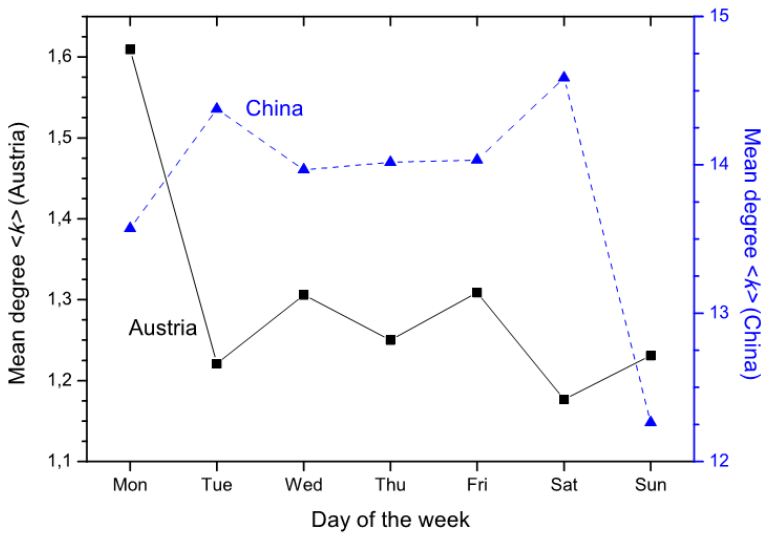


Figure 2.37: The change in the mean degree of airports in the Austrian and Chinese air traffic networks for different days of the week. The graph was obtained from (Zanin and Lillo 2013) and produced using the data of (Han et al. 2008) and (Li and Cai 2004).

Whilst, some studies have focused on assessing how the characteristics of an air traffic network changes with a relatively short space of time (e.g. different days of the week), other studies have assessed how these networks change over longer time periods (ranging from a few months to years). One such study, of the Brazilian air traffic network, has already been presented (Figure 2.35(b, c)) and considering these two degree distributions it can be seen that the overall classification of the network has not changed. However, it can be seen from these two distributions that the maximum degree node (i.e. the 'hub' airport) has reduced in size (in terms of the number of links) from just over 100 links to fewer than 80 links. It is also apparent that in 2006 there is only one 'hub' airport whilst there were two in 1995. There could be many reasons for this change, such as: higher operating costs at 'hub' airports, reduced airport capacity or introduction of 'budget' airlines, for example. This study does not make conclusions for this change and the network size (in terms of the number of nodes and links) is unclear and therefore conclusions regarding the decrease in network size cannot be independently made.

Another study, considering the change of air traffic networks over a long time period, focused on the Italian air traffic network (consisting of 42 nodes and 310 links). Guida

and Maria (2007) showed that this network formed a double power-law network, similar to the single power-law scale-free network developed by Barabasi and Albert (1999). This degree distribution is also similar to those shown by other air traffic networks. It can be seen from the degree distributions in Figure 2.38 that the overall classification of the network does not change for each of the three study time periods. Therefore, it can be concluded that air traffic networks show a truncated scale-free distribution, which is largely unchanging with time; so an air traffic network studied in 1995 should have the same characteristic network topology as that shown by the same air traffic network in 2005, for example.

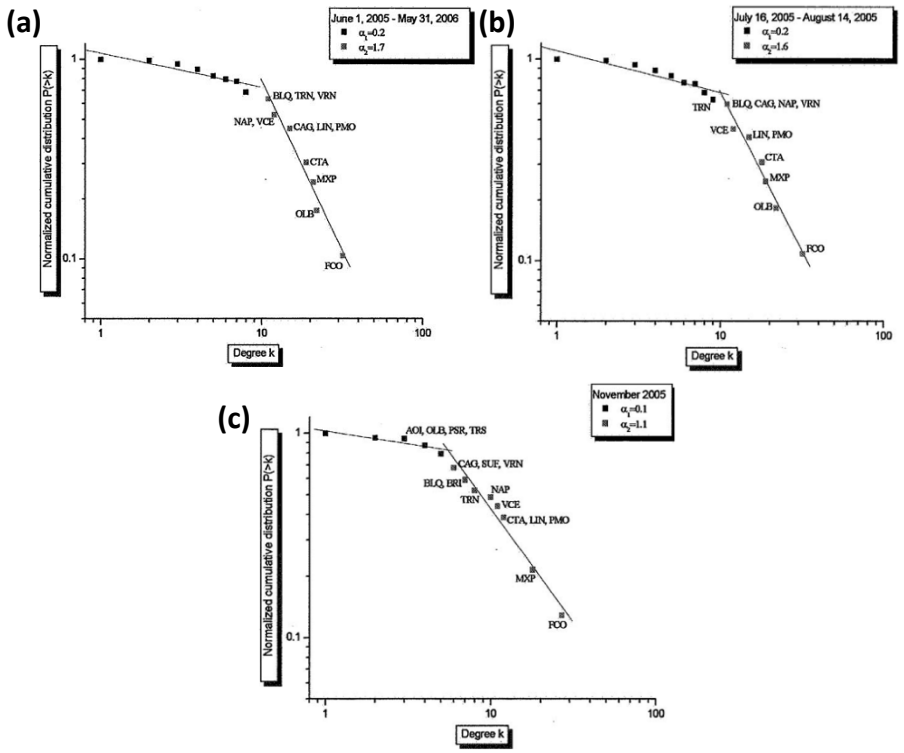


Figure 2.38: The degree distribution for the Italian air traffic network for three different times during the year (a) 1st June 2005 to 31st May 2006, (b) 16th July 2005 to 14th August 2005 and (c) November 2005 (Guida and Maria 2007).

In one further study, Guimera et al. (2005) analysed the properties of the wordwide air traffic network, initially showing that its degree distribution displayed a truncated power-law (Figure 2.39). In their study, they used nodes to represent cities and links to represent the air routes connecting these cities. They showed that the most connected airports are not necessarily the ones with the highest value of betweenness centrality, as previously discussed (see Figure 2.26).

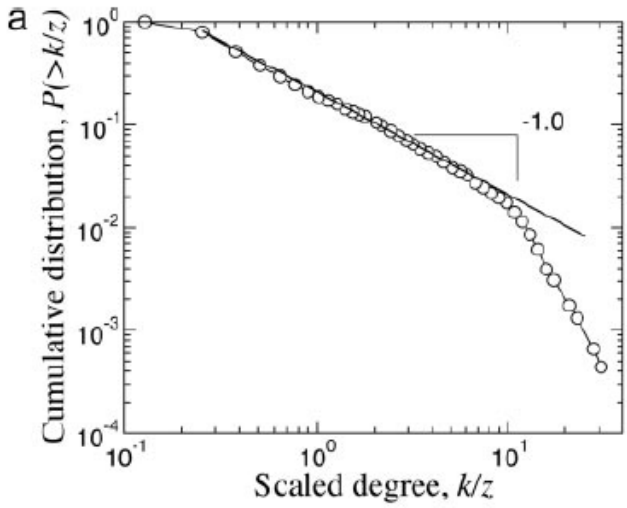


Figure 2.39: Showing the degree distribution of the worldwide air traffic network (Guimera et al. 2005).

2.7.4: WATER DISTRIBUTION SYSTEMS

Water distribution systems appear to receive the least attention, in terms of network graph theory analysis. This could be due, in part, to the lack of complete obtainable datasets for these systems as they are 'buried' infrastructure; however Yazdani and Jeffrey (2011) state that this may be due to "*the fact that purely topological graph-based techniques have limited scope as tools for reliability analysis of [water distribution systems]"*. For example, a study by Walski (1993) showed that a network theory approach does not account for the importance and location of the isolation values in the analysis of these systems and could therefore lead to inaccurate results. Although, Yazdani and Jeffrey (2011) do acknowledge that a network theory approach to analysing water distribution systems may be valid and that "*vulnerability and robustness of [water distribution systems] have not been systematically exposed to analysis by graph theory and complex network techniques*".

In their study, Yazdani and Jeffrey (2011) aimed to address this issue by considering the relationship between the structure and vulnerability of these systems against random failures and targeted attacks on network components. They achieved this by studying the structural properties of four water distribution systems, with different numbers of nodes and links, shown in Figure 2.40; initially finding that the degree distributions for these networks follow an exponential trend (Figure 2.41). They applied various graph theory metrics to analyse these networks to quantify different

network characteristics (see Table 2.8). Through this analysis they found that the "*spatial organisation of [water distribution systems] imposes severe limitations on their connectivity*", resulting in structural vulnerability patterns in these systems. They concluded that this analysis approach, applying various network metrics, could be used as a basis for a tentative ranking of vulnerability with regards to the network structure. However, Yazdani and Jeffrey (2011) advise caution when using topological measurements for the analysis of a real world system, as each graph theory metric only captures partial information regarding the network structure and that there is no unique measure of network robustness. They also state that these graph theory metrics may require alteration and adjustment to account for the location of isolation values, for example.

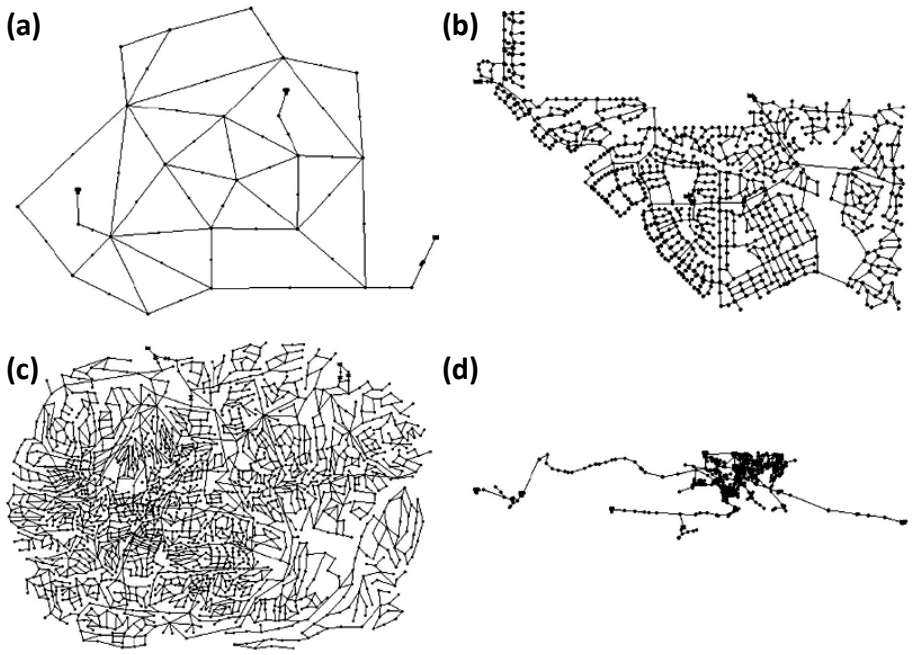


Figure 2.40: Showing a graph view of four water distribution networks, (a) Anytown, (b) Colorado Springs, (c) EXNET and (d) Richmond (Yazdani and Jeffrey 2011).

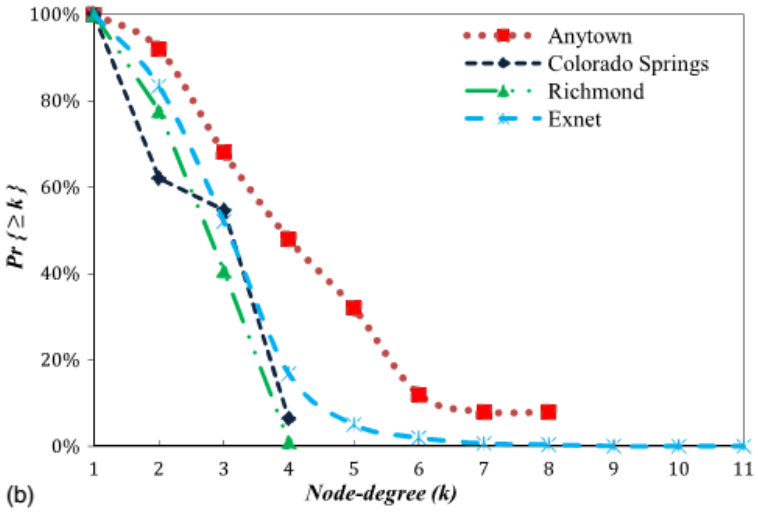


Figure 2.41: The degree distributions of the four water distribution systems shown in Figure 2.40 (Yazdani and Jeffrey 2011).

Table 2.8: The metrics used by Yazdaini and Jeffrey (2011) to quantify different characteristics of water distribution systems.

Metric	Definition	Network Characteristic Quantified
Average node degree	Average value of the node-degree distribution	Connectivity
Clustering coefficient	The fraction between the total number of triangles N_Δ and the number of connected triples N_3 in the network	Loops (redundancy)
Meshedness coefficient	The fraction between the total and the maximum number of independent loops in a planar graph	Loops (redundancy)
Spectral Gap	The difference between first and second eigenvalues of graph's adjacency matrix	Robustness
Algebraic connectivity	The second smallest eigenvalue of normalised Laplacian matrix of the network	Robustness

2.8: DEVELOPMENT OF SPATIAL NETWORK MODELS

The network models presented and discussed in this chapter have, so far, been purely topological models, where only the presence of a link between two nodes is considered (and not the location of individual nodes or the physical distance between pairs of nodes). However, as the analysis of real world infrastructure networks turns from the Internet and the World-Wide-Web (both requiring only very little space to operate) to airline and electrical distribution systems (requiring large amounts of space) the spatial element of these networks is becoming increasing important in the analysis. Indeed, the validity of using topological models to analyse geographically distributed networks has been questioned by some researchers (Hines et al. 2010). Put simply, the distinction between a topological model and a spatial model is the fixed locations of nodes in the spatial model (e.g. the nodes may have longitude and latitude coordinates) (Barthelemy 2011). The little work that has studied real world spatial networks still focuses mainly on characterising the topology of the system (into one of the network classes), while the spatial element of the same network receives less attention - if not neglected entirely (Boccaletti et al. 2006).

There are a few studies that analyse the spatial characteristics of real world networks, including that of Crucitti et al. (2006) who studied centrality in urban streets of different world cities, using nodes to represent intersections and links to represent streets (Figure 2.42). The aim of their study was to develop an extended visualisation and characterisation of the city structure. It can be seen from Figure 2.42(a), that the closenesss centrality measure shows the majority of highly scored nodes in the centre of the network, radiating outwards to the lower scores at the boundary of the considered area. This is in contrast to the betweenness centrality measure (Figure 2.42(b)) which highlights several routes in the city with a high score. Crucitti et al. (2006) correlated these routes with the most popular walking paths in the city, finding that there was a strong correlation. The authors also studied other cities and found that in these studies the betweenness centrality measure was also able to identify the primary structure of movement channels from the secondary routes.

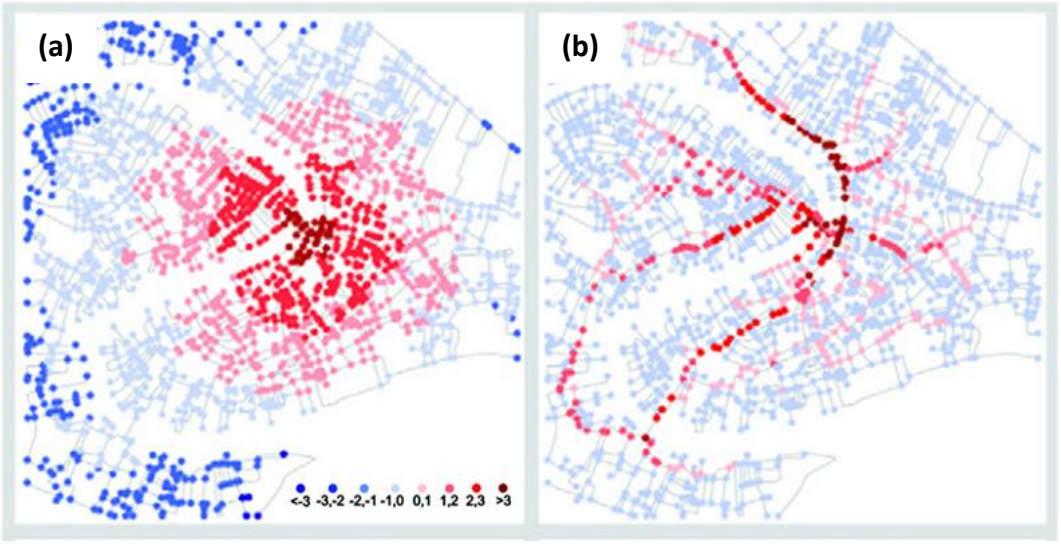


Figure 2.42: A colour-coded map showing the (a) closeness and (b) betweenness centrality of the urban street network in Venice, Italy (Crucitti et al. 2006).

Whilst, the majority of studies analyse the characteristics of real world networks only, there are a small number of other studies that have developed models to replicate the nodal connectivity of these spatial networks. The most notable of these studies is that of Gastner and Newman (2006b) who propose a model for connecting links between pairs of nodes, with a fixed spatial location, based upon their separation distance. They include a variable parameter, λ, in their algorithm, which is used to simulate users' preference. For example, when λ = 0 the resulting network resembles an airline network, in which users want to minimise the number of flights in their journey; and when λ = 1 the resulting network resembles a road network where users want to minimise the length of their journey (Figure 2.43). A similar model has also been developed by Qian and Han (2009), who also include a variable which can be altered to generate networks with different connectivity's. In these spatial network algorithms the locations of the nodes are generally pre-allocated and are usually based upon a real system (i.e. the main aim is to define the rules which govern link formation between pairs of nodes, rather than to understand the rules that govern nodal location).

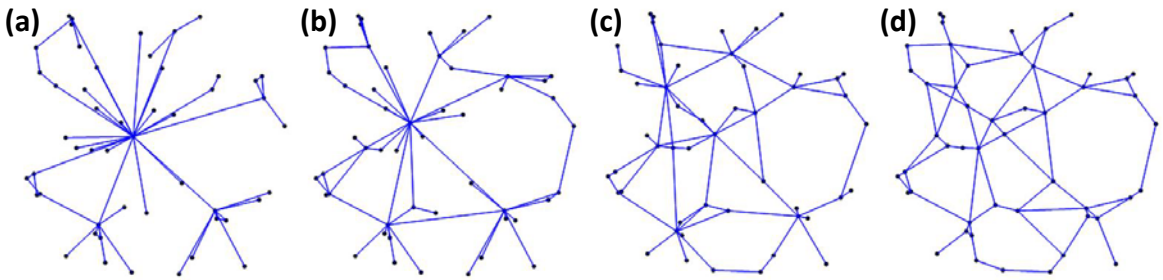


Figure 2.43: Networks generated with different nodal connectivity, for the same nodal layout, depending on user preference (λ), where: (a) λ = 0, (b) λ = 1/3, (c) λ = 2/3 and (d) λ = 1 (Gastner and Newman 2006b).

Whilst network theory studies have largely ignored the 'rules' governing the location of nodes within spatial networks, in favour of the 'rules' governing the formation of links, other studies have focused primarily on this problem, with some success. Gastner and Newman (2006a) developed an optimal spatial layout of facilities (representing, hospitals and airports, for example) where the distance between a person's home and the nearest facility was minimised (Figure 2.44).

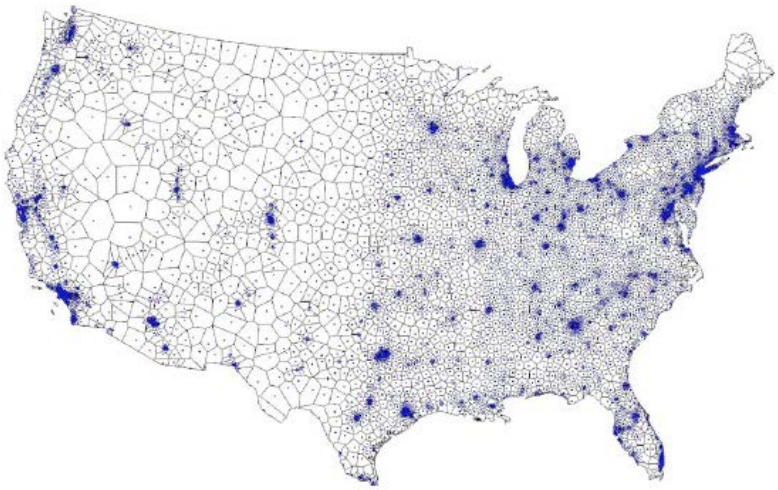


Figure 2.44: Facility locations in the US, as determined by the algorithm of Gastner and Newman (2006a).

However, other methods have focused on developing proxy models for real world cities. One of the most notable techniques is cellular automata, which has been used to predict urban growth around cities, including: San Francisco (Clarke et al. 1995), Washington / Baltimore (Clarke and Gaydos 1998) and Guangzhou (China) (Wu 2002). A cellular automation model is a dynamic system in which the geographical study area is divided into regular spatial cells, and time progresses in discrete steps. Each spatial cell has one of a finite number of states and the state of each cell is updated at each

time step according to a set of 'rules' (Liu 2009). The models require the initial input of four main layers of data describing the initial conditions in the study area, which are updated as the model runs: (1) digital elevation of the study area, (2) the location of the initial settlements, (3) historical transportation layers (e.g. road network) and (4) a layer showing excluded areas (e.g. national parks, water bodies, etc.). This data is gathered from historical maps, air photos and digital maps and as the data is obtained from a variety of sources there are often problems with assembling the dataset, including: inconsistent dimensions of features, generalisation in historical maps, different projections of the study area, different coordinate systems and different census boundaries. As such the main disadvantage in this method is that the accuracy of the results is highly dependent on the size of the input dataset and on the quality and quantity of the historical data (Clarke and Gaydos 1998), indeed if insufficient historical data for the study area is obtained then it is not possible to generate a synthetic model.

Previous studies using spatial network models have not considered the hazard tolerance of the networks to spatial hazard. It has previously been discussed that the likely hazards to affect infrastructure systems are spatial (e.g. a flooding event, hurricane) and as such the lack of research in this area seems surprising.

This chapter has presented an overview of the key literature surrounding the resilience of infrastructure systems. This review has shown that many infrastructure systems are normally analysed using physically based models, which whilst useful at providing scenario based information can be found lacking when used to assess the resilience of these systems, as only a limited number of scenarios can be tested (potentially leaving them vulnerable to unforeseen events). It was found that this problem has recently been addressed by applying network graph theory to try and understand the behaviour of these complex interacting systems; for example, Barabasi and Albert (1999) used this approach to show that targeted attack causes more disruption to the Internet than random system failures. In this network theory approach the topology of the system is modelled as a series of nodes and connecting links, which enables the fundamental properties of the system to be described. Using this approach also allows for the

development of network generation algorithms, which are capable of generating synthetic networks with the same properties as real world systems and can be used to assess systems where obtainable data is incomplete or for the analysis of future systems, which do not yet exist. Previous studies, using this approach, have shown that many infrastructure systems potentially configure to specific network architectures and therefore may have similar properties; however, some researchers are questioning the validity of using topological models to analyse infrastructure systems, due to the geographical distribution of these systems. Spatial models do exist in network graph theory and have been used to analyse a small number of infrastructure systems, however, these studies still focus on classifying the topology of the network and do not consider their spatial hazard tolerance. This research has also shown that the main threats to these systems are also spatially coherent and geographically distributed, further strengthening the argument of using spatial network models and spatial hazards to assess the resilience of infrastructure systems.

Therefore, this thesis will aim to address this issue, by analysing infrastructure systems using a network graph theory approach to provide a level of confidence that the system will perform adequately after a natural hazard. Unlike traditional network theory, spatial network models will be used to model the geographically dispersed nature of these systems and also to model the spatial component of the hazards threatening these systems. Due to the lack of complete and obtainable datasets for many infrastructure systems, this research will attempt to develop network generation algorithms that can reproduce synthetic spatial networks with the same characteristics as real world network. The study will then extend this dataset by generating other generic networks. The vulnerability of these networks will be assessed by applying the maximum cluster size and average path length measures. These measures are used in combination, as the maximum cluster size gives an indication of how fragmented the network has become by spatial hazard, whilst the average path length quantifies the change in performance within the network. This thesis will also assess the applicability of using graph theory metrics to highlight specific 'critical' nodes within these systems (i.e. nodes that when removed cause a disproportionate impact to the remaining network); it is likely from the results of previous studies that these metrics may need to be adapted or modified to increase their predictive capabilities.

CHAPTER 3: HAZARD TOLERANCE OF REAL WORLD SPATIAL NETWORKS

The previous chapter presented and discussed an overview of the key literature surrounding the resilience of infrastructure systems. In this review the limitations of using traditional analysis techniques to increase the resilience of an infrastructure system were discussed and a potential new method of using network graph theory for this purpose was presented. It was discussed that the majority of studies use topological models only to analyse infrastructure systems, which can be located over wide geographic regions, prompting some researchers to question the validity of these models. Spatial network models have since been developed and applied to the analysis of infrastructure systems; however, these studies only focus on the classification of the system and do not form synthetic proxy networks for real world systems, which allow the 'rules' governing the formation of these spatial networks to be understood and networks with incomplete data to be analysed. Finally, it was discussed that the spatial hazard tolerance of these networks is seemingly lacking from the analysis altogether, which is surprising when considering that the majority of threats to infrastructure systems are distributed over geographic regions.

This chapter uses the network graph theory approach to analyse a real world spatial network, namely the European air traffic network, and shows how the perceived topological resilience of this network to random hazard changes when these hazards are located over geographic regions. This real world network was chosen as tests for hazard tolerance can be validated using the data from the 2010 Eyjafjallajökull eruption. To determine whether the vulnerability shown by this network is (1) unique to the European air traffic network, (2) inherent of its network class, or (3) due to its specific nodal layout, networks with the same characteristics as the real world network are generated and subjected to spatial hazard.

3.1: CASE STUDY: THE DISRUPTION CAUSED TO THE EUROPEAN AIR TRAFFIC NETWORK BY THE EYJAFJALLAJÖKULL VOLCANO

The 2010 eruption of the Eyjafjallajökull volcano, in Iceland, occurred on the 14th March and forced almost 800 local residents to evacuate their homes (Petersen 2010). Continuing eruptions caused disruption to the European air traffic network (EATN), with restrictions on airspace and no fly zones from 14th April (Brooker 2010). The resulting airport closures and disruption to air travel caused more than 10 million passengers to be delayed. The economic impact to the airline industry, in terms of revenue loss for airlines from scheduled services, during the period 15th-21st April, was estimated at 1.7 billion US dollars (Mazzocchi et al. 2010). This amount of disruption is surprising as previous studies of air traffic networks have shown that they form truncated scale-free distributions (or a scale-free distribution with an exponential 'tail') and as such should be resilient to random hazard (see Chapter 2.5.3). To gauge the impact of this disruption to the EATN a graph theory network model, consisting of 525 airports and 3886 air routes, operated by 203 airlines, was constructed using data from Openflights (2010). This network is undirected and considers the presence of an air route only and not the number of flights / passengers along a particular air route, as this would constitute a weighted network which is outside the scope of this thesis.

To investigate whether the volcanic eruption had a disproportionate effect to the EATN, Flight Information Regions (FIR) that were closed for 12 hours or more on a particular day of disruption were identified, using the data of Eurocontrol (2010). This data was used to plot GIS images showing the open and closed FIRs for eight days of disruption. Three of these GIS plots have been shown in Figure 3.1(a-c), including the worst affected day (18th April). These GIS images show that the ash cloud mainly affected Northern Europe, but also closed Central Europe on the worst day of the event. To quantify the disruption to the network, the airports inside the closed FIRs and their connected air routes were removed from the network model to establish the percentage of closed airspace and cancelled air routes for each day of the disruption (Figure 3.1(d)). It was assumed that air routes which fly through an area of closed airspace (but where neither the source or destination airports were inside a closed area) were able to fly around this closed airspace.

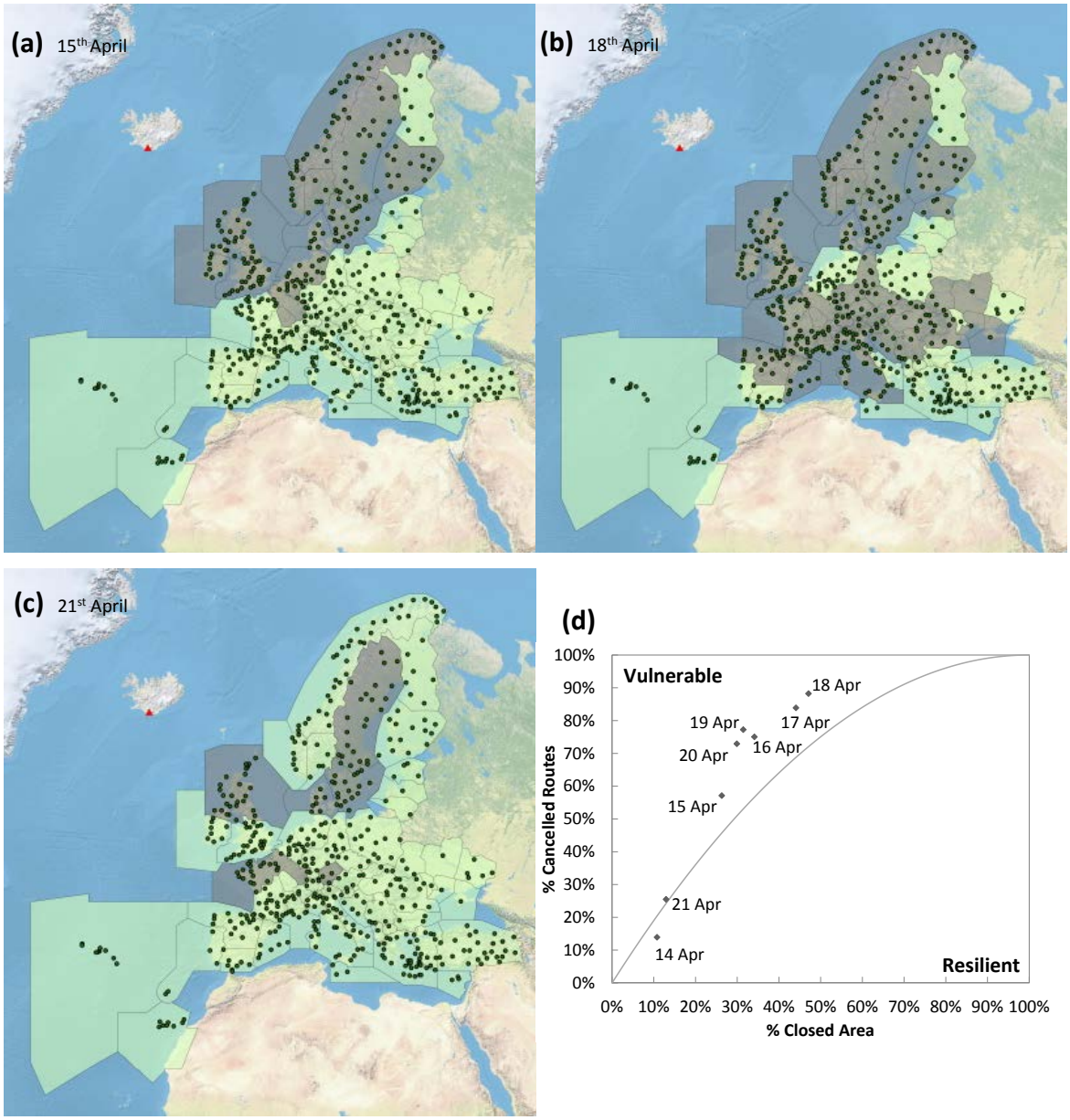


Figure 3.1: Open (light green) and closed (grey) FIRs in Europe (i.e. airspace) for (a) 15th April, (b) 18th April and (c) 21st April 2010 (Eurocontrol 2010). The airports are shown as dots and the Eyjafjallajökull volcano as a red triangle. Also, (d) showing proportion of travel disruption, relative to the proportion of closed airspace, during the Eyjafjallajökull eruption of 14th - 21st April 2010. The points on the graph represent the different days of disruption (labelled) and the random network (with random nodal layout) is shown by the grey line.

To determine whether the EATN is resilient or vulnerable to the Eyjafjallajökull volcanic event a benchmark of resilience needs to be established. In traditional network graph theory this is achieved by comparing the results, which are plotted in terms of the proportion of nodes and links removed, to that of a random network. However, this benchmark does not consider the size of the spatial disruption and the impact that this has to the remaining network. To overcome this shortfall, a spatial resilience benchmark is formed by allocating the nodes in a topological random network a random spatial location such that two spatial hazards of the same size, but with

different locations, remove an approximately equal number of nodes. The spatial resilience benchmark formed by using this method is shown in Figure 3.2.

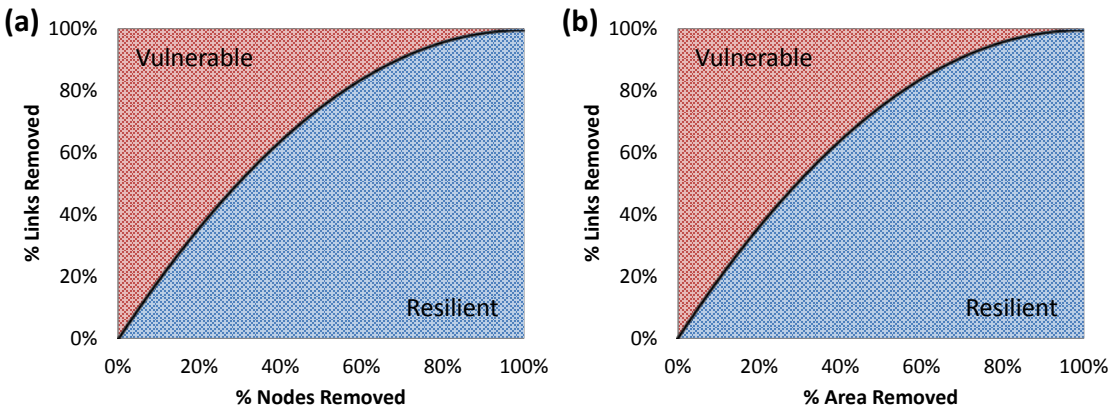


Figure 3.2: Showing the resilience random network benchmark plotted in terms of the proportion of removed links and (a) removed nodes and (b) removed area.

Plotting the proportion of air routes closed against the proportion of closed airspace for the Eyjafjallajökull event (Figure 3.1(d)) and comparing to a spatial benchmark random network (Figure 3.2(b)) the vulnerability / resilience of the network can be established. If the effect is proportionate to the cause (i.e. the disruption is proportionate to the area of closed airspace) then the points, representing different days of disruption, should sit on the line of the random network. From Figure 3.1(d) it can be seen that the EATN is more vulnerable, particularly to large spatial hazards, than the random network; although the network is more resilient, compared to the random network, for the initial day of disruption. These results demonstrate that the EATN is in fact vulnerable to the Eyjafjallajökull spatial hazard.

An initial investigation into the vulnerability of the EATN to spatial hazard is achieved by obtaining the degree distribution of the network (Figure 3.3). This distribution confirms that the network forms a truncated 'scale-free' distribution characteristic of other air traffic networks (Chapter 2.7.3) and that this network should therefore be resilient to random hazards (including the Eyjafjallajökull event) and vulnerable to targeted attack. It is worth noting the effect that 'windowing' has to this distribution. For example, it can be seen that there appears to be several nodes with degrees ranging from 118 to 133, however, there is only one node with a degree of 133 (as this is a cumulative probability distribution a point is placed for each possible value of degree).

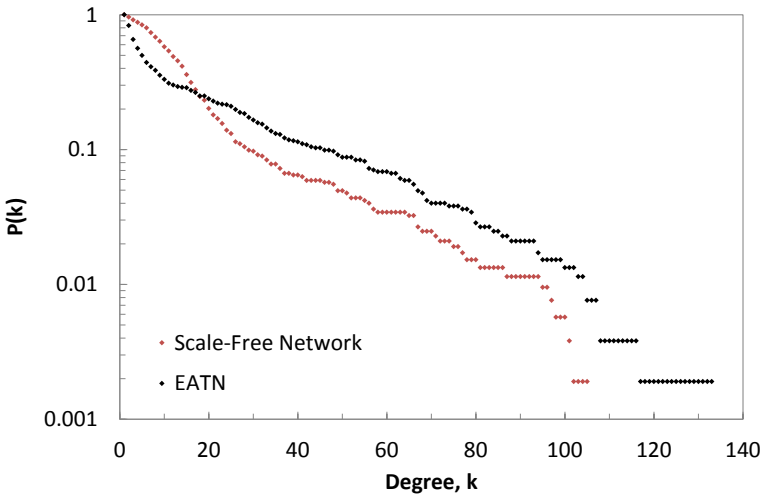


Figure 3.3: Plotting the degree distribution of the EATN (black dots) and a generated scale-free network (red dots), using the algorithm of Barabasi and Albert (1999).

To further investigate this vulnerability and to determine whether it is (1) unique to the EATN, (2) inherent of its network class or (3) due to the specific geographic location of nodes, synthetic networks with the same characteristics as the EATN are formed. This is achieved using the scale-free network generation algorithm of Barabasi and Albert (1999), where the m_0 value is equal to 14 and nodes are randomly allocated one of the actual airport locations as the network 'grows'. The degree distribution for this synthetic network is shown in Figure 3.3, where it can be seen that this synthetic network is a poor representation of the EATN. The generated scale-free network does not form a sufficiently well connected hub node (lacking 28 connections) and includes too many poorly connected nodes. Therefore, it can be concluded that traditional network generation algorithms can be deficient when used to form spatially distributed networks, as the 'rules' governing the formation of connections in these systems are not necessarily the same as those where space is not a governing factor (e.g. the Internet and World-Wide-Web).

3.2: DEVELOPMENT OF ALGORITHM TO GENERATE SYNTHETIC NETWORKS FOR THE EUROPEAN AIR TRAFFIC NETWORK

To generate synthetic networks with the same characteristics as the EATN, a new network generation algorithm is developed. This algorithm is based upon the scale-free generation algorithm of Barabasi and Albert (1999), but modifies the traditional algorithm to account for the spatial component of the network. As such, the new algorithm proposes that low degree nodes can capitalise on their close spatial proximity to a highly connected hub by attracting links that were bound for the high degree hub (through the idea of *preferential attachment*). For example, an airline may wish to establish a route to a major regional airport; however, the operating costs at this airport are high. Flying to a nearby airport will still attract passengers as it is only a short overland journey from this node to the highly connected hub, but for this subordinate node, the fares can be reduced due to the lower operating costs. It is therefore argued that the decision of where to establish a new route is made based on both degree and proximity. This modification is used to extend the algorithm of Barabasi and Albert (1999) by enclosing the network within a spatial domain and preferentially attaching new nodes based on the degree of all nodes within a sub-domain (neighbourhood) (Figure 3.4).

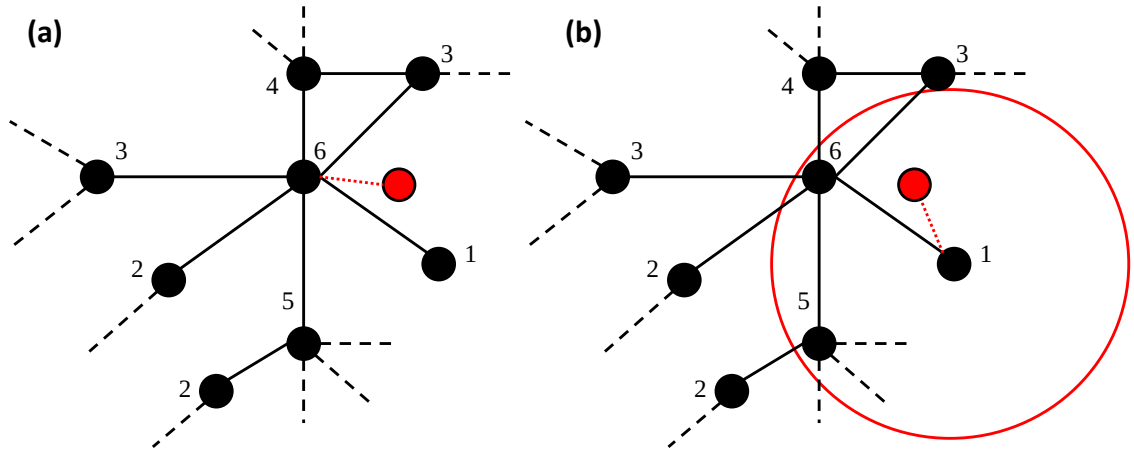


Figure 3.4: Demonstrating the idea of preferential attachment based on (a) degree and (b) degree and proximity, in part of a sample network. In this network the black dots represent nodes (with the adjacent number indicating its degree), the black lines represent links connecting these nodes and the dashed lines represent connections to other nodes in the network, that have been omitted for clarity. In (a) a new node (red) is introduced to the network, and using the algorithm of Barabasi and Albert (1999) would be most likely to attach itself to the high degree node; however, considering proximity as well as degree alters the probability because the spatial domain of the low degree node (in the centre of the red circle) includes the high degree node and therefore inflates its probability of attachment.

Following Barabasi and Albert (1999), an initial number of starting nodes, m_0, is chosen, but each node is now given a spatial location. At each timestep, a new node is added to the network and is given one of the pre-allocated nodal positions. This new node introduces between 1 and m_0 links to the network, which preferentially attaches this node to the existing network in the same manner as for a scale-free network, but with the spatial modification shown in Figure 3.4(b), where preference is now based on the degree of all nodes within the neighbourhood. The size of the neighbourhood is set by assigning a radius, *r*, which represents the distance people are prepared to travel overland to reach an airport. Setting this radius to zero removes the spatial dependence of the network and results in the generation of a scale-free network; while setting the radius to twice the size of the spatial domain results in random attachment (as the degree in each neighbourhood is equal to that of the degree in the whole network). To show that certain values of this radius (neighbourhood size) can produce an exponential network, the algorithm has been used to generate a network with 1000 nodes and 7370 links, with a radius value of 0.2. The degree distribution for this network is shown in Figure 3.5, where it can be seen that the distribution follows the straight line, when plotted on a log-linear scale, characteristic of exponential networks.

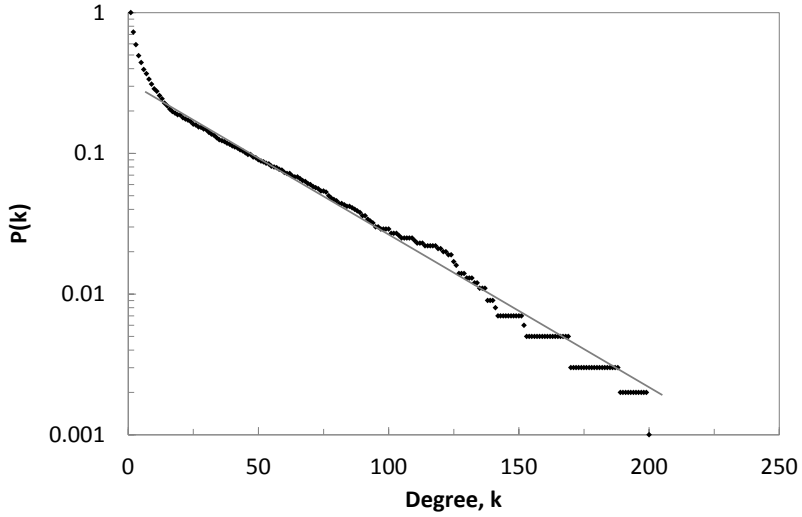


Figure 3.5: The degree distribution of an exponential network generated using the developed algorithm.

In addition to this spatial modification, the algorithm will also test the modification of Guimera and Amaral (2004), which allows a proportion of the new links, *p*, to connect between pre-existing nodes (referred to as the GA modification), and determines

whether this modification is necessary to produce reconfigurable networks, such as the EATN. However, the flight distance criteria for preferential attachment of Guimera and Amaral (2004) is not used, as intercontinental flights are not being considered and the deregulation of the EATN has led to flight path length becoming uncorrelated from degree. This can be demonstrated by plotting the flight length of different air routes against various measures of degree (Figure 3.6), showing that there is little or no correlation between the flight length and connectivity of an airport for the EATN.

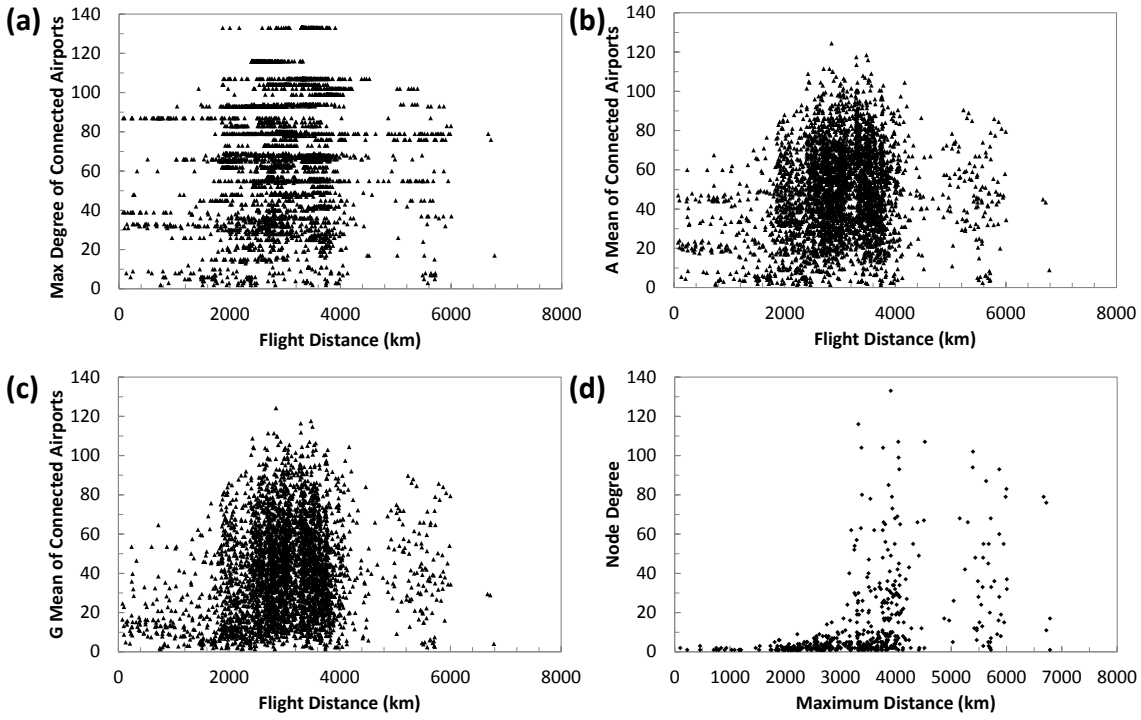


Figure 3.6: The air route distance between airports (in km) compared to (a) the maximum degree of connected airports, (b) the arithmetic mean of the two connected airports and (c) the geometric mean of the two connected airports for the EATN. Also showing (d) the correlation between the degree of an airport and the maximum distance flight from this airport. All of the plots show that there is no correlation between the air route distance and various measures of degree of the two connected airports.

To assess the ability of the proposed network generation algorithm to generate synthetic networks as proxies for the EATN using real world nodal locations, four different types of synthetic network (using different combinations of neighbourhood size and GA modification) have been generated. This allows the best combination of these to form the EATN to be determined and allows the 'rules' which govern the formation of air routes within the EATN to be identified.

1. Exponential network, with a constant neighbourhood size and including the modification of GA;
2. Exponential network, with a changing size of neighbourhood (depending on the distance from the node to the geographic centre) and including the modification of GA;
3. Scale-free network;
4. Scale-free network, with the modification of GA.

For the exponential networks, two different methods of assigning a neighbourhood size to nodes are considered, constant size and changing with distance from the geographic centre. The latter could be considered to be intuitive, because airports are more densely packed in the centre of the network giving people a greater selection of routes for smaller overland travel distances. The actual value of neighbourhood size is varied to determine the 'best fit' with the EATN and only the best fit value is presented in this thesis (due to space restrictions).

Both of these exponential networks also include the modification of GA (allowing a proportion of the new links to connect between pairs of existing nodes) and this modification will also be applied to one of the scale-free networks. The network generation algorithm for the scale-free networks has not been modified to account for the spatial distance between airports; this enables a direct comparison to the spatially modified exponential networks to determine if a spatial component should be included in the analysis of spatial networks or if it is enough to give the nodes a spatial location. Similarly, to the neighbourhood size, the exponential networks will also only be shown with the best fit value of GA modification (again due to space restrictions).

Traditional network generation algorithms focus solely on the replication of the degree distribution of the network, however, as this is a spatial network the ability of the algorithm to generate the spatial characteristics of the network must also be considered. This is achieved by replicating the spatial distribution and spatial degree distribution of the network (Figure 3.7). These distributions were obtained by first calculating the geographical centre of the airports (weighted by their degree) and then plotting the number of airports within a given radius (Figure 3.7(a)) and the cumulative degree (Figure 3.7(b)). For the EATN the geographic centre of the network is located in

Germany (approximately 190km east of Frankfurt). From Figure 3.7 it can be seen that both of these distributions exhibit an approximately bilinear form, meaning that they are uniform with distance from the geographical centre of the air traffic network up to radius of ~1500km, after which the distribution of both airports and their degrees becomes sparser but remains relatively uniform. The change in grade shown in Figure 3.7 occurs as the considered area extends into the Atlantic Ocean in the west, and the border of the European Union in the east.

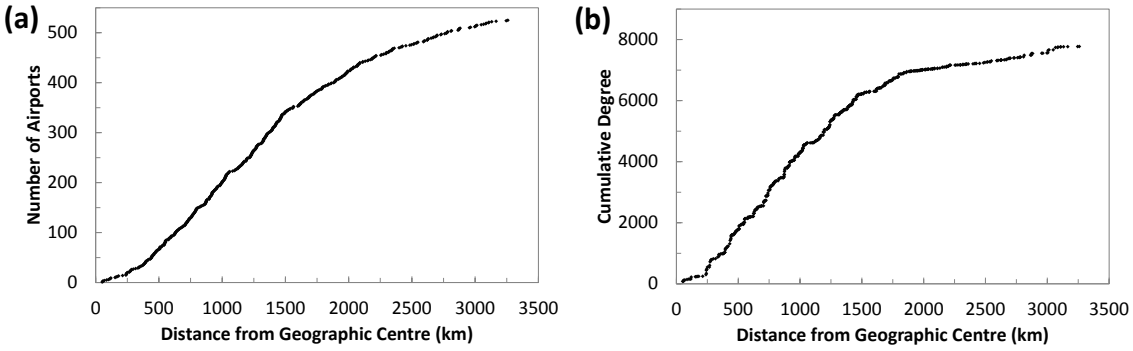


Figure 3.7: Plotting (a) the distribution of airports and (b) the spatial degree distribution of airports for the EATN.

These synthetic networks have all been generated using the actual EATN airport locations, therefore the spatial distribution of the synthetic networks will be an exact match to that shown in Figure 3.7(a). However, due to the 'growth' element of the network generation algorithm the order in which nodes are introduced to the network must be considered, as this will have an effect on the spatial degree distribution of the synthetic networks. Nodes which are introduced first to the network have more chances to attract links introduced from added nodes and consequently should have a higher degree than those introduced later to the network; therefore affecting the spatial characteristics of the synthetic networks, by determining the location of the high degree nodes.

Using the actual airport locations should allow the airports to be introduced to the network in the order of which they were first opened. However, this raises the issue of defining when an airport is first opened; should this be defined as the first flight from the airport? Or the first commercial flight from the airport? To overcome this issue, four different orders of introducing nodes to the network will be considered. This will allow the effect that the different introduction orders has to both the degree

distribution and spatial degree distribution to be determined and will also enable the introduction order which best fits the EATN to be identified.

1. *Distance* – nodes are introduced with distance from the geographical centre of the network, outwards;
2. *Proportional with Distance* – nodes in the centre of the network (i.e. those with a short distance from the geographical centre) are more likely to be introduced first, but not necessarily;
3. *Random* – nodes are introduced randomly to the network.
4. *Population* – one nodes from each of the 43 countries is randomly chosen and is introduced to the network in order of the country population (highest to lowest, e.g. Germany, France, UK, etc.). The remaining 482 nodes are then introduced randomly to the network.

There are three 'generic' node introduction orders and one introduction order which relies on the input of an additional dataset, namely population census data which has been obtained from ArcGIS (2013). This fourth node introduction order incorporates the idea that each country desires to open an airport within a short time of the network becoming established.

The results for generating synthetic networks for the EATN, using the actual airport locations and the four node introduction orders, are shown in Figure 3.8 and Figure 3.9. From these results it can be seen that the order in which nodes are introduced to the network has a small, but noticeable effect to the degree distribution and a significant effect on the spatial degree distribution of the synthetic networks.

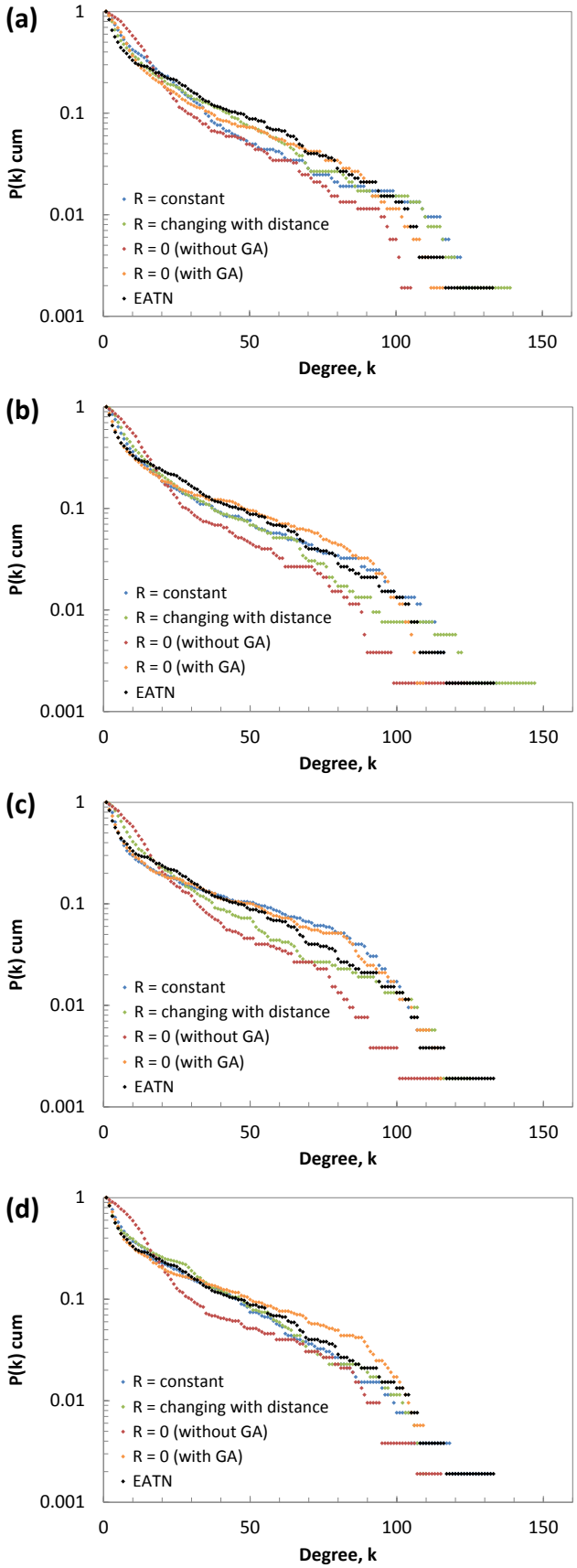


Figure 3.8: Showing the degree distribution for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm, where nodes are introduced (a) randomly, (b) proportional with distance, (c) with distance from the geographic centre and (d) based on the population of each country.

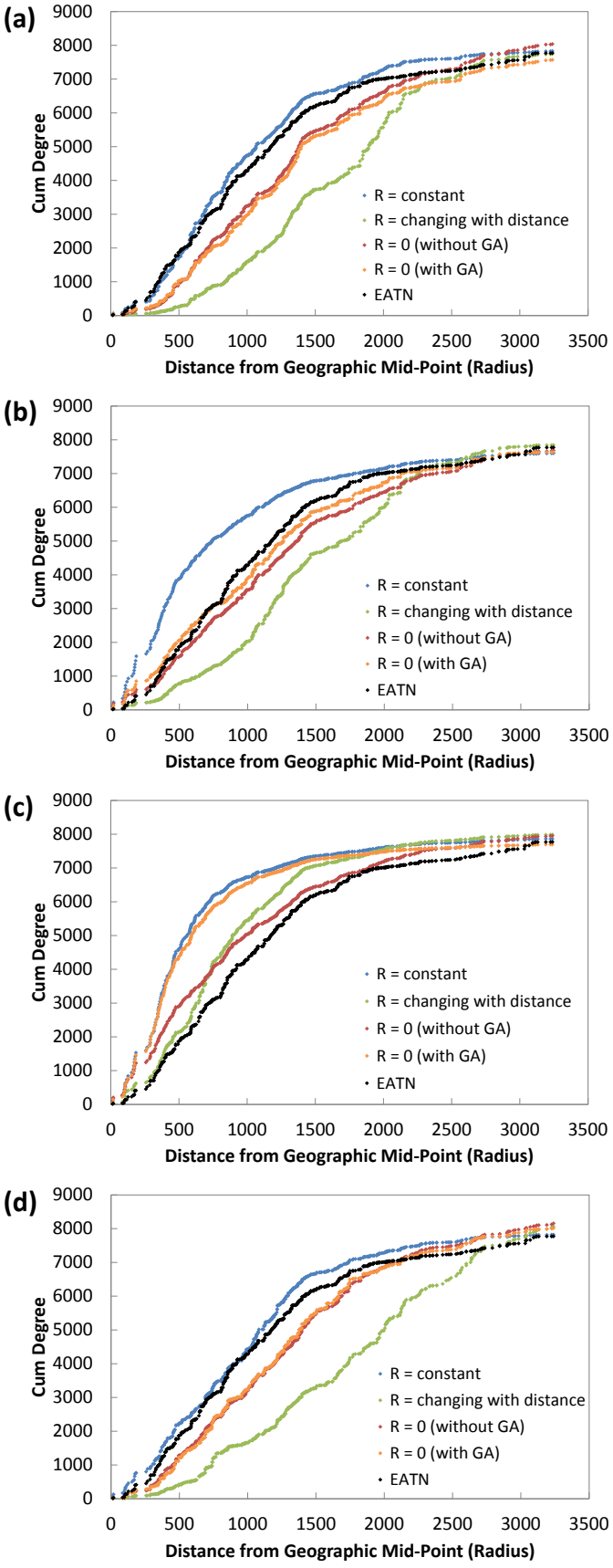


Figure 3.9: Showing the spatial degree distribution for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm, where nodes are introduced (a) randomly, (b) proportional with distance, (c) with distance from the geographic centre and (d) based on the population of each country.

Focusing on the degree distributions (shown in Figure 3.8) the synthetic network which best correlates with the EATN changes depending on the order in which nodes are introduced to the network. When the nodes are introduced randomly the exponential network with constant neighbourhood size (blue dots) and the modified scale-free network (orange dots) show the best correlation with the EATN. However, it should be noted that the exponential network contains too few mid-degree nodes and the scale-free network does not form a sufficiently well connected hub node. These two synthetic networks also show the best correlation with the EATN when the nodes are introduced proportional to distance and with distance from the geographic centre. However, it is the exponential network with constant neighbourhood size (blue dots) which best replicates the topological structure of the EATN when the nodes are introduced with population; in this case the unmodified scale-free network contains too many mid-degree nodes. Both the unmodified scale-free network (red dots) and the exponential network with the changing neighbourhood size (green dots) do not correlate well with the EATN network for all four node introduction orders (forming too large a hub and too small a hub node respectively). From these results, it can be concluded that, in air traffic networks, links must be allowed to form between pairs of existing nodes as the network 'grows' in order for the hub airports to form (i.e. these networks must include the modification of GA). It can also be concluded that a spatial component must be included in the network generation algorithm, as the exponential networks (blue) show a better correlation with the EATN distribution than the unmodified scale-free network (orange). Although, it is acknowledged that this difference is slight for all but the population node introduction order.

However, the ability of a synthetic network to replicate the characteristics of EATN should not be based on topological structure alone; it should be a compromise between this characteristic and its ability to replicate the spatial distribution of the EATN (Figure 3.9). Therefore, the spatial degree distribution of the synthetic networks also needs to be considered. From these spatial distributions it can be seen that the exponential network with the modification of GA (blue dots) is the most superior at forming the EATN when the nodes are introduced randomly, but does not replicate the spatial characteristics of the EATN when the nodes are introduced proportional to distance and with distance (in these cases it is the unmodified scale-free network

which best captures the spatial characteristics of the EATN). This difference can be explained by considering the spatial dispersion of high degree nodes throughout the network. Figure 3.10 plots the degree of all nodes in the EATN and in the synthetic exponential networks, with the GA modification, for all four node introduction orders. In this figure, it can be seen that introducing nodes proportional to distance and with distance causes too many high degree nodes to be located close to the geographic centre of the network compared to the EATN. Whereas, introducing nodes randomly spatially disperses these high degree nodes throughout the geographic region. However, the best compromise between degree distribution and spatial degree distribution occurs for this synthetic network (exponential network, with the modification of GA) when nodes are introduced with population. The reason behind this correlation is due in part to the 'rules' governing the formation of links in the synthetic network, but also in the specific order in which nodes were introduced to the network. From Figure 3.10(a, f) it can be seen that there is a correlation between the location of high degree nodes in the EATN and areas of high population density within Europe (with the high degree nodes being more likely to be located in a highly populated country). Therefore, initially introducing one node to each country in order of population gives the airport in highly populated countries more chances to attract links from newly opened airports, thereby replicating the correlation between hub airports and population density. In this synthetic network the size of the neighbourhood, which forms the best fit to the EATN, is approximately equal to 250km (2-3 hours driving time) meaning that this is the distance which people are prepared to travel overland to reach a nearby airport. It can also be concluded that the 'rules' governing the formation of links in the exponential network, with a constant neighbourhood size, are the same as those governing the formation of the EATN; as such, links must be allowed to form between pairs of existing nodes as the network 'grows' to allow the hub airports to form and air routes bound for a hub airport may divert to a subordinate node, providing that the node is within 250km of the hub airport.

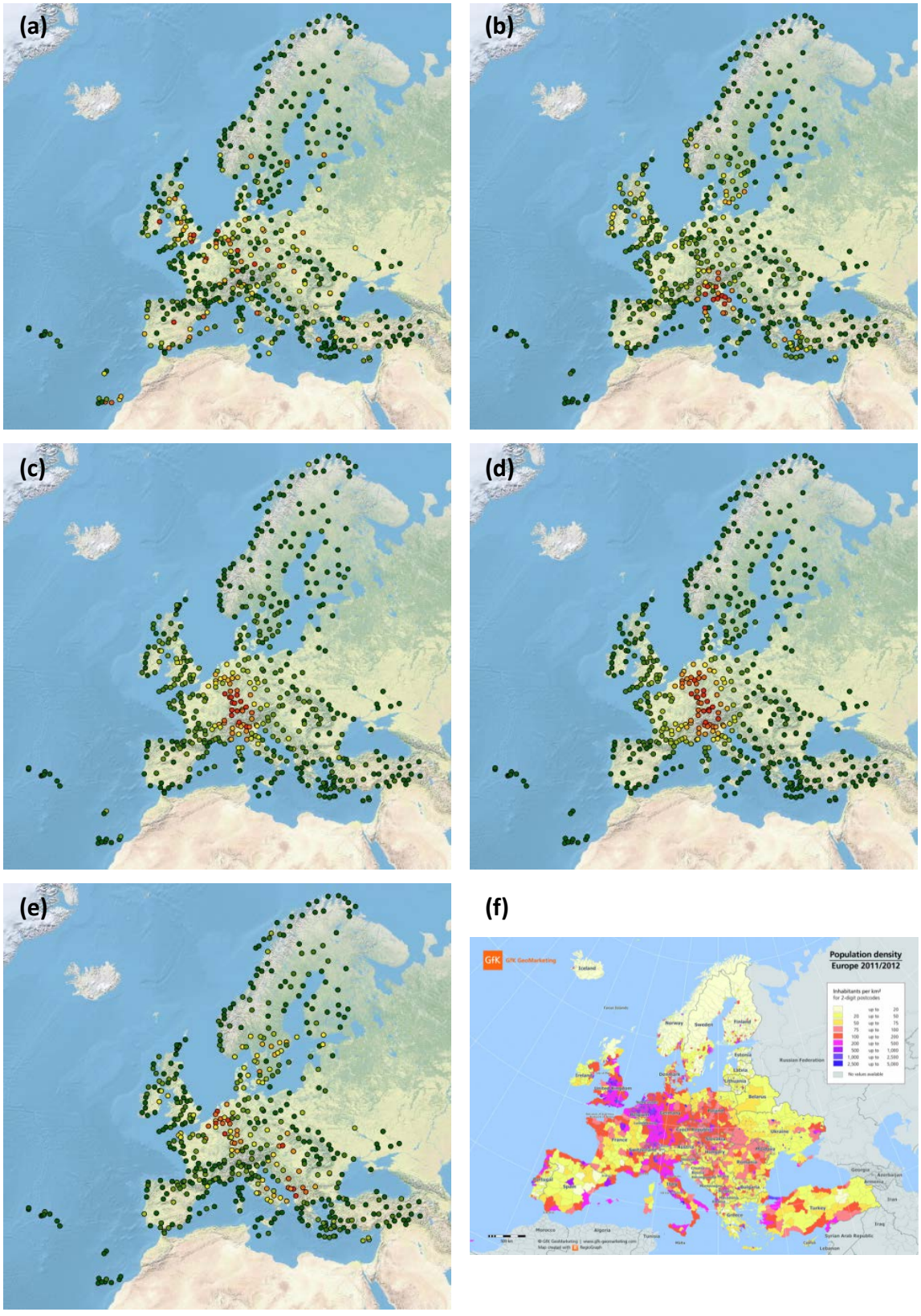


Figure 3.10: GIS generated images showing the location and the degree of nodes (red nodes are high degree and green are low degree) for (a) the actual EATN and generated networks where the nodes are introduced (b) randomly, (c) proportional with distance, (d) with distance and (e) with population. Also showing (f) the population density map for Europe (GfK GeoMarketing 2013).

These synthetic networks have assessed the ability of the proposed network generation algorithm to generate synthetic networks as proxies for the EATN; finding that an exponential network with the GA modification, where nodes are introduced based on population, is the most suited to replicating the topological and spatial characteristics of the EATN. However, this study has used the actual airport locations of the EATN and therefore the synthetic networks generated cannot be considered to be fully synthetic spatial networks. To overcome this shortfall, the spatial structure of the network should also be generated, in a similar manner to the networks topological structure, using a suitable generation algorithm.

It has previously been shown that the geographic distribution of airports within the EATN can be approximated by a bi-linear distribution (Figure 3.7(a)). Therefore, to investigate the effect that a generic nodal layout has on the ability of the network generation algorithm to replicate the topological and spatial characteristics of the EATN, the spatial distribution of nodes will be replicated using a bi-linear distribution.

To generate this bi-linear distribution of nodes, a distance from the geographic centre is defined inside which a proportion of the total nodes are randomly placed (by generating a random distance and bearing from the geographical centre). The remainder of the nodes are randomly placed in the area between this distance and the defined spatial boundary of the network. The resulting nodal layout has been shown in Figure 3.11(a), along with the spatial distribution of nodes Figure 3.11(b).

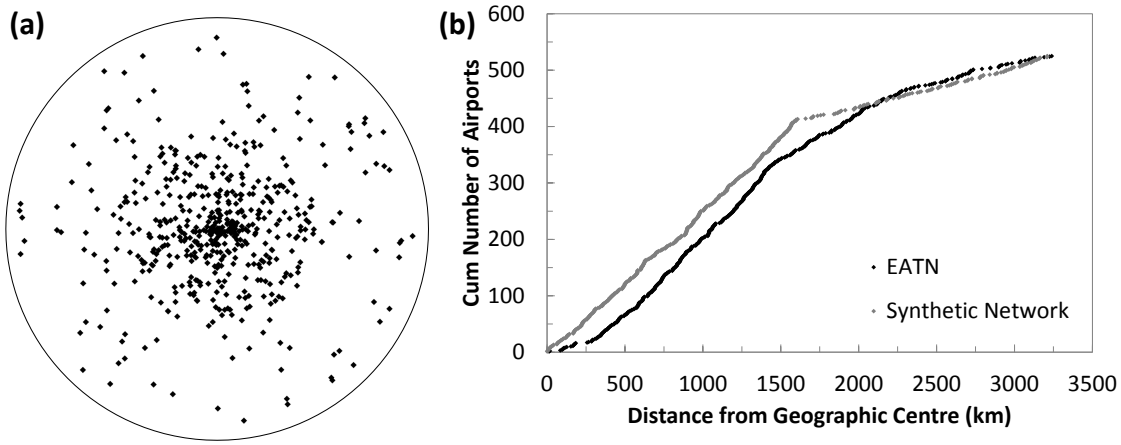


Figure 3.11: (a) Simulated random bi-linear nodal layout for the EATN, where the black dots represent the nodes and the grey line the spatial boundary of the network. (b) A comparison for the spatial distribution of nodes for the EATN (black) and the bi-linear nodal layout shown in (a) (grey).

This synthetic nodal layout has been used to generate the same four different types of synthetic network, for three node introduction orders (as this is a synthetic nodal layout it is not possible to introduce nodes in order of population), to determine which can best replicate the topological and spatial structure of the EATN. The degree and spatial degree distributions for these synthetic networks can be seen in Figure 3.12 and Figure 3.13 respectively.

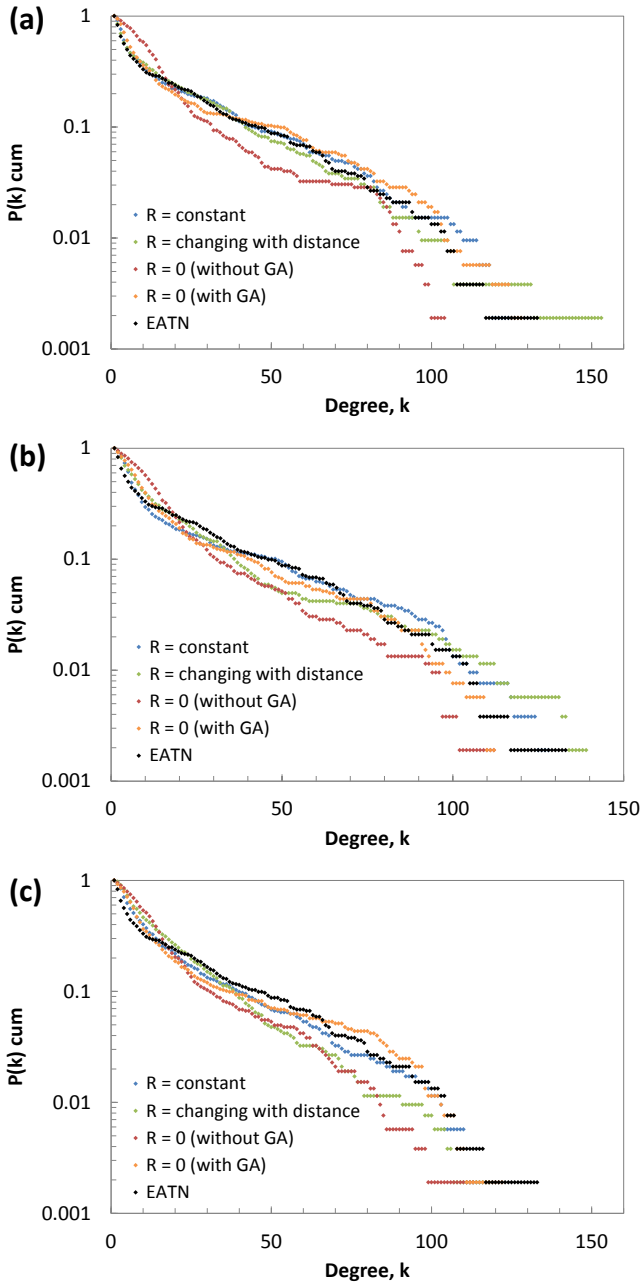


Figure 3.12: Showing the degree distribution for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm for a bi-linear nodal layout; where nodes are introduced (a) randomly, (b) proportional with distance and (c) with distance from the geographic centre. In the legend, R refers to the size of the neighbourhood radius and GA refers to the modification of Guimera and Albert (2004).

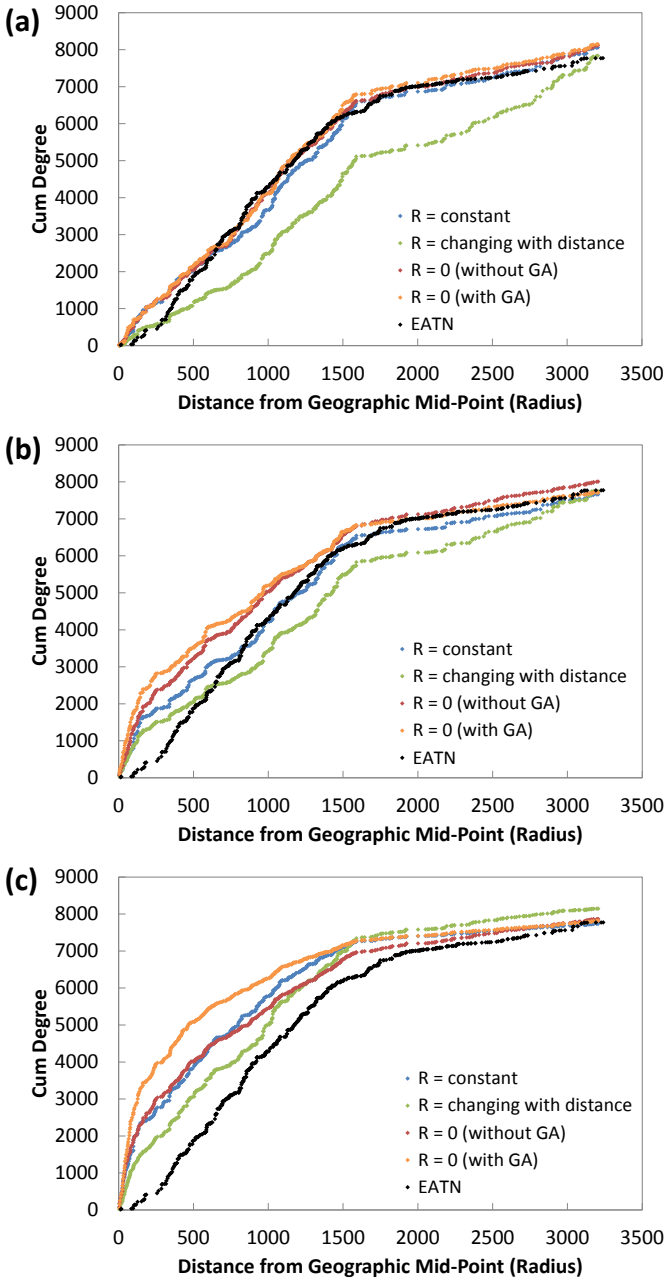


Figure 3.13: Showing the spatial degree distribution for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm for a bi-linear nodal layout; where nodes are introduced (a) randomly, (b) proportional with distance and (c) with distance from the geographic centre. In the legend, R refers to the size of the neighbourhood radius and GA refers to the modification of Guimera and Albert (2004).

Considering the degree distributions for the synthetic networks (Figure 3.12), it can be seen that the exponential network with the constant neighbourhood (blue dots) shows the best correlation with the distribution for the EATN (black), for all three node introduction orders. This is closely followed by the scale-free network with the GA modification (orange dots), however this network does not have a large hub airport unlike the exponential network (although this is difficult to see in Figure 3.12, due to overlapping results, but has a degree of 120 in Figure 3.12(a)). The exponential

network with the neighbourhood which is proportional to the distance from the geographic centre (green dots) tends to form a hub node with a degree which is larger than that of the EATN and is subsequently lacking in mid-degree nodes. The unmodified scale-free network (red dots) includes too many low degree airports and does not form a hub airport. Therefore it can be concluded that, in a similar manner to using the actual EATN airport locations, links must be allowed to form between pairs of existing nodes as the network 'grows' in order for the hub airports to form (i.e. these networks must include the modification of GA) and that a spatial component must be incorporated in the decision to form an air route (rather than using only degree).

The degree distributions for the four different networks alter slightly for the three different node introduction orders; although, the exponential network with a constant neighbourhood remains the best fit for the EATN distribution. However, the spatial degree distribution is again significantly affected by the order in which nodes are introduced (Figure 3.13). Introducing nodes randomly to the network creates the best fit spatial degree distribution with the EATN distribution for all four types of synthetic network (apart from the area close to the geographic centre of the network), with the exception of the exponential network with changing neighbourhood size. Whereas, introducing nodes proportion to distance and with distance creates a poor fit for the EATN for all four types of synthetic network, particularly in the area close to the geographic centre of the network. Figure 3.14 shows the bi-linear nodal layout, and indicates the degree of each node, for the exponential networks, with a constant radius for all three node introduction orders. From this figure, it can be seen that introducing nodes with increasing distance from the geographic centre causes hub airports to form close to the geographic centre of the network; whereas introducing nodes randomly to the network distributes the high degree nodes throughout the spatial area. This is similar to the distributions obtained using the actual EATN airport locations for the same node introduction orders (Figure 3.9) and again demonstrates the impact that node introduction order has to the spatial characteristics of the generated network.

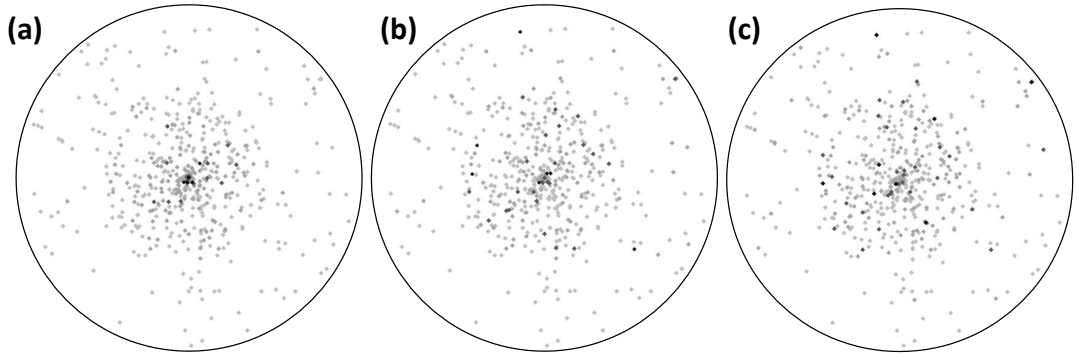


Figure 3.14: Showing three nodal layouts where the nodes have been introduced with (a) distance, (b) proportional with distance and (c) randomly. The black dots inculcate nodes with a high degree and light grey indicate those with a low degree and the black line indicates the circular spatial boundary of the network.

It can therefore be concluded that for a synthetic bi-linear nodal distribution the exponential network, with a constant neighbourhood size, and including the GA modification, is the best fit synthetic network for the EATN data. This is the same network which best replicated the topological and spatial structure of the EATN when the actual airport locations were used and again demonstrates that links must be allowed to attach between pairs of existing nodes in the network as the network 'grows' and the decision to form an attachment to an existing airport must be based on spatial location as well as degree. The value of neighbourhood in these exponential networks is again equal to approximately 250km (or 2-3 hours driving time).

Whilst these networks have been generated using a synthetic nodal configuration, and can therefore be considered fully synthetic spatial networks, the accuracy of the bi-linear distribution to model the distribution of airports in the EATN can be questioned. In order to generate a good fit for both the degree and spatial degree distributions for the synthetic networks, the accuracy of this bi-linear distribution needed to be compromised (which can be seen in Figure 3.11(b)) and is therefore not the best fit for the data. It can also be seen from Figure 3.15 that the EATN can easily be fitted inside a circular boundary, but that the bi-linear configuration (shown in Figure 3.11 (a)) is visually not a good fit for this data (primarily due to the distribution of land mass). In order to improve the accuracy to which the spatial configuration of airports is modelled in the EATN a more sophisticated method of assigning nodal locations is needed.

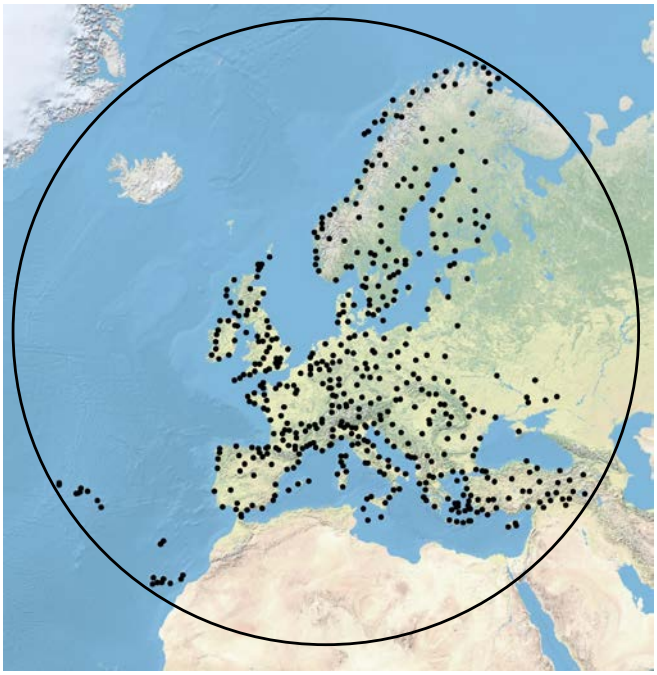


Figure 3.15: Plotting the airports of the European air traffic network within a circular spatial boundary.

A new algorithm is developed, which can generate proxy nodal configurations for real world nodal layouts (including the EATN). To achieve this, the characteristics of two real world networks are initially investigated; this ensures that variables to control different characteristics are incorporated into the algorithm. The locations of locations of Wal-Mart and Target stores over the same study area (USA) are investigated, as these two datasets are used as they are among the most documented, with previous studies analysing the spatial diffusion of stores (Graff and Ashton 1993; Holmes 2011) and the contrasting corporate strategies (Graff 1998). These two datasets were used rather than the EATN, or other air traffic network, as the date at which an airport opened is difficult to determine (as previously discussed), whereas the opening dates for stores in these two datasets is well defined. The growth of these two datasets has also been well documented, with many freely available videos showing the locations of stores opening over a given timeframe (FlowingData 2009; FlowingData 2010). Figure 3.16 shows the spatial layout of the Wal-Mart (3176 stores) and Target (1734 stores) datasets, along with their associated spatial distributions (both of these datasets were obtained from edigitalz.COM (2012)).

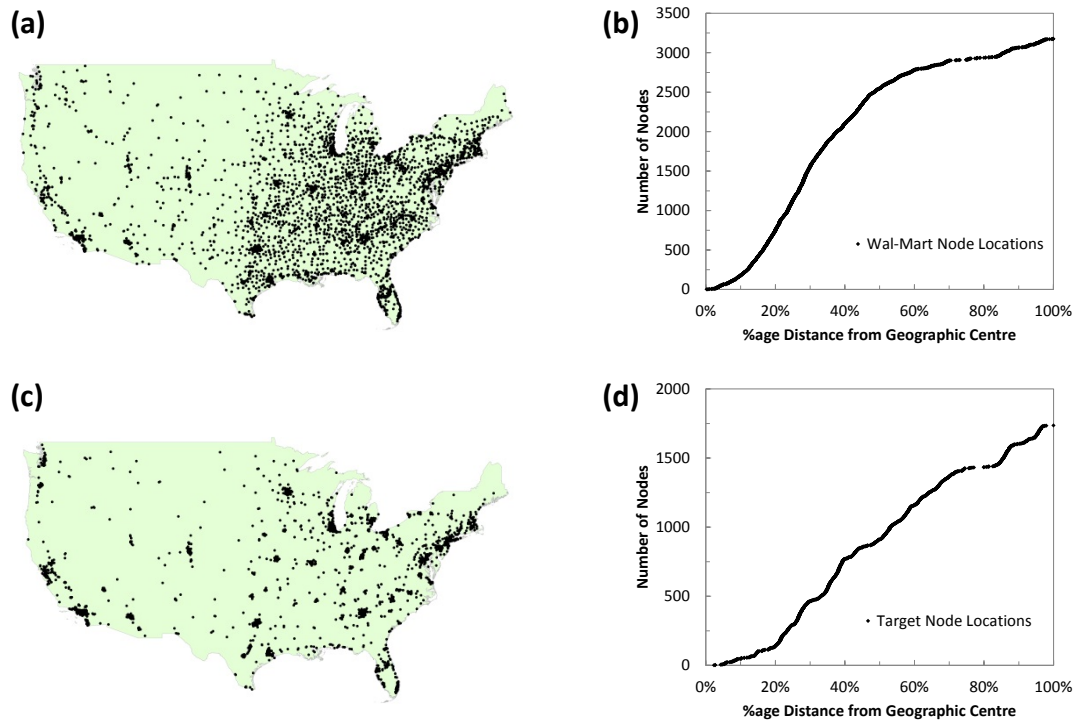


Figure 3.16: Showing (a) the spatial layout of nodes in the Wal-Mart dataset and (b) the associated spatial distribution; (c) showing the spatial layout of nodes for the Target dataset and (d) the associated spatial distribution. The geographic centre for the Wal-Mart dataset is located approximately 130km North-East of St Louis and for the Target dataset is located 250km West of St Louis. The results have been shown in terms of the percentage distance from the geographic centre due to enable a direct comparison between the two datasets (as they have a different maximum radius).

From Figure 3.16(a, c) it can be seen that the two datasets are visually very different. The Target dataset appears to have much smaller and denser clusters of stores than those of Wal-Mart, which, in addition to the clusters of stores, has an even spread of stores over the East of the country. This visual difference in clustering of the two datasets can be confirmed by using the Nearest Neighbour Analysis developed by Ebdon (1977). The Nearest Neighbour Index either indicates: a completely clustered nodal pattern, where the nodes lie in the same location on top of each other (returning a value of 0.00); a completely dispersed pattern, where there is an equal distance between all nodes (returning a value of 2.15); or a random arrangement of nodes (returning a value of 1.00) (as shown in Figure 3.17).

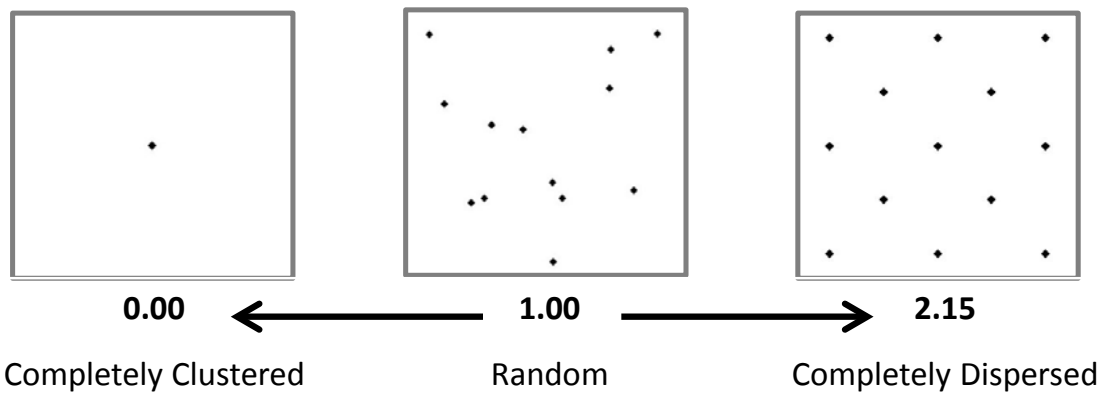


Figure 3.17: Showing the extreme values for the Nearest Neighbour Index developed by Ebdon (1977), where 0 indicates a completely clustered layout, 1.00 a random layout and 2.15 a completely dispersed layout.

The following example demonstrates how the Nearest Neighbour Index is calculated, using an example nodal configuration, shown in Figure 3.18.

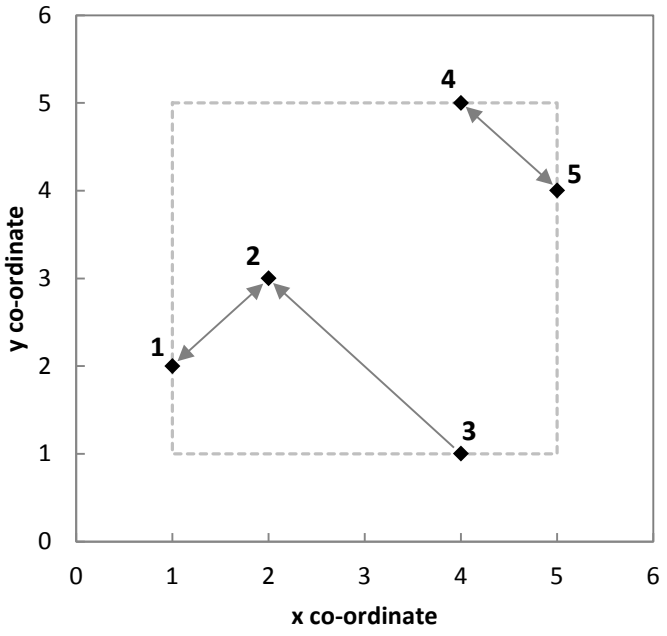


Figure 3.18: A nodal distribution used to show an example of the Nearest Neighbour Index calculation. The nodes are represented by the black dots (with their node numbers), the grey arrows indicate the nearest neighbour of each node (determined by distance) and the grey dotted box defines the spatial boundary of the nodes.

The Nearest Neighbour Index, *R*, is calculated using Equation 3.1; and is simply a ratio between the observed mean nearest distance between the nodes and the expected mean nearest neighbour distance for a fully dispersed nodal layout (with the same number of nodes and area).

$$R = \frac{\bar{d}_{OBS}}{\bar{d}_{RAN}} \quad \textbf{3.1}$$

The expected mean nearest neighbour distance for a fully dispersed nodal layout ($\bar{d}_{RAN}$) is given by equation 3.2, where *p* is the density of the whole nodal layout.

$$\bar{d}_{RAN} = \frac{1}{2\sqrt{p}} \quad \textbf{3.2}$$

For this example (Figure 3.18), $\bar{d}_{RAN}$is calculated as:

$$\boldsymbol{\bar{d}_{RAN}} = \frac{1}{2\sqrt{p}} = \frac{1}{2\sqrt{(5/16)}} = \mathbf{0.894} \quad \textbf{3.3}$$

The observed mean nearest neighbour distance ($\bar{d}_{OBS}$) is calculated using Equation 3.4, where *d* is the nearest neighbour distance for each node and *n* is the number of nodes in the layout.

$$\bar{d}_{OBS} = \frac{\sum d}{n} \quad \textbf{3.4}$$

The nearest neighbour, for each node, has been shown diagrammatically in Figure 3.18 (depicted using the grey arrows, pointing from a node towards its nearest neighbour) and also shown in Table 3.1, along with the calculated separation distance (*d*).

Table 3.1: Calculation of the Nearest Neighbour Distance

Node	Nearest Neighbour	Nearest neighbour distance (d)
1	2	1.414
2	1	1.414
3	2	2.828
4	5	1.414
5	4	1.414
n = 5		***Σd = 8.484***

The observed mean nearest neighbour distance ($\bar{d}_{OBS}$) can therefore be calculated using Equation 3.4 as:

$$\bar{\boldsymbol{d}}_{\boldsymbol{OBS}} = \frac{\sum d}{n} = \frac{8.484}{5} = \mathbf{1.697} \quad \textbf{3.5}$$

Nearest Neighbour Index, *R*, can now be calculated, using Equation 3.1*,* as:

$$\boldsymbol{R} = \frac{\bar{d}_{OBS}}{\bar{d}_{RAN}} = \frac{1.697}{0.894} = \mathbf{1.898} \quad \textbf{3.6}$$

From the result of the Nearest Neighbour Analysis it can be seen that the example nodal layout is between the random and dispersed indicators (Figure 3.17).

Applying this analysis to the Wal-Mart and Target datasets (Figure 3.16), returns a value of 0.67 for Wal-Mart and 0.43 for Target, confirming that the Target dataset has denser clusters of stores.

The spatial distributions for these nodal layouts (Figure 3.16(b, d)) also show that there are differences between the two datasets. The Wal-Mart stores form a distinct bi-linear distribution due to the area of high nodal density located in Eastern USA, which is also the location of the geographic centre (approximately 130km North-East of St Louis). Whereas the Target stores form a linear spatial distribution, that is affected by the location of the individual clusters in the network (causing a sharp increase in the number of stores for a small change in the distance from the geographic centre).

In order to generate proxies for real world networks, the algorithm must be able to not only generate these large scale distributions, but also replicate the smaller scale attributes of the individual clusters. And as these are dynamic networks (i.e. they 'grow' over a given timeframe), the growth of these individual clusters must also be considered. Three clusters have been isolated from the Wal-Mart dataset (by visual inspection) and are shown in Figure 3.19. It can be seen that each cluster is approximately circular in shape and as such the area covered by each cluster has been calculated by setting the oldest store as the circle midpoint and then calculating the radius of the circle as the distance from this store to the furthest store. This has then been used to calculate the radius of the cluster at each timestep (i.e. from the initial store opening to the final store opening in each cluster) and is also shown in Figure 3.19. From this figure, it can be seen that for the first few stores added to each cluster the radius increases rapidly, but then only increases slightly, if at all, with further opened stores. This is due to the opening of one store close to the outer boundary of

the cluster in an early timestep. The remaining stores then open within this boundary, meaning that the radius of the cluster does not change, or changes only marginally, after a few stores have been opened.

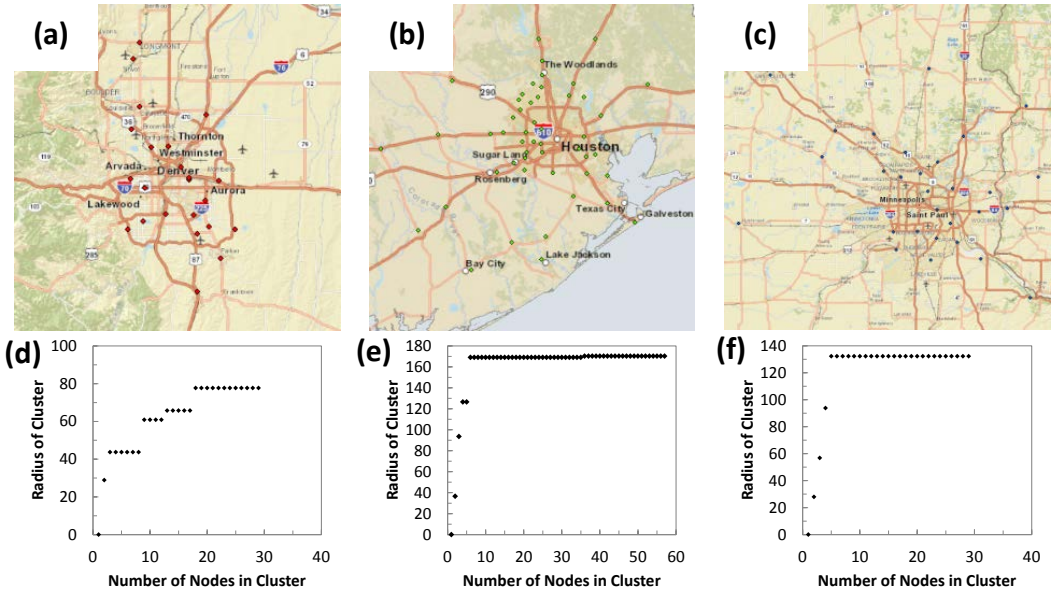


Figure 3.19: Showing three individual clusters from the Wal-Mart dataset: (a) Denver, (b) Houston and (c) Minneapolis, where the dots show the location of stores. The area of each cluster is defined as a circle, where the first store opened is the midpoint (i.e. the first node introduced) and the radius extends from this point to the store furthest from the centre. Graphs showing how the radius of each cluster changes with each opened store have been plotted for each cluster: (e) Denver, (f), Houston and (g) Minneapolis.

From the analysis of these two real world datasets it can be concluded that, even over the same study area, real world nodal layouts can show different characteristics. The Target dataset shows much denser clusters of stores than the Wal-Mart dataset, which also includes a large area of spatially dispersed stores over Eastern USA. Therefore, to be able to model a range of real world networks the algorithm must be able to generate synthetic networks with a different number, location and density of clusters of nodes. The algorithm must also be able to generate individual clusters of nodes where the density of the cluster increases linearly with the addition of new nodes.

The algorithm follows a similar framework to the cellular automata models, outlined in Chapter 2.8; however, this algorithm does not require the input of inaccurate or potentially unobtainable historical datasets, instead all inputs are observed from the present-day layout of the network. Following cellular automata, the algorithm starts with the input of a set of initial conditions from which the nodal layout forms over a given timeframe. This input includes the definition of the spatial boundary of the network and the location of a set of seed nodes (which form a small proportion of the

total number of nodes in the network). However, unlike cellular automata models the location of these seed nodes are not determined from historical data sets (using the first settlements in the study area), but are based upon the identification of clusters of nodes in the present-day dataset. These seed nodes are allocated an initial radius value, which are allowed to change over time, negating the need for regular inputs of historical data (e.g. transportation layers). This radius value is allocated to each node based upon the observed density of the cluster in the present-day network. Using these inputs the network is allowed to 'grow' and the remaining nodes are added individually to the network at each 'timestep' until the total number of nodes is reached.

At each timestep the algorithm determines if an added node will be located within the radius of one of the individual clusters or will be located outside the influence of all of the clusters, depending on a user specified probability value. This probability value is chosen so that the Nearest Neighbour Index of the synthetic nodal layout is close to that of the actual nodal layout. By allowing a small proportion of the total number of nodes in the network to be located outside the cluster radii, a rural environment over the whole of the spatial boundary is represented. If all nodes are allowed to form outside the influence of the cluster radii (i.e. the probability is set at 1) the resulting nodal layout is uniform with area. However, if the added node is to be located inside the radius of a cluster, then this node is 'attracted' to the different individual clusters based upon a calculated probability value. This probability value is dependent upon the density of the cluster and is calculated using Equation 3.7. The probability is not fixed for the whole analysis but rather is recalculated after each node is added. The probability value encompasses the idea that a city, with a high population density, can be expected to have more nodes (representing train stations, for example) than a rural community which has a significantly lower population density.

$$P(cluster) = \frac{number\ of\ nodes_{CLUSTER}}{radius_{CLUSTER}} \qquad \textbf{3.7}$$

With the addition of a new node to the cluster, the radius of the cluster is allowed to expand outwards, in order to simulate the 'growth' pattern of the individual clusters in the network as shown by the real world networks (Figure 3.19). This expansion is logarithmic, meaning that for only a few added nodes the radius of the cluster

increases significantly, but soon reduces to only increasing marginally with further added nodes and been plotted on Figure 3.20 and is calculated using Equation 3.8. The data for the expansion of the Denver cluster in the Wal-Mart dataset is also included in Figure 3.20, where it can be seen that the logarithmic expansion is a good proxy for the real-world data.

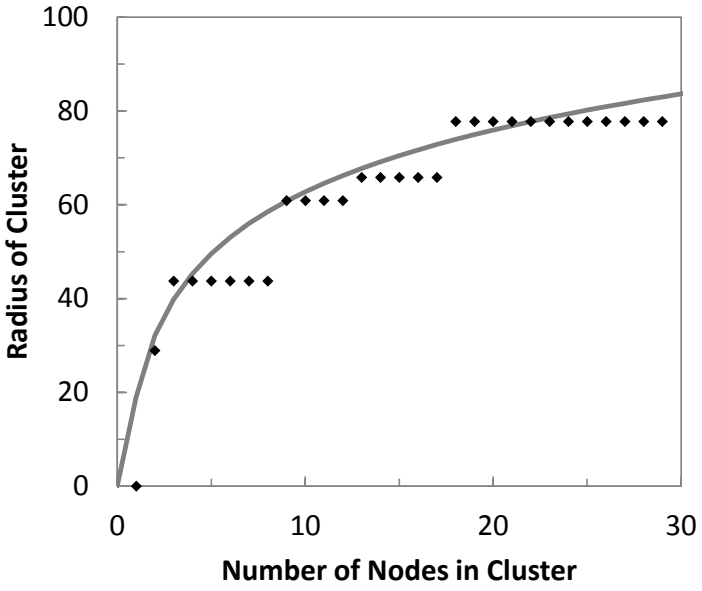


Figure 3.20: Showing the relationship between the number of nodes in an individual cluster and the resulting change in radius of that cluster (grey line) used in the algorithm and the actual relationship between these two variables for the Denver cluster in the Wal-Mart dataset (black dots).

$$Radius = C_D\,(\ln(number\ of\ nodes) + 1) \qquad \textbf{3.8}$$

The algorithm also incorporates variables to alter the density of the network as a whole and that of individual clusters (relative to each other). The C_D term in Equation 3.8 controls the density of the whole nodal layout (i.e. the global density) and has the same effect to each individual cluster of nodes. Its effects can be seen visually in Figure 3.21, where two clustered layouts have been generated using the same initial inputs (i.e. seed location, initial radius size) but a different C_D value. The first nodal layout (Figure 3.21(a-d)) has a C_D value of 200 and the second layout (Figure 3.21(e-h)) has a C_D value of 400. It is worth noting that these C_D values are relative and dimensionless. It can be seen that the larger C_D value results in a nodal layout that has visually less dense clusters than that of the smaller C_D value. Applying the Nearest Neighbour analysis to these two networks, returns an Index value of 0.62 for the

network with a C_D value of 200 and an Index of 0.94 for the network with a C_D value of 400; confirming that a larger C_D value results in a network with less dense clusters of nodes.

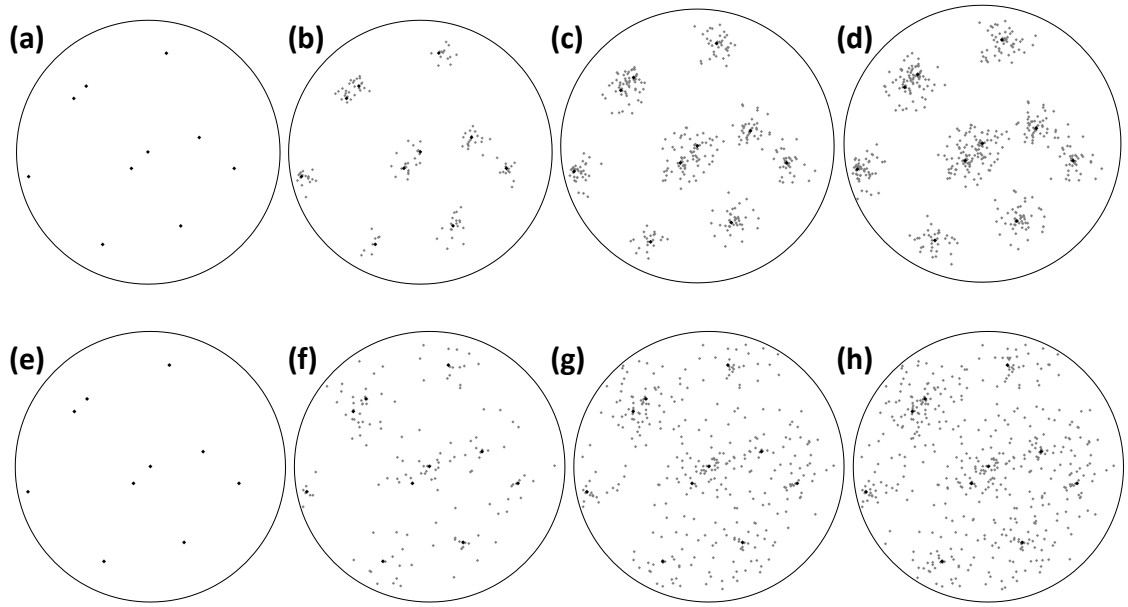


Figure 3.21: Showing the progression of the clustering algorithm for two generated networks ((a)-(d) and (e)-(h)) with different C_D values (200 and 400 respectively). Where the black dots represent the starting nodes and the grey dots show the added nodes, the outer circle defines the spatial boundary of the network. (a) and (e) show the seed nodes (all of the starting nodes have the same radius); (b) and (f) show the layout after 150 nodes have been added; (c) and (g) show the layout after 350 nodes have been added; (d) and (h) show the final nodal layout.

Whilst the C_D term alters the density of the whole nodal layout and has the same effect to each individual cluster of nodes, the density of these individual clusters, relative to each other, can also be altered by changing the initial radius assigned to each seed node. This reflects the different densities of real world clusters of nodes, which can be seen from Figure 3.19. Assigning a seed node a large radius results in a low density cluster (simulating the density of train stations in a rural environment, for example), whilst a small radius results in a dense cluster (for example, simulating the density of housing in an urban setting). Figure 3.22 shows an example nodal layout, with 200 nodes, generated using 3 starting nodes with different radii values. The starting node in the top left of the spatial layout has the largest radius (with a value of 800) and forms the least dense cluster. Whereas, the bottom right cluster has the smallest radius (with a value of 10) and forms the densest cluster. The central starting node has a radius value between these two extremes and therefore has a density value between

the other two starting nodes. Again, it is worth noting that in a similar manner to the C_D value, these values are relative and dimensionless.

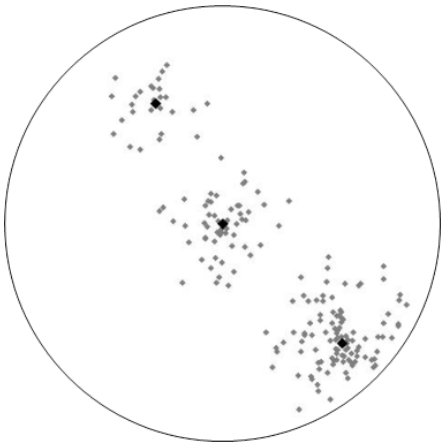


Figure 3.22: Showing three seed nodes (black) with different radii values and the subsequent added nodes (grey). The top left starting node has a radius value of 800, the central starting node has a radius of 500 and the bottom right node has a radius of 10.

The clustering algorithm has initially been verified by generating proxies for the Wal-Mart and Target datasets (previously shown in Figure 3.16). These proxies were generated by defining 30 seed nodes for the Wal-Mart dataset (less than 1% of the total number of stores) and 48 seed nodes for the Target dataset (3% of the total number of stores). The location of these seed nodes was determined by visually identifying clusters of nodes in both networks (using Figure 3.16(a, c)) and these seed nodes were given one of three radii values. A proportion of nodes were allowed to form outside the influence of the clusters in both networks (10% of nodes for the Wal-Mart dataset and 15% of nodes for the Target dataset). The resulting spatial distributions for these proxy networks have been shown, and compared to the real world networks, in Figure 3.23.

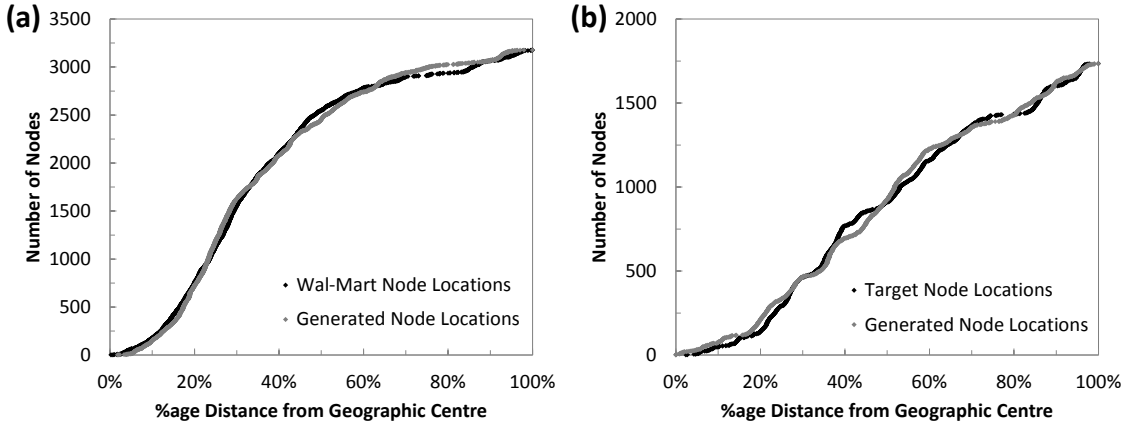


Figure 3.23: Showing the generated spatial distribution of the nodes (grey) compared to the actual distribution of stores (black) for (a) Wal-Mart and (b) Target.

It can be seen from Figure 3.23, that both proxy networks have similar distributions to their real world counterpart, with the exception of the location of a few clusters in the Target dataset (around 40% of the distance from the geographic centre). These proxy networks also have approximately the same Nearest Neighbour Index as the real world networks as shown in Table 3.2.

Table 3.2: Showing the nearest neighbour index values for the actual and proxy Wal-Mart and Target datasets.

Dataset	Nearest Neighbour Index	
	Actual Dataset	Proxy Nodal Layout
Wal-Mart	0.67	0.68
Target	0.43	0.47

The individual clusters in the synthetic networks also show similar characteristics as those of the real world networks, but this is not replicated exactly. For example, Figure 3.24 plots how the radius of the Wal-Mart Minneapolis cluster and its synthetic counterpart changes with opened stores. From this figure it can be seen that the radius of the actual cluster increases at a higher rate than that of the synthetic cluster and that the synthetic cluster also contains more nodes (at the end of the algorithm). This difference is due, in part, to the difficulties in defining individual clusters of nodes in the actual dataset. Figure 3.25 shows the Wal-Mart dataset and highlights the visually defined boundary of the Minneapolis cluster (red line). This line defines a dense area of nodes, but it is difficult to determine if this is the extent of the whole

cluster or if the less dense area (defined by the purple line) should also be included. There is also an additional complication in identifying individual clusters of nodes, as there can be 'overlapping' between nodes of different clusters, particularly for those in close spatial proximity. For the synthetic networks it is possible to establish exactly which nodes form part of each cluster (even if the radius value of two seed nodes overlaps), but this cannot be easily determined for the actual datasets. This can lead to differences between the actual and synthetic networks when viewed on a small scale, but does not impact upon the ability of the algorithm to replicate the spatial configuration of nodes within the network (as shown by the spatial distributions, Figure 3.23).

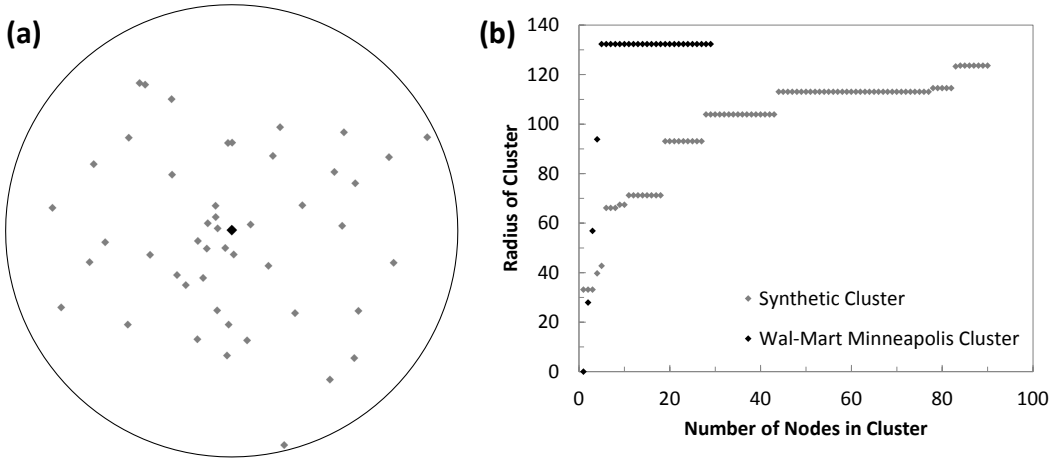


Figure 3.24: Showing (a) one cluster from the proxy Wal-Mart network, where the seed node is shown as a black dot, the added nodes as grey dots and the spatial boundary is indicated by the black line; and (b) showing how the radius of the cluster changes with added nodes.

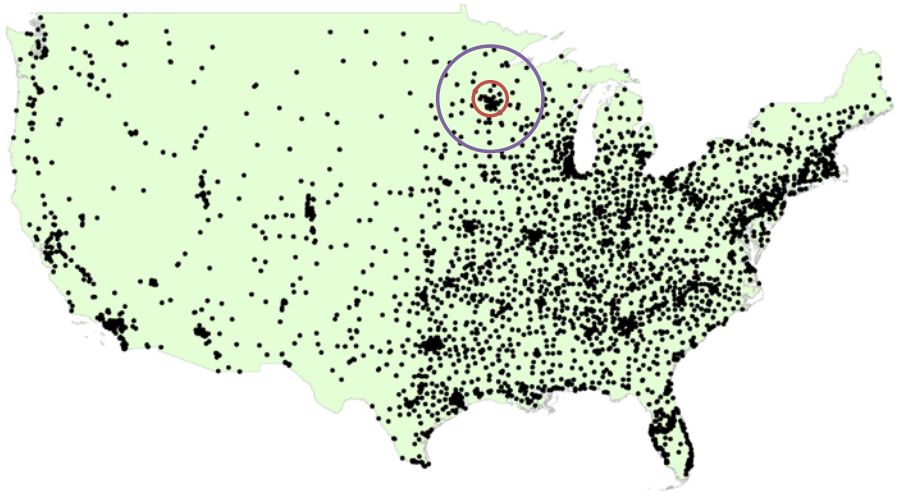


Figure 3.25: Showing the location of stores in the Wal-Mart dataset and highlighting two possible boundaries for the Minneapolis cluster.

After validating the 'clustering' algorithm, by generating synthetic configurations for the stores in the Wal-Mart and Target datasets, a range of synthetic nodal configurations for the EATN have been generated (Figure 3.26). To generate these configurations, 13 seed nodes were defined and assigned one of three radii values (10, 50 or 80). In this algorithm the initial nodes (and their radius values) were chosen in part to approximate the land mass of Europe, and as such, no nodes were allowed to form outside the influence of these clusters. Four additional seed nodes were also used to define the population mass in around Central Europe (all with a radius value of 50). The spatial distribution for the EATN and one of the synthetic nodal configurations have been plotted in Figure 3.26, where it can be seen that the synthetic network is a good proxy for the actual dataset.

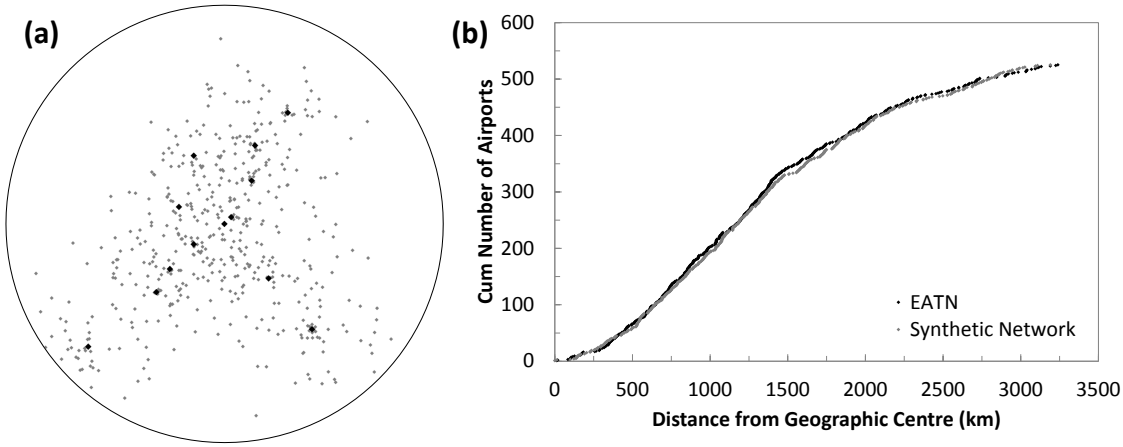


Figure 3.26: (a) Simulated clustered nodal layout for the EATN, where the black dots represent the initial nodes, the grey dots the added nodes and the black line the spatial boundary of the network. (b) A comparison for the spatial distribution of nodes for the EATN (black) and the clustered nodal layout shown in (a) (grey).

To assess the ability of the network generation algorithm to replicate the topological and spatial structure of the EATN, the four different types of synthetic network and three node introduction orders, as previously used to generate the networks with a bi-linear spatial configuration of nodes, have been used. The degree and spatial degree distribution for these synthetic networks have been shown in Figure 3.27 and Figure 3.28, respectively.

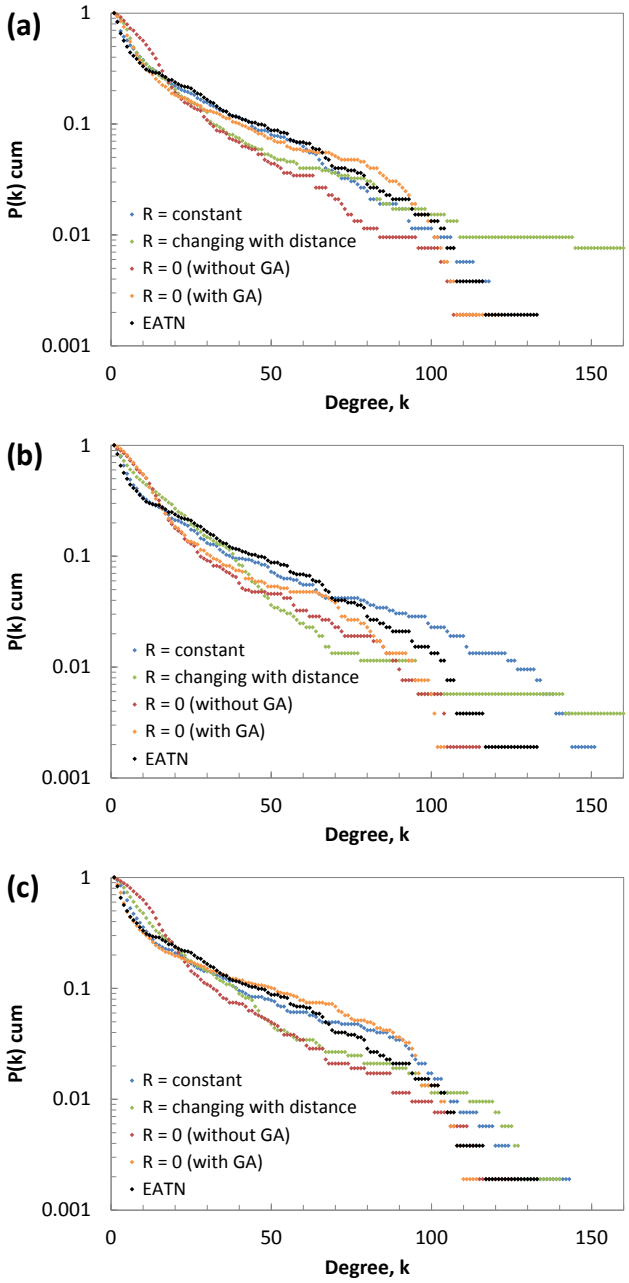


Figure 3.27: Showing the degree distribution for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm with a clustered nodal layout; where nodes are introduced (a) randomly, (b) proportional with distance and (c) with distance from the geographic centre. In the legend, R refers to the size of the neighbourhood radius and GA refers to the modification of Guimera and Albert (2004).

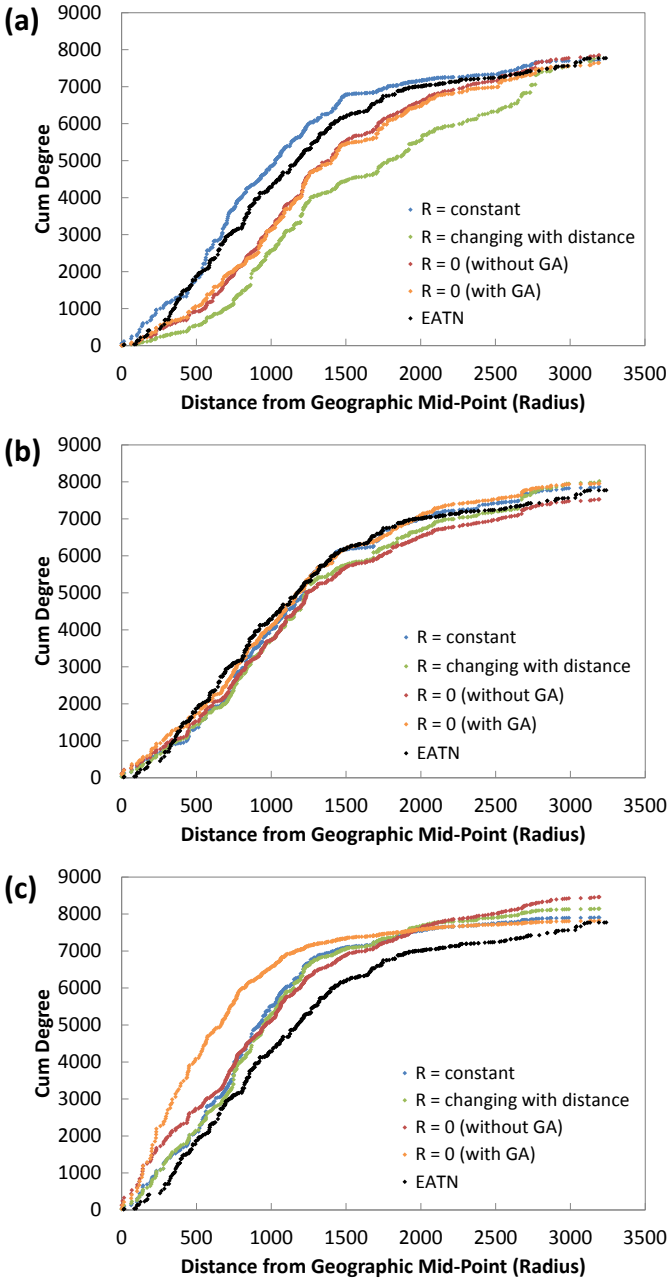


Figure 3.28: Showing the spatial degree distribution for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm with a clustered nodal layout; where nodes are introduced (a) randomly, (b) proportional with distance and (c) with distance from the geographic centre. In the legend, R refers to the size of the neighbourhood radius and GA refers to the modification of Guimera and Albert (2004).

From the degree distributions and spatial degree distributions, shown in Figure 3.27 and Figure 3.28 respectively, it can be seen that the order in which nodes are introduced to the networks again affects both of these distributions. Introducing the nodes proportional with distance results in the formation of the best fit spatial degree distributions (when considering all network types), but compromises the degree distribution of the same networks. Whereas, introducing the nodes randomly can generate a 'lower' spatial degree distribution (meaning that there are too few high

degree nodes around the geographic centre of the network) and introducing the nodes with distance generates a 'higher' spatial degree distribution (meaning that there are too many high degree nodes around the geographic centre of the network).

It can be see that the best combination of degree distribution and spatial degree distribution occurs for the exponential network with a constant neighbourhood size (blue dots) when the nodes are introduced randomly to the network (Figure 3.27(a), Figure 3.28(a)). This is closely followed by the scale-free network, which includes the modification of GA (orange dots); this network produces a good fit for the spatial degree distribution (when nodes are introduced both randomly and proportional with distance), however these networks lack hub airports and include too many low degree nodes. In contrast, the exponential network with a changing neighbourhood size creates hub airports that have too high a degree. The unmodified scale-free network is also not a good proxy for the EATN, as the hub airports do not have a sufficiently high degree and the network includes too many low degree nodes.

These results show the same trend as those previously analysed for networks generated with both the actual EATN airport locations and the bi-linear configuration of nodes. Therefore, it can be concluded that an exponential network, with constant neighbourhood size, and including the GA modification, is the best fit synthetic network for the EATN data (replicating both the topological and spatial characteristics of the network). As such, it can be concluded that links must be allowed to attach between pairs of existing nodes in the network as the network 'grows' and that the decision to form an attachment to an existing airport must be based on spatial location as well as degree.

3.2.1: HAZARD TOLERANCE OF THE SYNTHETIC NETWORKS

The synthetic EATN networks will be subjected to a range of hazards to assess their hazard tolerance and determine if the vulnerability shown by the EATN to the Eyjafjallajökull event is characteristic of the network class and/or spatial degree distribution or if it is unique to the EATN.

The synthetic networks with the bi-linear and clustered nodal layouts will be subjected to a simulated EATN event (as the exact airspace closures cannot be mapped onto these networks); whilst the synthetic networks generated using the actual nodal locations will be subjected to the actual Eyjafjallajökull event. All networks (the actual EATN and the three synthetic networks) will also be subjected to random, but spatially coherent, hazards to assess their hazard tolerance to other locations of the spatial hazard. Random benchmark networks will also be generated with the same number of nodes and links as the actual EATN, and the synthetic networks, and are generated for both a random nodal layout (forming the benchmark in Figure 3.2(b)) and the same configuration as the actual EATN. These random networks will be subjected to the same hazards as the EATN (the actual Eyjafjallajökull event for those with the actual nodal locations and the simulated Eyjafjallajökull event for the random nodal locations) to form a benchmark for resilience for each hazard.

Ten synthetic networks for each nodal layout have been generated using the network generation algorithm developed in the previous sub-chapter. These networks all have a constant neighbourhood size (equivalent to 250km) and include the modification of GA. The nodes were introduced with population for the actual EATN nodal configuration and randomly for the two synthetic nodal configurations. The resulting degree and spatial degree distributions are similar to those previously generated in this Chapter (Table 3.3) It is worth noting, that for the synthetic networks with the bi-linear and clustered nodal layouts a different nodal layout (but one that has the same nodal distribution) is used to generate each of the 10 synthetic networks.

Table 3.3: Showing the relevant Figures for the degree and spatial degree distributions for the generated networks.

Nodal Configuration	Degree Distribution	Spatial Degree Distribution
Actual EATN	Figure 3.8(d)	Figure 3.9(d)
Bi-Linear	Figure 3.12(a)	Figure 3.13(a)
Clustered	Figure 3.27(a)	Figure 3.28(a)

The initial test of hazard tolerance determines if the vulnerability shown by the EATN to the Eyjafjallajökull event is characteristic of its network class, or is unique to the EATN. This is achieved by subjecting the synthetic networks, generated using the

actual nodal locations, to the Eyjafjallajökull event (Figure 3.1). The results of this analysis are shown in Figure 3.29 and are also compared to two random networks, one has the same nodal locations as the EATN and the other has random nodal locations. The results of this analysis show that the synthetic networks are in good agreement with the actual EATN, with the exception of the small hazard areas. This is due to the synthetic networks having the same degree and spatial degree distributions as the EATN, but not necessarily the exact replication of the degree of each node. For example, Gatwick (UK) and Turany (Czech Republic) are both 648km from the geographic centre of the network, Gatwick has a degree of 107 and Turany a degree of 2, exchanging these two degrees will result in the same degree and spatial degree distribution (as they are the same distance from the geographic centre); however, there will be a slight difference in the hazard tolerance to this spatial hazard, as they have different bearings from the geographic centre. If a large number of synthetic networks were generated (say 1000), then a small number would replicate the EATN exactly. However, due to the random elements in the generation of these proxy networks it is possible that some networks will have the same distributions but different placement of the high degree nodes, therefore, causing differences in the hazard tolerance (particularly for small spatial hazards). This effect is also observed in results presented later in this thesis and for clarity will be referred to as 'localisation'.

Plotting the results in terms of the percentage area (airspace) removed (Figure 3.29(b)) shows that both the EATN and synthetic networks have approximately the same hazard tolerance as the random network with the same nodal locations. However, they are more vulnerable than the random networks with random nodal locations. It can therefore be concluded that, for this location of spatial hazard, it is the spatial configuration of nodes within the EATN which causes the inherent vulnerability in the network, rather than solely the placement of the high degree nodes. Although, this is not always the case, as for some locations of the spatial hazard the EATN and the synthetic networks are more vulnerable than the random network with the same nodal locations.

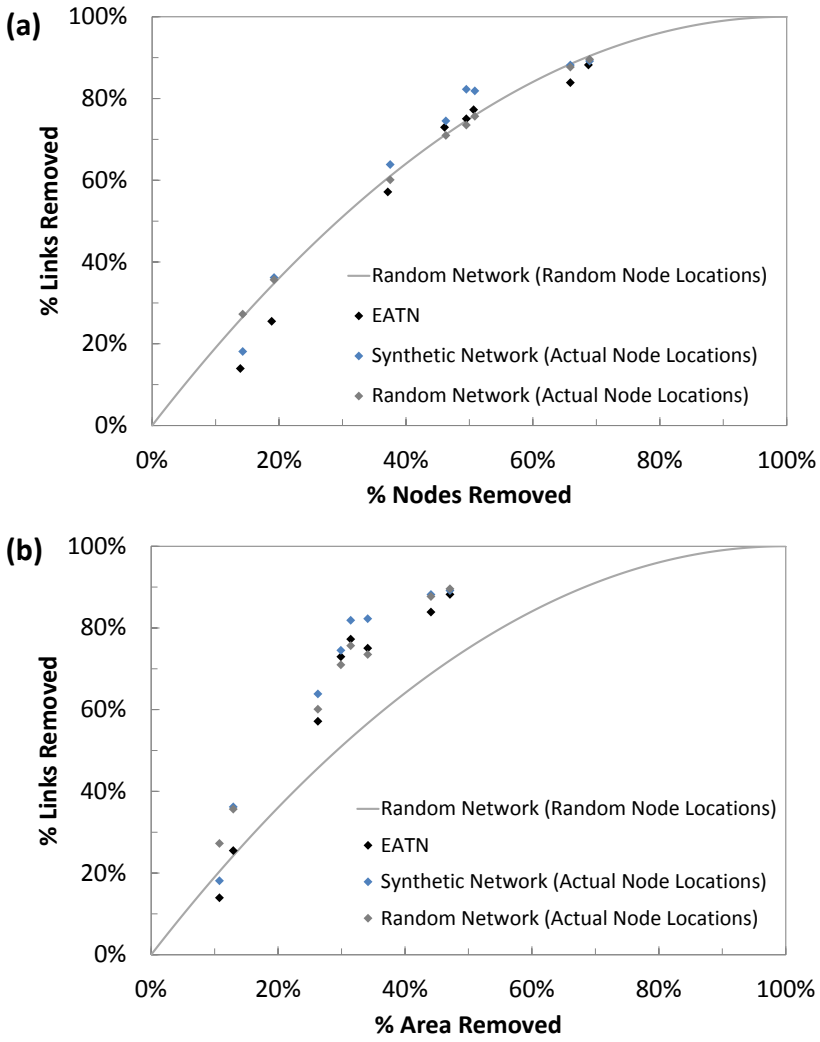


Figure 3.29: The actual EATN (black dots) and the average of 10 synthetic EATN networks (blue dots) subjected to the actual Eyjafjallajökull event, plotting the results in terms of percentage links removed (i.e. percentage of closed air routes) and (a) percentage of nodes removed (i.e. percentage of closed airports) and (b) percentage area removed (i.e. proportion of closed air space). Also shown are two random networks, one with the actual EATN nodal locations (grey dots) and the other with random nodal locations (grey line).

To further confirm that the vulnerability of the EATN is attributed to the unique nodal layout of the network, the synthetic networks with the bi-linear nodal layout and clustered nodal layout are subjected to a simulated Eyjafjallajökull event. These networks have the same nodal configuration as the EATN (Figure 3.7(a)), but a different nodal layout and are also enclosed in a circular boundary to represent the extent of the airspace. To simulate the Eyjafjallajökull event, a circular hazard will be placed at the edge of the spatial boundary and allowed to grow outwards until the whole of the network area is covered (Figure 3.30).

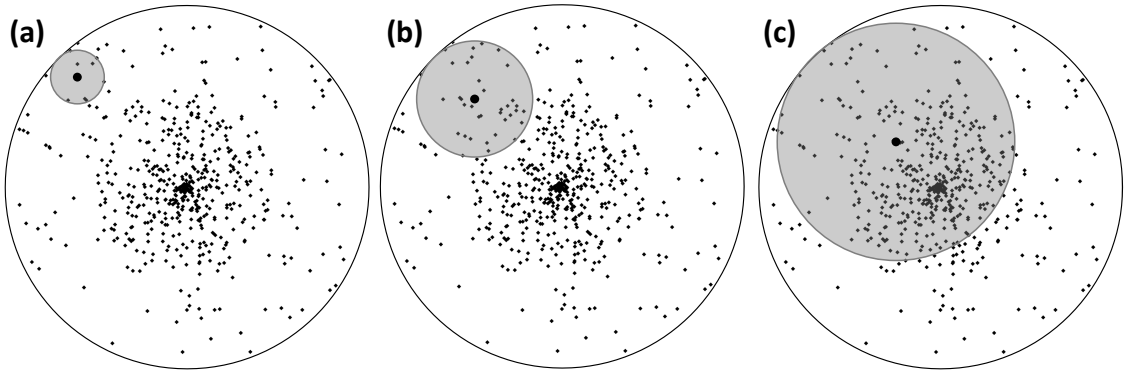


Figure 3.30: Showing three sizes of the simulated Eyjafjallajökull event, in which the hazard starts at the spatial boundary of the network (black line) and grows outwards until the whole network area is covered (i.e. from (a) to (b) to (c)).

The results for these simulations have been compared to the actual Eyjafjallajökull event for the EATN and to the random network, with a random nodal layout in Figure 3.31. Due to the progressive nature of the simulated Eyjafjallajökull hazard (i.e. it 'grows' outwards) the results can be plotted as a line (produced from 10 simulations of the spatial hazard for each nodal configuration), rather than the individual points used for the actual Eyjafjallajökull event. Plotting the results in terms of the percentages of nodes and links removed shows that the results (for both the bi-linear and clustered nodal layouts) are in good agreement with the actual Eyjafjallajökull event and show approximately the same hazard tolerance as the random networks. This can be attributed to the random order in which nodes were introduced to the synthetic networks, causing the high degree nodes to be dispersed throughout the network (Figure 3.14(c)). Therefore, when one high degree node is removed from the network many lower degree nodes are also removed, negating the impact of the removal of the high degree node.

However, when the results are plotted in terms of the percentages of removed area and links both the synthetic networks and the actual EATN have a different hazard tolerance than the random networks with a random nodal layout (Figure 3.31(b)). For small sizes of the spatial hazard, up to 20% of the area, the synthetic networks are more resilient than the random networks and for hazards larger than this 20% network area they are more vulnerable. The results showing the percentage of nodes removed (Figure 3.31(a)) shows that this sharp increase in vulnerability is not due to the removal of the high degree nodes (hub airports), but is instead due to the removal of a large percentage of nodes for a small increase in the hazard size. Therefore, it can be

concluded that it is the nodal layout of the EATN which renders it vulnerable to larger sizes of the Eyjafjallajökull event spatial hazard. However, as the majority of nodes are located close to the geographic centre of the network, the networks are resilient to hazards which remove the area close to the spatial boundary of the network (i.e. small sizes of the Eyjafjallajökull event).

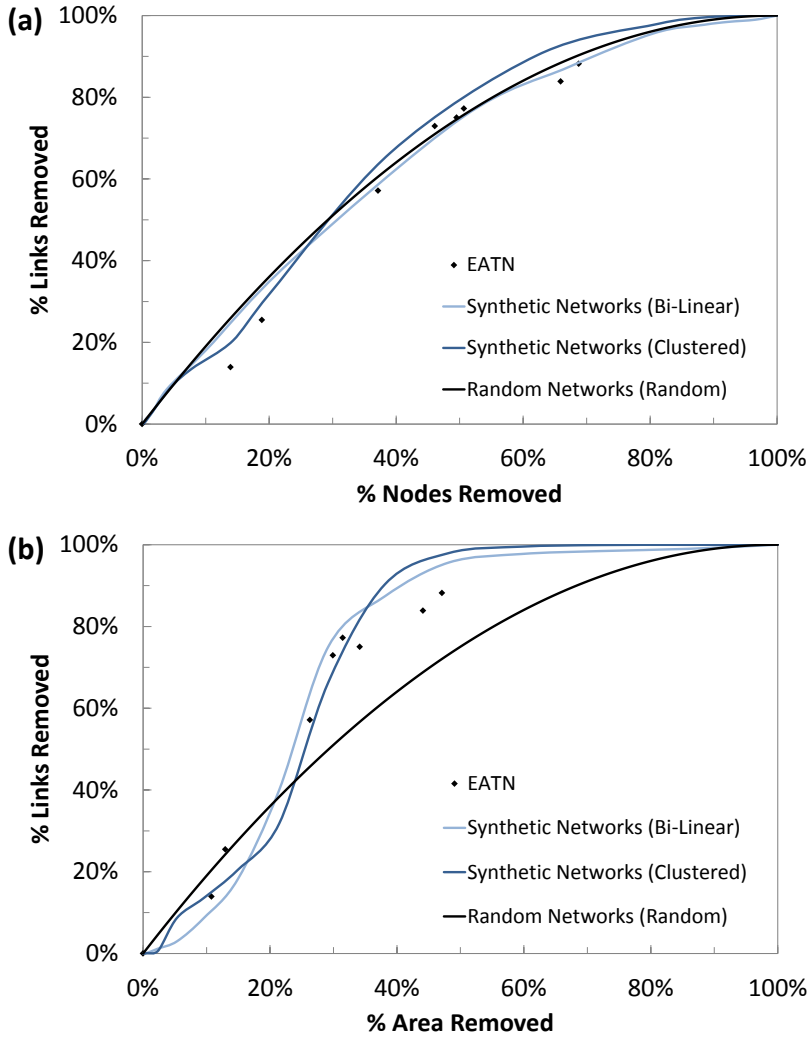


Figure 3.31: The actual EATN (black dots) subjected to the Eyjafjallajökull event and the average of 10 synthetic networks for both the bi-linear (light blue line) and clustered nodal layouts (dark blue line), subjected to a simulated Eyjafjallajökull event (Figure 3.30). Also showing one random network with random nodal locations (black line). The results are plotted in terms of the percentage of links removed and the percentage of (a) nodes and (b) area removed.

To determine the hazard tolerance of the EATN, and the synthetic networks, to other random (but coherent) spatial hazards, the networks are subjected to 20 random hazards (of different sizes and locations). Typical positions, and sizes, of the random hazards have been shown in Figure 3.32 to show their generic shape. Unlike the simulated Eyjafjallajökull event, these hazards do not 'grow' to cover the whole of the

spatial area of the network. They are one size only and provide a 'snapshot' view of the hazard tolerance; therefore, the results are plotted as a series of points and not as a line. To generate these hazards a random x- and y-coordinate are generated, along with a random radius. The hazards have been applied initially to the actual EATN and to the synthetic networks with the same nodal locations as the EATN. These hazards have then been translated onto the synthetic nodal layouts, with a different coordinate system (as they are not located on the curved surface of the Earth). Due to the different co-ordinate systems used it is not possible to replicate the hazard exactly; however, the same distance and bearing from the geographic centre of the network is maintained and therefore the effect to the analysis is deemed to be minimal.

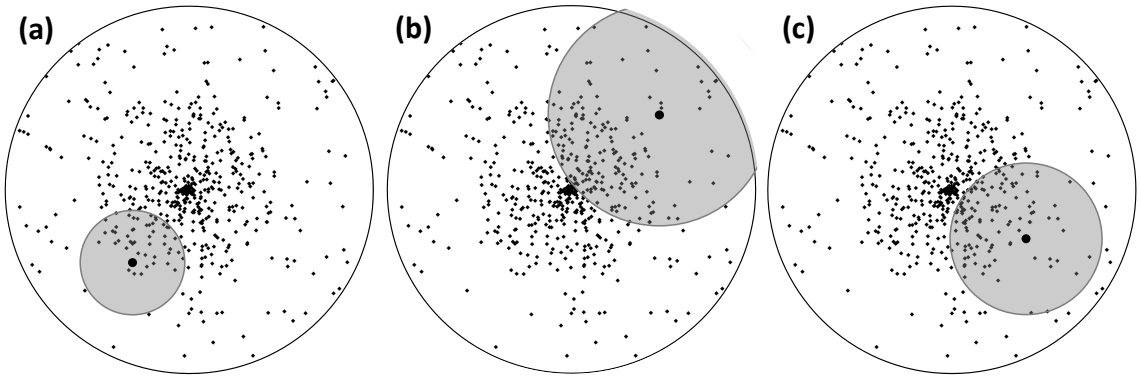


Figure 3.32: Showing three locations and sizes of the simulated random spatial hazard, the centre of the hazard is a randomly generated point within the spatial boundary of the network and has a randomly generated radius value. Unlike the simulated Eyjafjallajökull event (Figure 3.30), these hazards do not 'grow' outwards.

The hazard tolerance of the EATN and its synthetic counterparts are shown in Figure 3.33. The results for the synthetic networks are in good agreement with the EATN (although there is a reasonably large scatter) for the majority of the random hazards, with a few exceptions, which tend to occur when the hazard size is small. For example, there are a few positions of the random hazard to which the EATN is resilient (removing between 10% and 30% of the nodes, Figure 3.33(a)), which are not replicated by the synthetic networks. This is due to the synthetic networks replicating the degree and spatial distributions of the EATN, but not necessarily the exact degree of each node, as previously discussed.

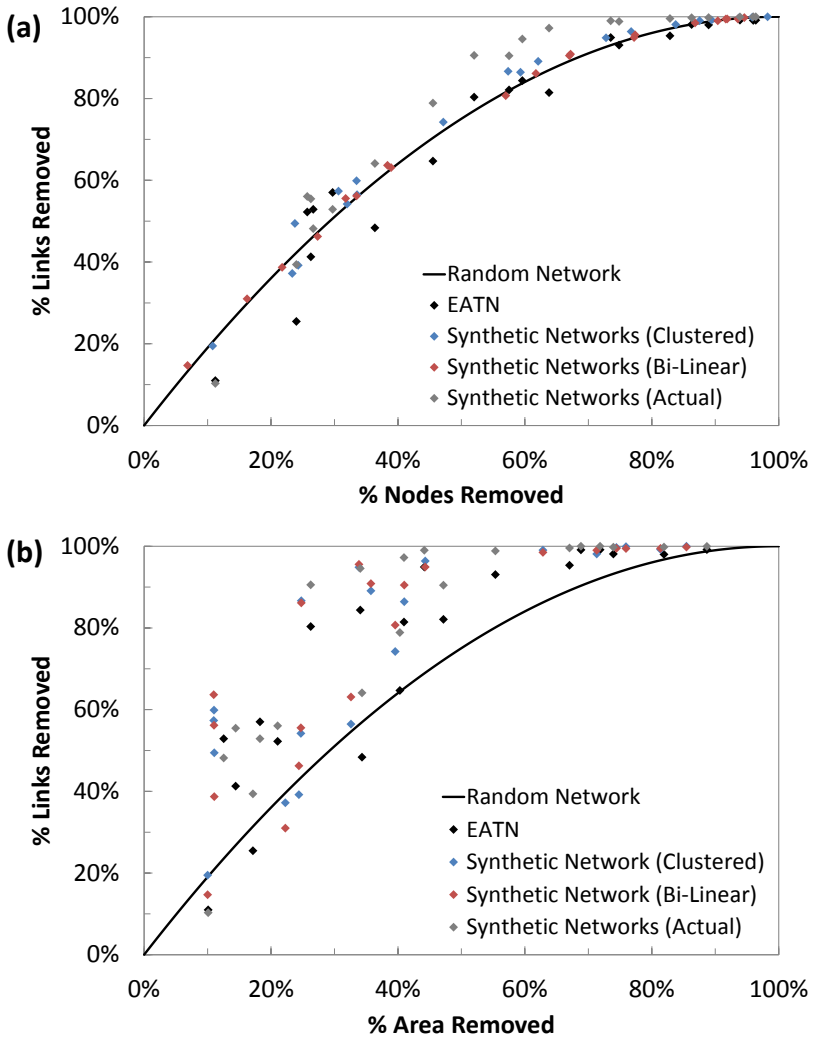


Figure 3.33: The actual EATN (black dots) subjected to a random spatially coherent hazard and the average of 10 synthetic networks for the bi-linear (red dots), clustered (red dots) and actual (grey dots) subjected to the same random spatially coherent hazards. Due to the differences in the co-ordinate systems there are slight variations in the percentage area calculated between the actual and synthetic networks (i.e. the actual network is on a curved surface and the synthetic networks are on a flat surface).

There is a significant difference in the perceived hazard tolerance of the EATN, and the synthetic networks, when the results are plotted in terms of the percentage area removed rather than the percentage nodes removed. For example, it can be seen from Figure 3.33(b) that there are four sizes of the spatial hazard (around 10-15% of the area removed) to which the EATN shows a different hazard tolerance from the synthetic networks and indeed the synthetic networks show a different hazard tolerance to each other (ranging from 10% to 53% links removed for these four hazards). This change in hazard tolerance can be attributed to the location of the spatial hazard over the network. Figure 3.34 plots these four positions of the spatial hazard over the actual EATN and from this figure it can be seen that two positions of the spatial hazard occur close to the edge of the airspace (Figure 3.34(a, d)). Due to

the spatial distribution of nodes in the network, hazards located close to the edge of the airspace remove fewer nodes than those located close to the geographic centre of the network. Therefore, when the results are plotted in terms of the percentage area and links removed there is a significant difference between the hazard tolerance of the EATN for these four random hazards (Figure 3.33(b)), which is not evident when plotting the percentage of nodes and links (Figure 3.33(a)). The hazard tolerance of the actual EATN is closely replicated in the synthetic networks with the same nodal locations, but not in the networks with the synthetically generated nodal layouts. This is due to the synthetic nodal configurations having the same spatial distribution of nodes as the EATN, but not the exact placement of nodes, causing the 'localisation' effect as previously discussed. It can therefore, be concluded that it is the combination of hazard size and location which affects the hazard tolerance of a network.

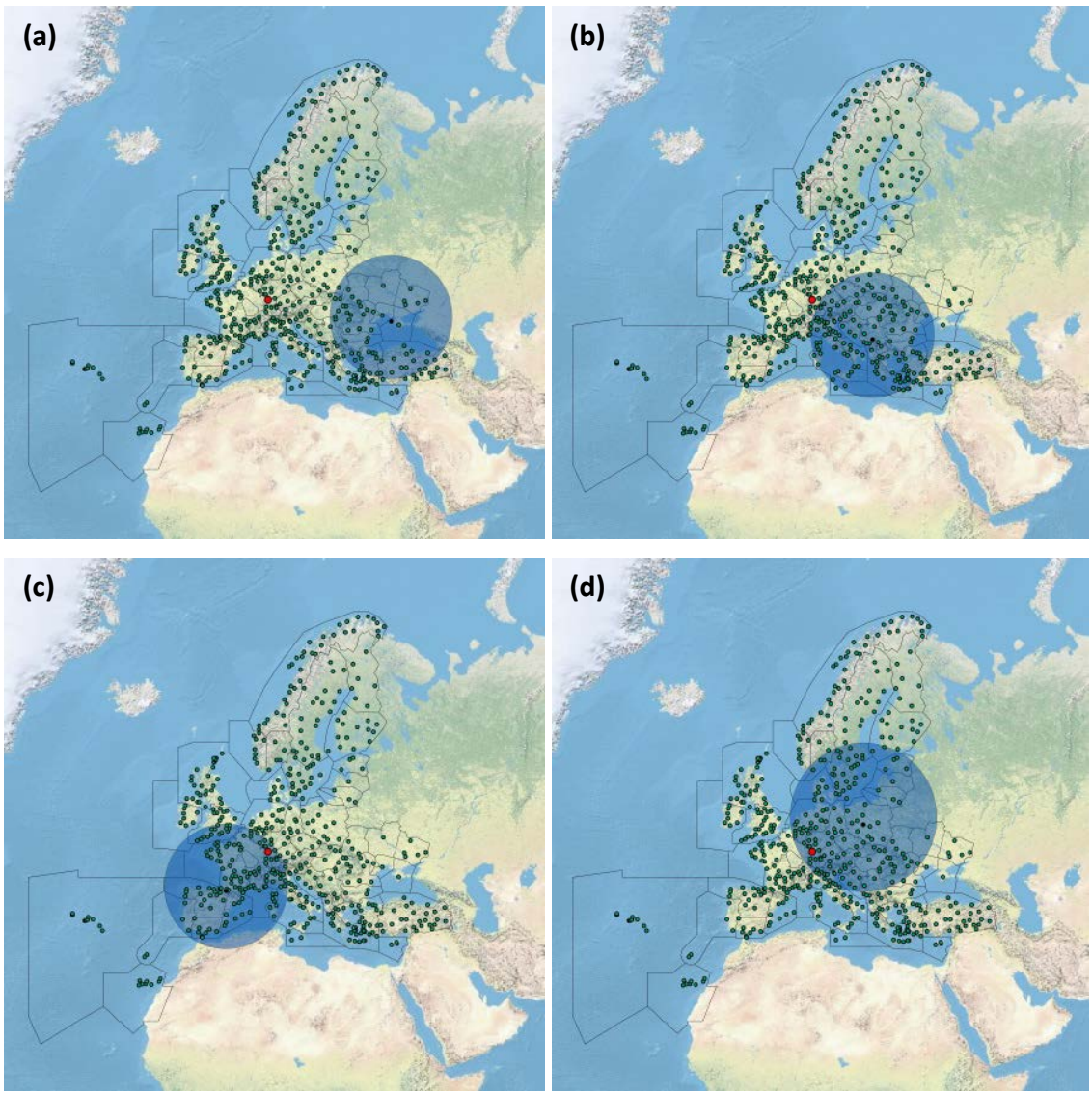


Figure 3.34: GIS generated impacts showing four positions of the random spatial hazard over the EATN, with approximately the same hazard area (around 10%) where the airports are shown as green dots, the weighted geographic centre is shown as a red dot, the FIRs are indicated by the black lines, the centre of the random spatial hazard is shown by a black dot and the shaded blue circle indicates the size of the hazard. It is worth noting, that only the area of the hazard which lies within the FIR of the EATN is considered as part of the hazard area.

To determine the effect of removing the area of high density nodes around the geographic centre of the network a further spatial hazard is used - the 'central attack' spatial hazard, shown in Figure 3.36. In this assessment of hazard tolerance, the centre of the hazard is fixed on the geographic centre of the network and the hazard is allowed to grow outwards from this point to the spatial boundary of the network (i.e. the extent of the airspace). Unlike the simulated Eyjafjallajökull event, the centre of the hazard is fixed as the hazard increases in size.

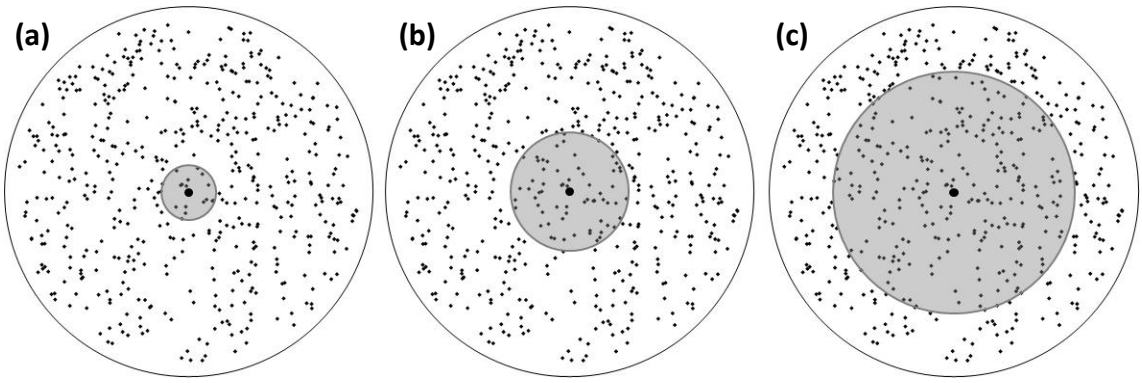


Figure 3.35: Showing three sizes of the simulated 'central attack' spatial hazard, in which the hazard starts at the spatial centre of the network and grows outwards until the whole network area is covered (i.e. from (a) to (b) to (c)).

This hazard has been applied to the actual EATN only and the results compared with those for the actual Eyjafjallajökull event and the random network, with random nodal layout (Figure 3.36). From these results it can be seen that removing the spatial area around the geographic centre of the hazard has a devastating effect to the EATN; when the hazard is only 5% of the network area over 40% of the links have been removed (this compares to a removal of less than 10% of links in the random network, for the same hazard size). Therefore, spatial hazards which remove the area of high nodal density around the geographic centre will render the EATN vulnerable and demonstrates that the actual EATN is vulnerable not only to the Eyjafjallajökull event, but also to other locations of a spatial hazard. For example, winter storms have caused disruption to air travel within Europe in recent years, with an event in 2010 causing the cancellation of 30% of flights from Orly and Charles de Gaulle airports in Paris and '*severe restrictions*' to the number of flights leaving London Heathrow (Jolly and Werdigier 2010).

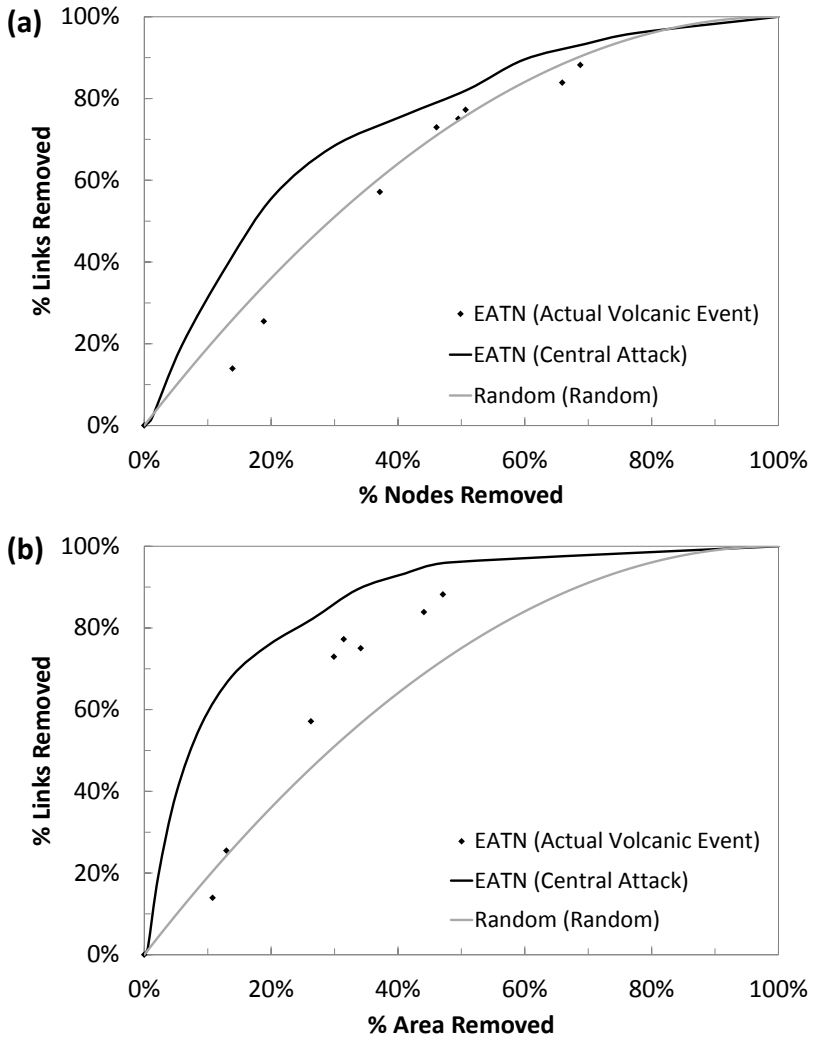


Figure 3.36: Showing the actual EATN subjected to the actual volcanic event (black dots) and also subjected to the 'central attack' spatial hazard (Figure 3.35) (black line). Also showing a benchmark random network, with random nodal location (grey line). The results are plotted in terms of the percentage of links removed and the percentage of (a) nodes and (b) area removed.

3.2.2: APPLICATION OF NETWORK MEASURES TO QUANTIFY CHANGE IN PERFORMANCE AND CONNECTIVITY

The assessment of the hazard tolerance of the EATN, and its synthetic counterparts, has so far focused on quantifying changes in the percentages of nodes/area/links removed for different locations and sizes of spatial hazards (i.e. the quantification of the proportion of closed, or removed/failed, infrastructure components). These results can be further analysed to provide information regarding the percentage of cancelled flights, number of delayed passengers, etc. This information is useful when considering the potential impacts of a hazard; however, these results do not give an

indication into the efficiency of the remaining network, or to the connectivity of the network. For example, there may be relatively few flights cancelled, but if these flights are those which are considered to be 'crucial' to flight operations then passengers could expect to experience severe delays. This information cannot be obtained by studying these results alone. To determine how the efficiency and connectivity of a network changes with an applied hazard, network performance measures must be applied: namely, MCS and APL (refer to Chapter 2.5.4 for details of these measures). In this Chapter, these measures are applied to the results of the actual and simulated Eyjafjallajökull event to gauge how the networks degrade as the hazard increases in size. The MCS and APL of the EATN and three synthetic networks have been calculated and are presented in Figure 3.37, plotted against both the percentages of nodes and area removed. The random network, with random node locations, is also included in these graphs as a benchmark for resilience. It is worth noting that for the actual Eyjafjallajökull event (for the EATN and applied to the synthetic network with the same nodal locations) the results are plotted as points only, as this hazard size does not 'grow' across the network unlike the simulated Eyjafjallajökull event (where the results are plotted as a line).

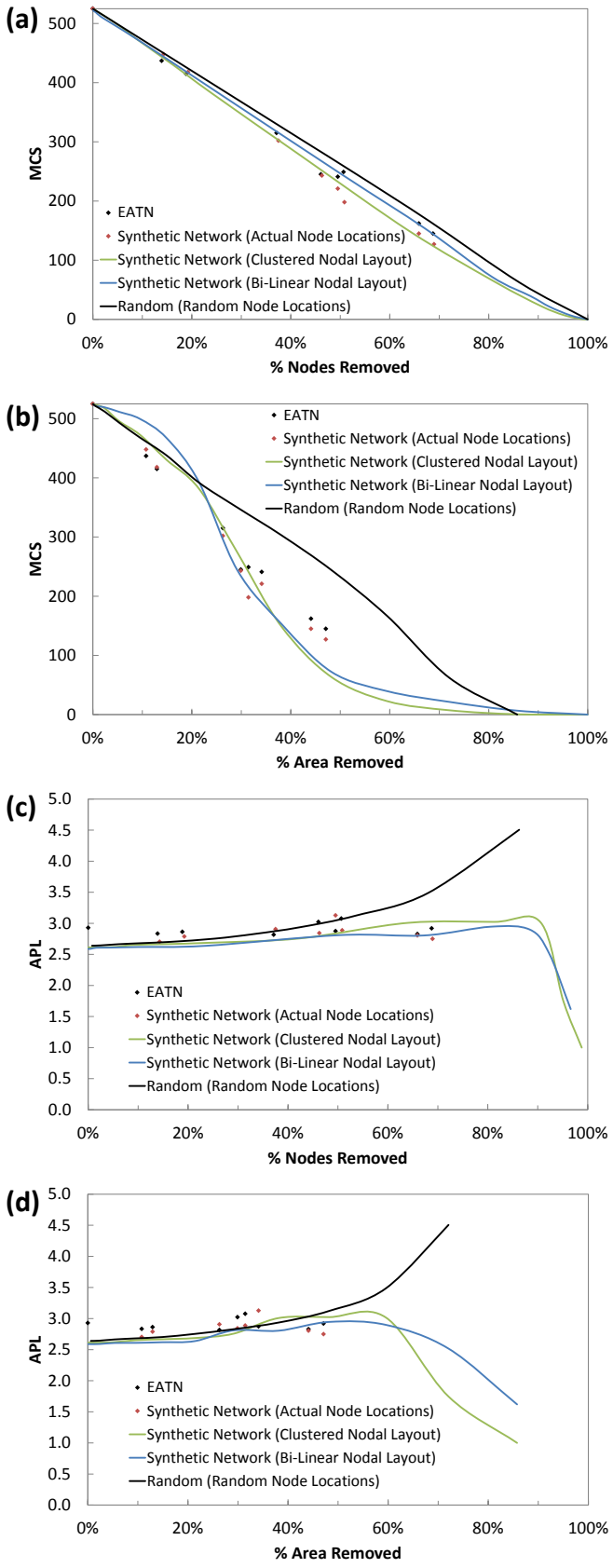


Figure 3.37: Showing the change in (a, b) MCS and (c, d) APL for the EATN and the average of 10 synthetic networks when subjected to the actual / simulated Eyjafjallajökull events.

From Figure 3.37 it can be seen that the results for the synthetic networks are generally in good agreement with the EATN, particularly when the results are plotted in terms of the percentage nodes removed. Comparing the MCS results to the random network, shows that the actual EATN and the synthetic networks have approximately the same resilience as the random network when plotting the results in terms of the percentage nodes removed as per existing theory (Figure 3.37(a)). However, when the results are plotted in terms of the percentage area removed the hazard tolerance of the EATN and the synthetic networks dramatically changes. The synthetic networks are initially resilient to small sizes of the spatial hazard and become increasingly vulnerable as the hazard size increases, becoming vulnerable after around 20% of the network area has been removed (compared to the random network). This resilience to small sizes of the Eyjafjallajökull hazard is not replicated by the actual EATN. This can be attributed to the differences between the actual Eyjafjallajökull event and the simulated hazard. The simulated hazard starts at the outer boundary of the network and 'grows' inwards (Figure 3.30), whereas the actual event was, on certain days, not spatially coherent (i.e. the hazard affected FIRs that were not connected). Therefore, the actual hazard could have removed a small proportion of the dense area at the centre of the network, which is not replicated in the simulated Eyjafjallajökull event (shown in Figure 3.30). The dramatic decrease in the resilience of the EATN and synthetic networks, compared to the random network, can be attributed to spatial distribution of nodes within the EATN. There is a high concentration of nodes around the geographic centre of the network, therefore when these nodes are encompassed by the spatial hazard the percentage of nodes removed dramatically increases compared to the percentage of area removed. This in turn affects the MCS of the network, as nodes are removed the MCS decreases significantly for a small increase in the hazard size. Considering the correlation between the MCS and the percentage of nodes removed shows that the vulnerability of the EATN (and synthetic networks) is caused by the location of nodes, rather than the arrangement of links (as the networks have the same resilience as the random network when plotted in terms of the percentage nodes removed).

Figure 3.37(c, d) shows that the APL of the EATN and the synthetic networks does not noticeably change until over 80% of nodes or 60% of the network area are removed.

Therefore as APL is a measure of efficiency, this suggests that although these networks have broken into clusters the largest cluster in the network is still efficient at transferring service (in this case, air passengers or aircraft). However, it should be noted that once the APL starts to drop it should no longer be considered a valid measure (due to the reduction in the size of the largest cluster as discussed in Chapter 2.5.4). Comparing the results to the random networks shows that the EATN and the synthetic networks are more resilient, as the random network has a higher value of APL for the same percentage nodes / area removed (after 40% of nodes or 50% of area is removed). These results for the APL suggest that air passengers were able to reach their destination airport with relatively few changes during the Eyjafjallajökull event, as long as their destination airport was not encompassed by the ash cloud; although, this calculation of APL does not account for the availability of aircraft. Many airlines operate a hub and spoke system, meaning that their air routes are orientated around one central airport and if this central airport is encompassed by the ash cloud then all of the aircraft in their control would be unable to fly (as they cannot fly from an unaffected airport to the closed central airport and vice versa). However, if one of the 'spoke' airports was to be affected by the ash cloud, then the other air routes (from the hub airport) would be operational and the airline as a whole would remain largely unaffected by the hazard. Therefore, the APL gives an insight into the efficiency of the system, but should not be considered in isolation in a full analysis. Studying the impacts of specific cancelled flights due to aircraft unavailability is outside the scope of this work (this would require a weighted network, which is outside the scope of this research), but should be considered by individual airlines when assessing their own individual hazard tolerance.

It is interesting to note that in Figure 3.37 the random and synthetic networks show a higher efficiency than the actual EATN under normal operational conditions (with an APL value of 2.64 for the random networks, compared to 2.93 for the EATN). This could be due to the slight differences in the number of links in the generated networks (as it can be difficult to generate a random or exponential network with an exact number of links), however as this difference is less than 2% of the total number of links for all generated networks this is unlikely. This difference in efficiency is more likely to be due to the saturation of the network (i.e. the ratio of nodes and links). To

demonstrate this effect 20 random and exponential networks (generated using the same properties as the 'best fit' EATN network), with different numbers of links and 525 nodes, have been generated and their APL calculated. The relationship between these two parameters is shown in Figure 3.38, where it can be seen that these parameters follow a power law relationship for both networks. From this figure, it can also be seen that for a small number of links the exponential network is the most efficient, due to the more 'sophisticated' network generation algorithm forming 'hub' nodes which connect the majority of lower degree nodes making the network easy to navigate. However, as the number of links increases, and the networks move towards saturation, the random networks show a higher efficiency than the exponential networks. This is due to the increased in connectivity in the random networks, meaning that two nodes chosen at random are now more likely to be connected; whereas, two nodes chosen at random in the exponential network are still likely to be connected via a high degree network, forming a longer path between the two nodes and a more inefficient network.

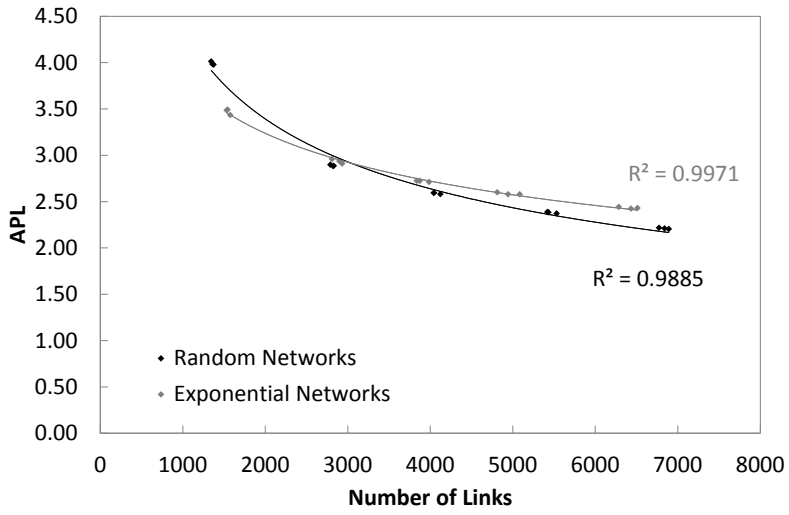


Figure 3.38: A comparison between the number of links in a network and its shortest average path length (APL) for random networks (black) and exponential networks (grey). The trend lines for both the random and exponential networks follow a power law.

3.3: HAZARD TOLERANCE OF OTHER AIR TRAFFIC NETWORKS

This chapter has so far assessed the vulnerability of the EATN to a variety of spatial hazards, including the actual Eyjafjallajökull event. This has included the generation of synthetic networks (forming proxies for both the nodes and links) to determine if the vulnerability shown by EATN to the Eyjafjallajökull event, and to other spatial hazards, is unique to the EATN or is inherent of its network class and/or spatial distribution. This sub-chapter will consider whether the vulnerability of the EATN (and the synthetic networks) is characteristic and inherent to air traffic networks and whether other air traffic networks show the same degree and spatial distributions as the EATN. To achieve this, air traffic networks of the China and US have been obtained from Openflights (2010) and in a similar manner to the EATN only the presence of an air route is considered and only flights between airports in these networks are considered (e.g. intercontinental flights are discarded). Proxies for the location of nodes and arrangement of links within these two networks will be generated (using the algorithms developed for the EATN) and the actual and synthetic networks will be subjected to the central attack spatial hazard (Figure 3.35) to assess their inherent hazard tolerance. The spatial distribution of airports in both of these datasets has been shown in Figure 3.39.

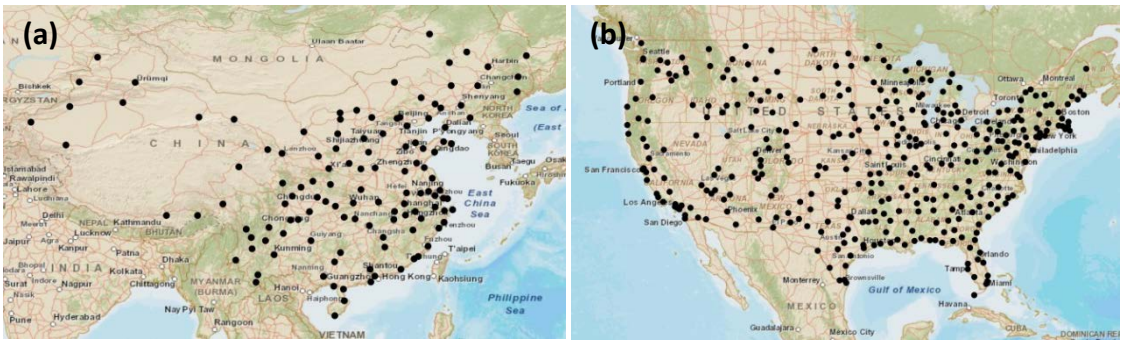


Figure 3.39: Showing the airport locations of the (a) China and (b) US air traffic networks.

The China air traffic network (CATN) consists of 124 airports and 828 air routes, while the US air traffic network (USATN) consists of 363 airports and 2289 air routes; the degree distributions for both networks are plotted in Figure 3.40. It can be seen that these two networks have similar degree distributions to the EATN (Figure 3.3) and can be classed as a truncated scale-free network (or a scale-free network with an exponential 'tail'). Therefore, both of these air traffic networks should be resilient to

random hazard and vulnerable to targeted attack. It can be seen from Figure 3.40(a, b) that the CATN includes one airport with a degree that is significantly larger than the next highest degree airport in the network, namely, Beijing Capital International Airport (as illustrated by the 'windowing' issue).

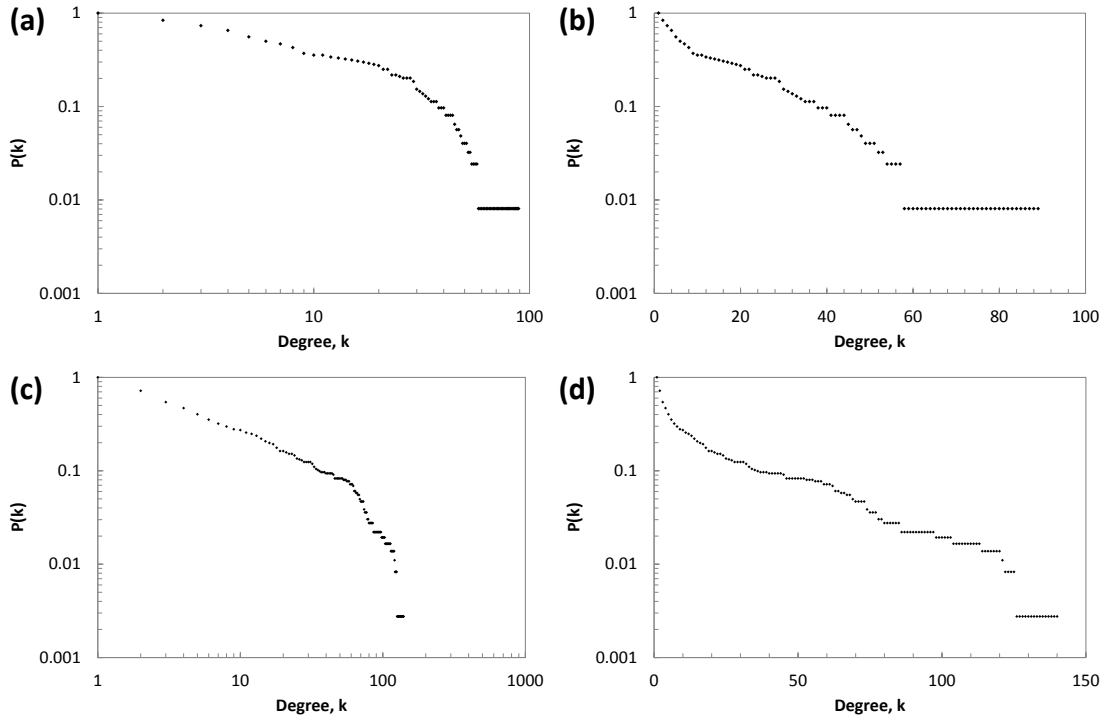


Figure 3.40: Showing the degree distribution, plotted on a log-log and log-linear scales, respectively, for the (a, b) China and (c, d) USA air traffic networks.

The spatial distribution of nodes and the spatial degree distributions for these two air traffic networks have been obtained using the same methods as applied to the EATN (Figure 3.7) and have been plotted in Figure 3.41. It can be seen that these two distributions are again similar to those obtained for the EATN as they both form an approximate bi-linear distribution. However, both air traffic networks are lacking the high concentration of nodes very close on the geographic centre of the network (within 250km), although there is a high concentration of nodes close to this area in both networks. This lack of airports around the geographic centre of the networks means that generating a synthetic nodal layout using the bi-linear representation is not a good fit for the data, as shown in Figure 3.42; therefore, this method of generating a nodal layout will not be used for both the CATN and the USATN.

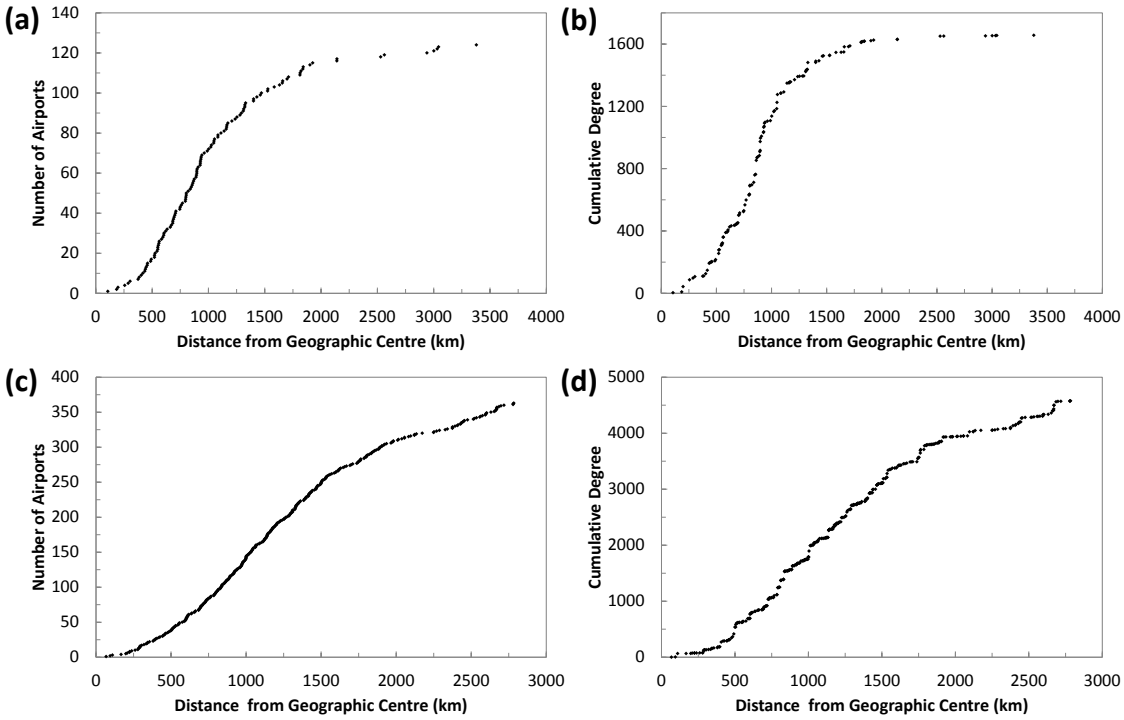


Figure 3.41: Showing the spatial distribution of airports and the spatial degree distribution, respectively, for the (a, b) China and (c, d) USA air traffic networks.

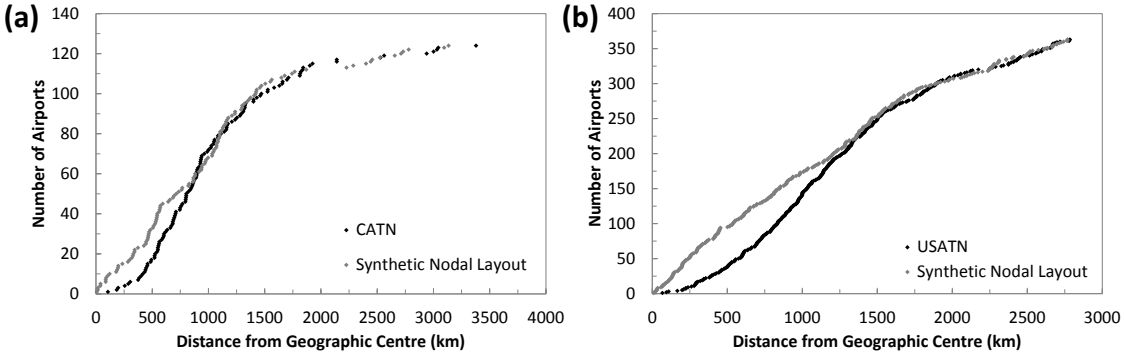


Figure 3.42: Showing the spatial distribution of nodes for (a) the China air traffic network and (b) the US air traffic network and a generated bi-linear nodal configuration.

Once the degree and spatial distributions have been obtained for the datasets, the synthetic networks for each air traffic network can be generated. In a similar manner to the EATN, the synthetic networks will be generated using the actual nodal layout and a synthetic clustered nodal layout. The links between nodes will be generated using the network generation algorithm, developed for the EATN, to determine whether it simulates the rules governing air route formation in other air traffic networks.

3.3.1: GENERATING SYNTHETIC NETWORKS FOR THE CHINA AIR TRAFFIC NETWORK

To assess the ability of the network generation algorithm, previously developed in this Chapter, to form proxy networks with the same topological and spatial characteristics as other air traffic networks, the algorithm is used to form a proxy for the CATN. This is achieved using the actual airport locations, where nodes are introduced using the same four node introduction orders as previously used to generate the EATN (introducing nodes with distance, proportional with distance, randomly and with population). The same four types of synthetic network are also generated to assess the 'rules' which govern the formation of links within the CATN. The resulting degree and spatial degree distributions for these synthetic networks are shown in Figure 3.43 and Figure 3.44. In these figures, only the results where the nodes have been introduced with population and randomly are shown (due to space restrictions), as these two introduction orders produced the 'best fit' data.

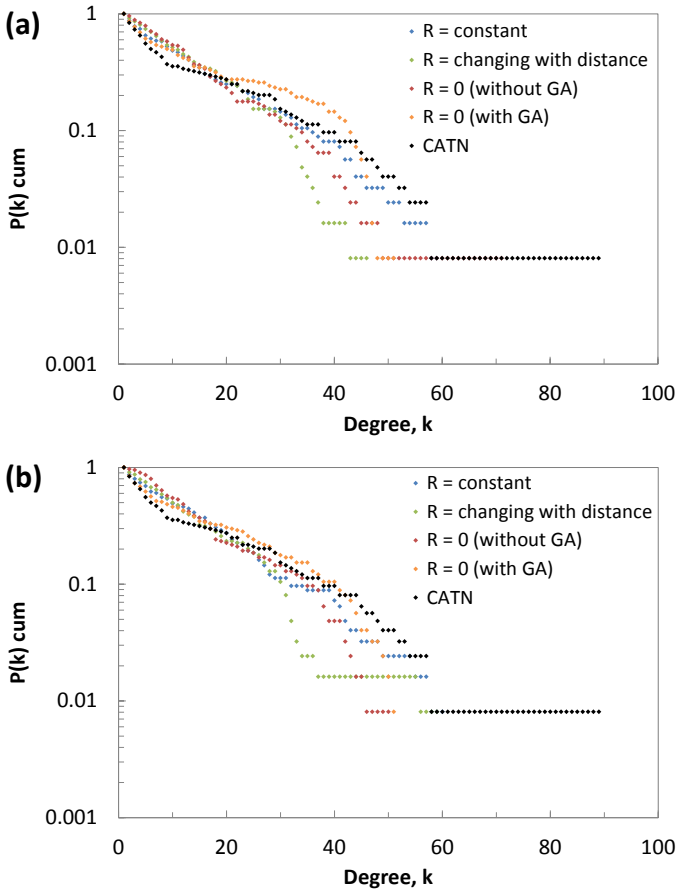


Figure 3.43: Showing the degree distribution for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm for the actual node locations, where nodes are introduced (a) randomly and (b) with population to the network.

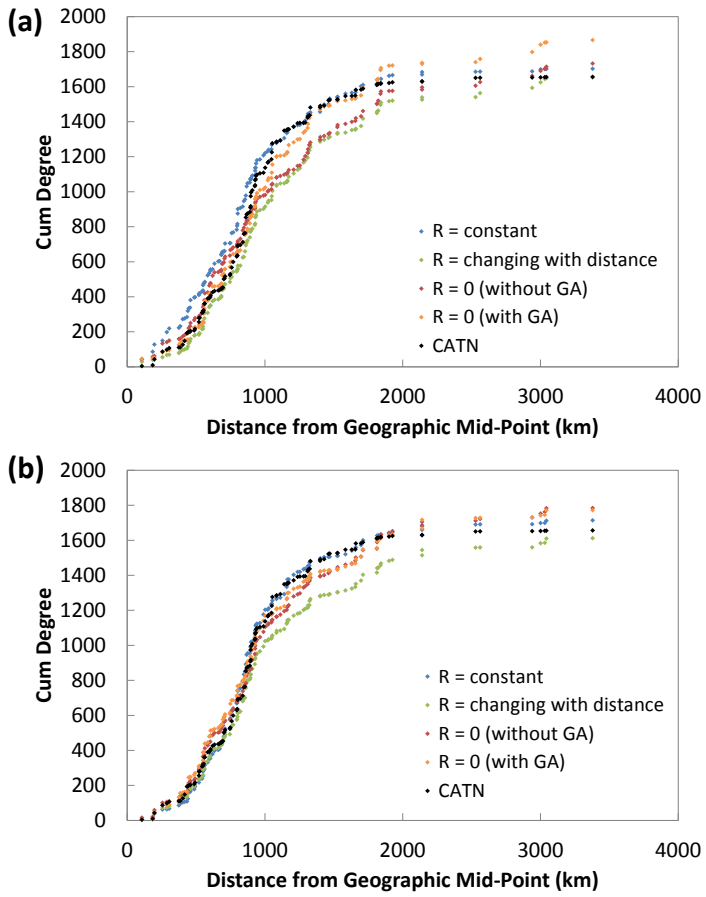


Figure 3.44: Showing the spatial degree distributions for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm for the actual node locations, where nodes are introduced (a) randomly and (b) with population to the network.

From Figure 3.43 and Figure 3.44 it can be seen that the exponential network with a constant neighbourhood size which includes the modification of GA (blue dots) produces the best fit for the CATN for both the random and population node introduction orders (when considering both the degree and spatial degree distributions). Whereas, the synthetic networks without the modification of GA do not form hub airports with sufficient connections (red dots) and a changing neighbourhood size forms a spatial distribution with too few links from 1000km from the geographic centre (green dots). From these distributions, it can be concluded that whilst the CATN and EATN have different number of airports and air routes and different topological and spatial configurations, the 'rules' which govern the formation of connections in these networks are the same.

The degree of each airport in the CATN and the 'best fit' synthetic network (where nodes are introduced randomly) have been plotted using GIS and shown in Figure 3.45. From this figure it can be seen that the synthetic network is a good proxy for the CATN,

however it does not replicate the degree of each airport exactly (similarly to the 'localisation' effect observed in the EATN as previously discussed). It can also be seen that for the CATN not all of the high degree airports occur in one small spatial area and that there is a fairly dense area of nodes along the East coast (Figure 3.45(a)).

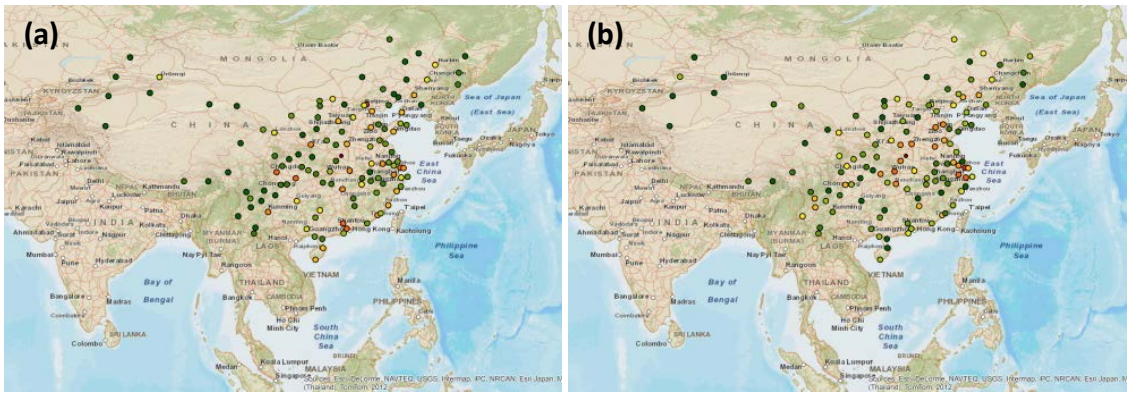


Figure 3.45: GIS generated images of the (a) actual China air traffic network and (b) a generated network (the blue line in Figure 3.43(a) and Figure 3.44(a) where the colour of the node indicates its degree (red to green, for high to low degree). The black dot in each part shows the location of the geographic centre of the actual network (note that this is not recalculated for the synthetic network).

These synthetic networks have shown that the CATN can be generated using the same 'rules' as the EATN; however, this has been achieved using the actual node positions only. For these networks to be considered fully synthetic spatial networks, their nodal positions should also be generated. It has been shown that a bi-linear configuration is a poor fit for the CATN (Figure 3.15(a)) therefore the more sophisticated 'clustering' algorithm is used.

The nodal configuration has been generated by defining the location of five seed nodes (4% of the total number of nodes in the network), with one of two different radii values; four nodes are used to represent the landmass of China and one additional node is located over the area of high population density. Similar to the EATN no nodes are allowed to form outside the boundary of the clusters (as these are used to form the 'land mass' of the network) and the whole nodal layout is placed within a circular spatial boundary. The resulting nodal configuration and spatial distribution can be seen in Figure 3.46. The spatial distribution of nodes (Figure 3.46(b)) is a good proxy for the CATN, however it is not an exact replication. This is due to the smaller number of airports in the network than compared with the EATN and therefore the placement of these nodes has a greater impact on the resulting spatial distribution.

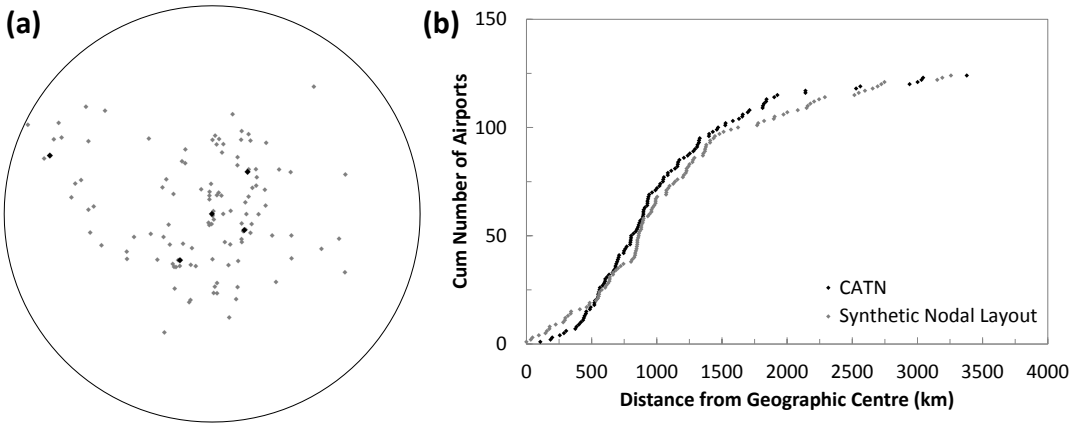


Figure 3.46: (a) Simulated clustered nodal layout for the China air traffic network (CATN), where the black dots represent the seed nodes, the grey dots the added nodes and the black line the spatial boundary of the network. (b) A comparison for the spatial distribution of nodes for the CATN (black) and the synthetic nodal layout (grey).

This nodal configuration has been used to form synthetic networks for the CATN, again assessing the ability of the four types of network to replicate the topological and spatial characteristics of the EATN. Three node introduction orders were assessed (introducing nodes with distance, proportional to distance and randomly), however, due to space restrictions only the results where nodes have been introduced randomly are shown, as these produced the 'best fit' for the CATN. The degree and spatial degree distributions for these generated networks are shown in Figure 3.47.

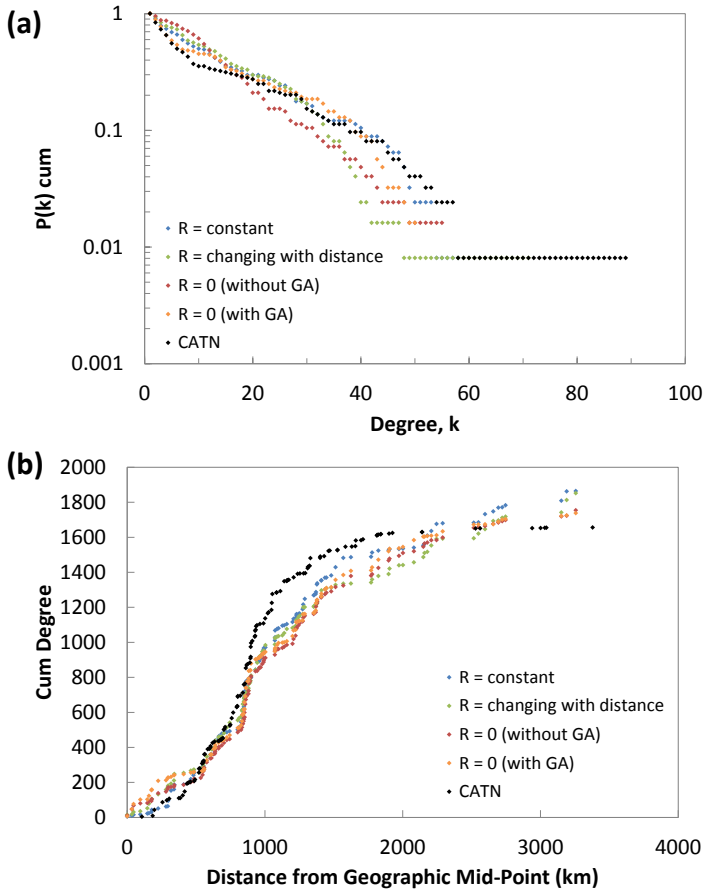


Figure 3.47: Showing degree distribution and spatial degree distributions, respectively, for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm, where nodes are introduced randomly to the network for the clustered nodal layout (Figure 3.46).

From these distributions it can be seen that the exponential network with constant neighbourhood size, including the modification of GA (blue dots), again forms the best proxy for the CATN. The network without the modification of GA again forms a hub node with too few connections (red dots). However, the fit of the synthetic networks to the actual CATN is not as good as that obtained for the EATN and its synthetic networks. This could be attributed to the smaller network size, making it more sensitive to small changes in the algorithm input values or could be due to the regulation of flights in the CATN (unlike the EATN). This is particularly evident in the spatial degree distribution for these networks generated using the (Figure 3.47(b)), as there are too few airports with a high degree in the region between 1000km and 1500km from the geographic centre. Although, this was not observed when the networks are generated using the actual CATN nodal locations (Figure 3.43(b) and Figure 3.44(b)) and could therefore be attributed to the synthetic nodal layout.

3.3.2: GENERATING SYNTHETIC NETWORKS FOR THE US AIR TRAFFIC NETWORK

The ability of the network generation algorithm to generate one further air traffic network is tested using the USATN. In a similar manner to the CATN, this is initially assessed using the actual airport locations and then using a generated nodal configuration. The same four types of synthetic network are generated, using the same four node introduction orders (introducing with distance, proportional to distance, randomly and with population); however, only the results where nodes are introduced randomly and with population are presented, due to space restrictions, as these form the 'best fit' for the USATN. The degree and spatial degree distributions for these synthetic networks are shown in Figure 3.48 and Figure 3.49.

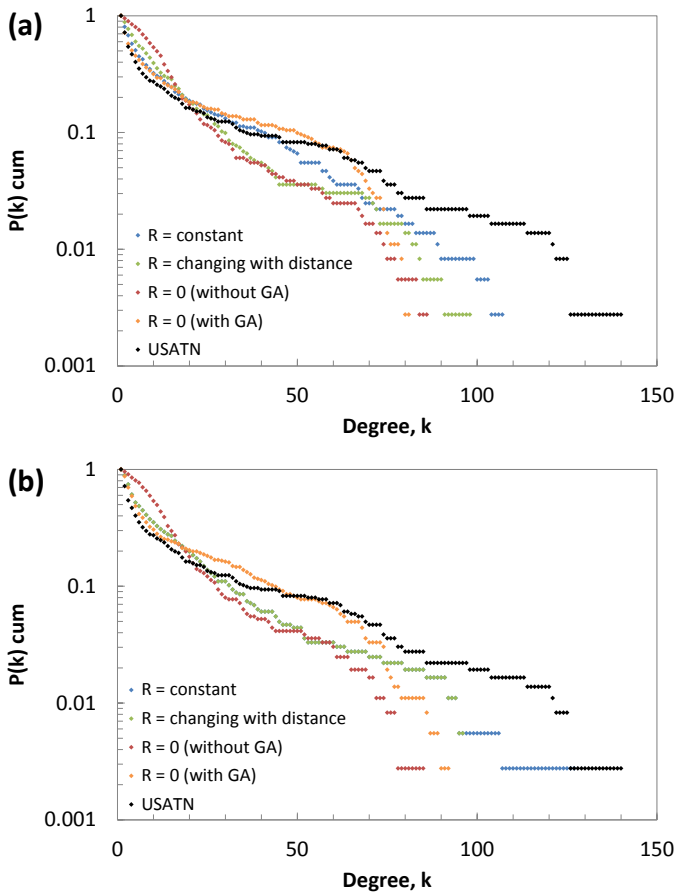


Figure 3.48: Showing the degree distribution for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm for the actual node locations, where nodes are introduced (a) randomly and (b) with population to the network.

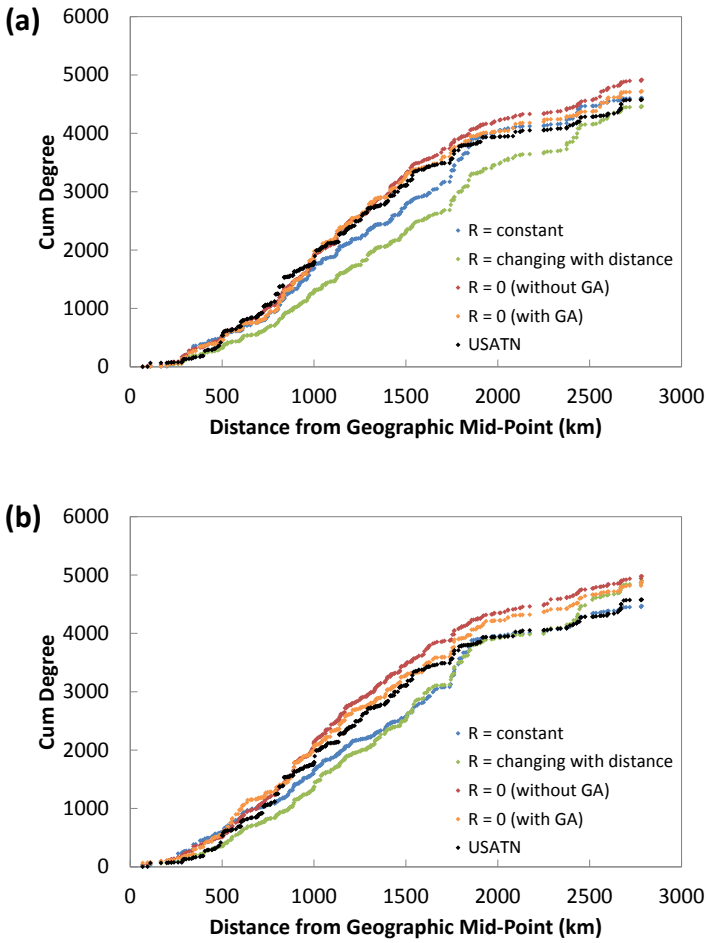


Figure 3.49: Showing the spatial degree distributions for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm for the actual node locations, where nodes are introduced (a) randomly and (b) with population to the network.

From these results, it can be seen that the 'rules' which govern the formation of air routes in the EATN and the CATN also produce the best fit degree and spatial degree distributions for the USATN. However, the fit is lacking in places. The synthetic networks where nodes are introduced randomly are lacking hub airports (Figure 3.48(a)) and introducing nodes with population results in a lack of mid-degree airports (Figure 3.49(a)). However, the exponential networks generated using the modification of GA have the highest degree node and form the best fit for the USATN (blue dots). This lack of hub airport is likely to be due to the geographic distribution of nodes within the USATN, and more specifically to the apparent spatial dispersion of airports within the US (with the exception of two denser areas of airports located on the East and West coasts). This is in contrast to both the EATN and CATN which both have a visible area of high density airports around the geographic centre of the network (Figure 3.15 and Figure 3.39(a)). Within the synthetic exponential networks, air routes

bound for a high degree node may 'divert' to a lower degree node, if the high degree node is within the neighbourhood of the subordinate node. However, due to the dispersion of airports over the US there is less likelihood that the neighbourhood of each node will contain a high degree node. Therefore, each node has a more 'equal' chance of attracting a link from a new node. Whereas, for EATN and CATN nodes located in the area of high density around the geographic centre of the network have a higher probability of attachment, due to their close spatial proximity to other nodes.

The spatial degree distributions for both nodal layouts are a good fit for the USATN (Figure 3.48(b) and Figure 3.49(b)), with the exception of the around between 1000km and 1750km from the geographic centre (considering the synthetic network which 'best fits' the degree distribution only, blue dots). Figure 3.50 plots the degree of each node in the actual USATN and the generated network where nodes are introduced randomly (blue dots in Figure 3.48(a) and Figure 3.49(a)). It can be seen from this figure that there are several hub airports present in the actual data set (red dots) which are not replicated in the synthetic network (occurring around Detroit, Chicago, Minneapolis, Denver and Dallas). The reason behind the lack of hub airports in this area could be due to the random order in which nodes were introduced to the network (i.e. if these nodes were introduced 'late' to the network they would not have had many chances to attract links). However, this is unlikely as 10 networks were generated using each of the four types of networks, all of these generated networks used a different node introduction order and all networks lacked a hub airport. The lack of hub airports is due to the rule governing the formation of a neighbourhood around each node. The optimal value for the neighbourhood size in this network (i.e. the size of neighbourhood that produced the best fit) is equal to 150km overland distance to reach an airport, which is the smallest size distance of all three generated air traffic networks (this was 250km for the EATN and 200km for the CATN). When considering the differences between the population densities for Europe (Figure 3.10(f)), China (Figure 3.51(a)) and the US (Figure 3.51(b)) it is apparent that two values of neighbourhood are required to generate the USATN with greater accuracy. From these maps it is clear that Europe and China have one main area of high population density (also where the majority of airports are located), but that there are several areas of high density in the US. Therefore, it is likely that the people in these

high dense areas are not prepared to travel as far overland to reach an airport as those living in the less dense (more rural) areas.

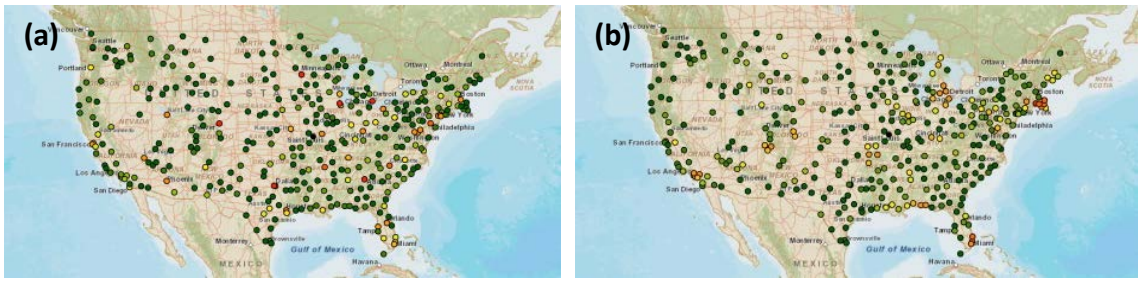


Figure 3.50: GIS generated images of the (a) actual US air traffic network and (b) a generated network (the blue line in Figure 3.53(a, b), where the colour of the node indicates its degree (red to green, for high to low degree).

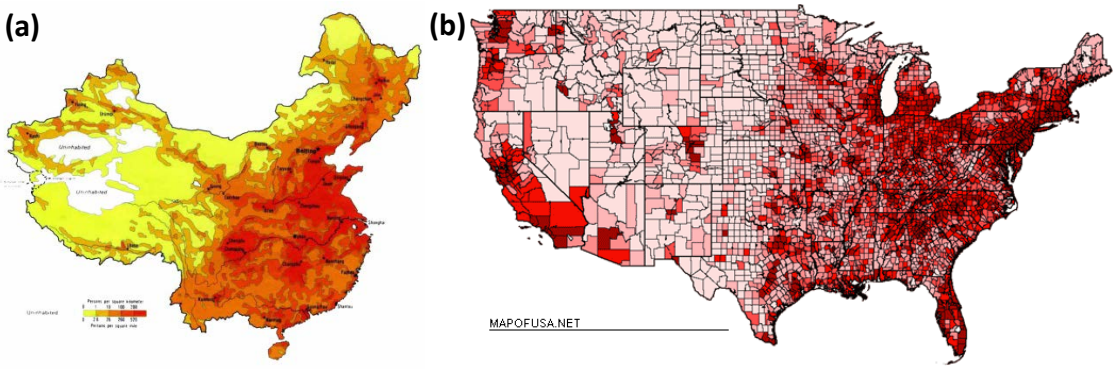


Figure 3.51: Showing population density maps for (a) China (China Travel Go 2013) and (b) the US (MapsofUSA.net 2013).

Similarly to the CATN, these synthetic networks have assessed the ability of the network generation algorithm to form proxy networks for the USATN using actual nodal locations. However, to be fully synthetic spatial networks, the nodal configuration of this network should also be generated. This is achieved using the 'clustering' algorithm developed earlier in the Chapter and previously used to generate synthetic configurations for the EATN and CATN.

However, for this nodal layout the spatial boundary is rectangular, rather than circular, as this best fits the actual nodal layout of the network. In this clustered nodal layout, the algorithm starts with 11 seed nodes (3% of the total number of nodes in the network) that have one of three radii values. In the same manner as the CATN, the majority of these seed nodes are used to form the landmass and two additional nodes are placed in the areas of high population density, as such nodes are only allowed to

form within the radius of one of the starting nodes. The generated spatial nodal distribution is a good fit for the dataset and is shown in Figure 3.52, along with the nodal layout.

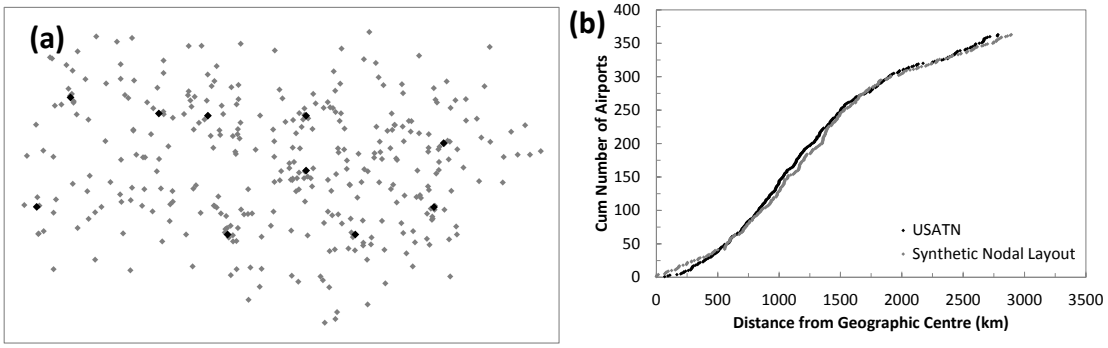


Figure 3.52: (a) Simulated clustered nodal layout for the US air traffic network (USATN), where the black dots represent the initial nodes, the grey dots the added nodes and the black line the spatial boundary of the network. (b) A comparison for the spatial distribution of nodes for the USATN (black) and the clustered nodal layout shown in (a) (grey).

This nodal layout has been used to generate synthetic networks for the USATN, again assessing the ability of the four types of network to replicate the topological and spatial characteristics of the EATN. Three node introduction orders were assessed (introducing nodes with distance, proportional to distance and randomly), however, due to space restrictions only the results where nodes have been introduced randomly are shown, as these produced the 'best fit' for the USATN. The degree and spatial degree distributions for these generated networks are shown in Figure 3.53.

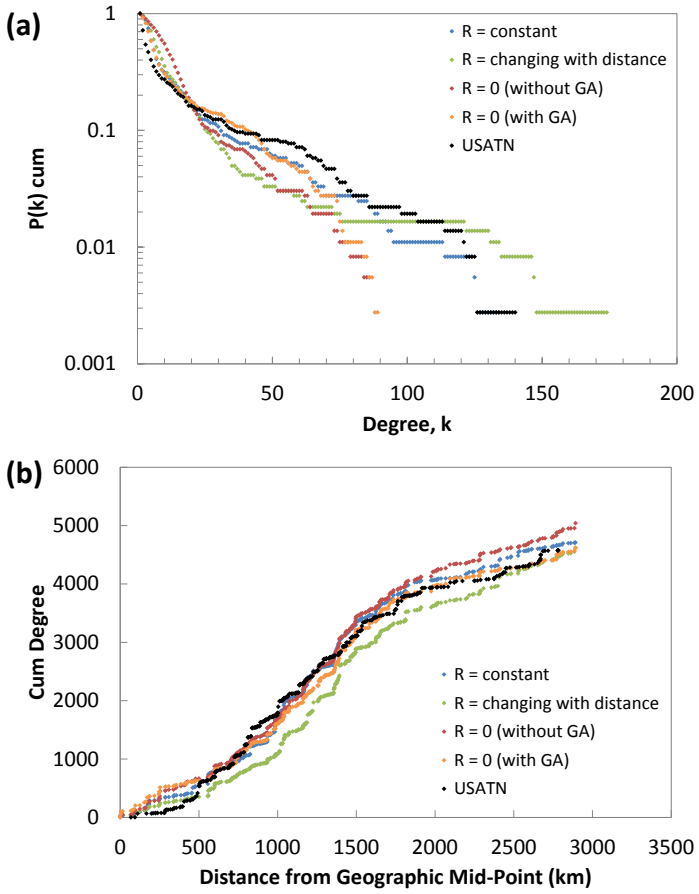


Figure 3.53: Showing the (a) degree distribution and (b) spatial degree distribution, for the exponential (blue, green) and scale-free (red, orange) networks generated using the synthetic network generation algorithm, where nodes are introduced randomly to the network the clustered nodal layout (Figure 3.52).

From the distributions, shown in Figure 3.53, it can be seen that it is the exponential network, with constant neighbourhood size and including the modification of GA, which again forms the best fit for the actual air traffic network. The exponential network where the size of the neighbourhood changes with distance forms too large a hub airport and the scale-free networks fail to generate a sufficiently large hub airport. However, the spatial degree distribution for all four types of synthetic network is a good fit for the USATN, with the exception of the exponential network with changing neighbourhood size.

From these spatial and degree distributions, and those shown earlier in the Chapter, it can therefore be concluded that for all three air traffic networks (for both the actual and synthetic nodal configurations), it is the exponential network with a constant neighbourhood size., which includes the modification of GA, that best replicates both the topological and spatial characteristics of the actual air traffic network. Therefore,

although these three air traffic networks all have a different number of airports and air routes, as well as different topological and spatial characteristics they are all governed by the same set of 'rules'.

3.3.3: HAZARD TOLERANCE OF THE CHINA AND US AIR TRAFFIC NETWORKS TO SPATIAL HAZARDS

The hazard tolerance of the CATN and the USATN, and their 'best fit' synthetic counterparts, will be assessed using only one position of the spatial hazard. The 'central attack' spatial hazard will be used (Figure 3.35) to enable the hazard tolerance for the 'worst case' location of the spatial hazard to be assessed. Due to the lack of obtainable airspace data for the CATN and USATN the proportion of airspace removed by this spatial hazard cannot be calculated, therefore the results will be presented in terms of the percentage distance that the hazard is from the geographic centre. This distance is measured from the geographic centre of the network to the airport that is furthest from this point and the results are given in percentages to enable the hazard tolerance of networks of different sizes to be compared and the results of this analysis is shown in Figure 3.54. The CATN and USATN could have been placed within an artificial spatial boundary (e.g. either a circle or the extent of landmass) and the area removed calculated using this boundary, however, any results obtained and plotted using the proportion of area removed could lead to assumptions and conclusions when compared to the EATN (for which the actual airspace data is used).

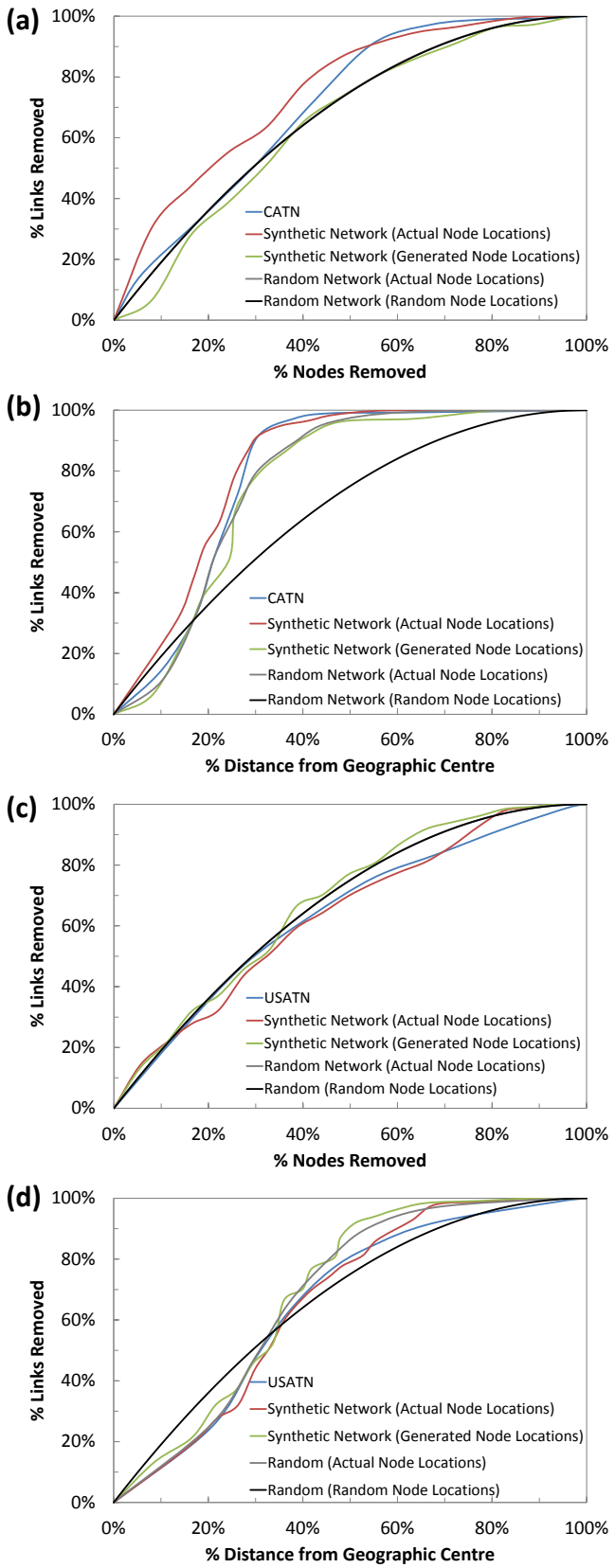


Figure 3.54: The hazard tolerance of the (a, b) China air traffic network and (c, d) US air traffic network and two of their synthetic proxies to the central attack spatial hazard (Figure 3.35). Also showing the hazard tolerance of random networks with the same node locations as the air traffic networks (grey line) and random node locations (black line). It is worth noting that the random networks with the same nodal locations as the air traffic networks show the same results as the random networks with random nodal locations in (a) and (c) and therefore cannot be distinguished in the graphs.

In Figure 3.54, only one synthetic network has been plotted for each of the different nodal layouts, this network is the same as those shown in the degree and spatial distributions in Figure 3.46 and Figure 3.52 (blue dots). Only one network has been presented in this figure, rather than an average of the 10 analysed networks, enabling the results to be compared with the degree and spatial degree distributions obtained. It was decided that this would be more appropriate, rather than presenting the average, due to the lack of fit in the degree and spatial distributions for these two air traffic networks (the fit for these distributions is not as good as those obtained for the EATN). As such, the possible reasons behind the lack of fit for the hazard tolerance of these synthetic networks, compared to their real world counterparts can be better explored and explained.

From Figure 3.54 it can be seen that the synthetic networks show approximately the same hazard tolerance as the real world networks, with a few small exceptions. The synthetic CATN generated with the actual nodal locations overestimates the vulnerability of the CATN when the results are plotted both in terms of the proportion of nodes and distance removed by the spatial hazard. The reason behind this overestimation is apparent when considering the lack of fit for the spatial degree distribution of this network (plotted in Figure 3.47). This synthetic network has a slightly higher proportion of mid to high degree nodes located close to the geographic centre of the network, therefore as this spatial hazard removes nodes outwards from this point a higher proportion of links in the synthetic network are removed for the same number of nodes removed.

To show that the scatter of results in the hazard tolerance of the synthetic networks is small, all 10 analysed networks for the USATN with synthetic nodal layouts has been shown in Figure 3.55 (it is worth noting that each of these networks has a different nodal layout). From this figure it can be seen that an average (or trend line) could be easily fitted through the results and that the associated scatter would be small. It is also worth noting the sharp changes in the percentage of links removed for a small increase in the hazard area (which is also visible in Figure). This is due to the presence of areas of high nodal density of 'clusters' of nodes in the network. The removal of one of these 'clusters' will remove a large proportion of nodes, for a small increase in hazard size, and therefore cause the sharp increase in the percentage of links removed.

The scatter of results in the EATN and CATN are not shown, but are similar to those shown for the USATN.

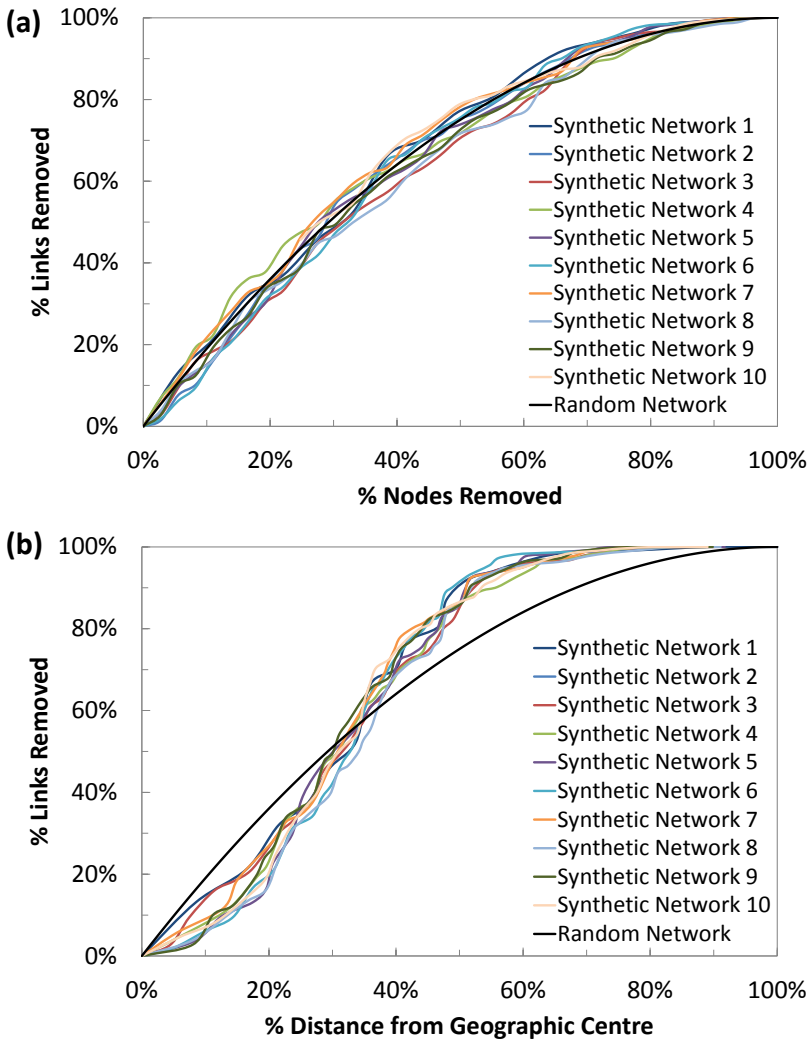


Figure 3.55: Showing the hazard tolerance of ten synthetic networks for the USATN with generated nodal locations (different for each network) subjected to central attack spatial hazard, plotting the results in terms of (a) percentage nodes removed and (b) nodes removed within a specified distance from the geographic centre of the network.

From this hazard tolerance analysis, shown in Figure 3.54, it can also be seen that both real world air traffic networks show some resilience to the spatial hazard when the results are plotted in terms of the proportion of nodes and links removed (as the results are close to those for the random benchmark network). Although, the CATN shows an increased vulnerability after 40% of the nodes have been removed by the spatial hazard, due to the removal of the high degree airport (Beijing Capital International Airport). However, plotting the results in terms of the proportion of area removed by the spatial hazard alters the perceived hazard tolerance of both networks. Both networks initially show an increased resilience to the hazard, until nodes within

18% (CATN) or 35% (USATN) of the distance from the geographic centre have been removed, after these points it can be seen that with further expansion of the spatial hazard the networks become increasingly vulnerable. This initial increased resilience in both networks can be explained by considering the lack of high degree airports close to the geographic centre of the CATN (shown by the spatial degree distribution, Figure 3.41(b)) and by the dispersion of high degree nodes throughout the USATN (which can be seen visually in Figure 3.50(a)).

To further investigate the differences between the hazard tolerances of all three air traffic networks the results have been plotted on a single graph, along with a series of random benchmark networks, which each have the same nodal locations as one of the three air traffic networks. Comparing the hazard tolerance of the air traffic networks to these random benchmarks will establish whether the vulnerability in the air traffic networks is due to the spatial configuration of nodes or the specific location of the high degree nodes. The hazard tolerances for these six networks have been plotted in Figure 3.56, along with the random benchmark network (with random nodal locations).

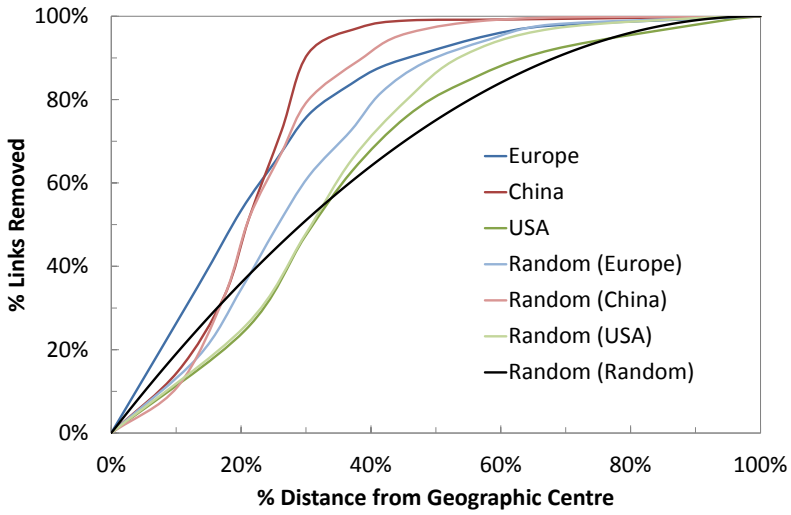


Figure 3.56: Showing the percentage of links removed and the percentage distance from the geographic centre (to the furthest node) for the central attack spatial hazard (Figure 3.35), for the European, China and US air traffic networks. The corresponding random network for each real world air traffic network has also been shown (this random network has the same nodal locations, but a different arrangement of links as the real world network), along with the random network with random nodal locations. Note that the results for the European air traffic network are the same as those shown in Figure 3.36, but with a different x-axis.

From Figure 3.56 it can be seen that the EATN is the most vulnerable of the three air traffic networks to the central attack spatial hazard, followed by the CATN, with the USATN showing the most resilience to this hazard. Comparing the results of the EATN

to the random network with the same nodal locations (blue lines) shows that the random network shows an increased resilience to small sizes of the spatial hazard (until over 20% of the distance from the geographic centre is covered by the hazard). Therefore, it can be concluded that the vulnerability shown by the EATN to small sizes of this spatial hazard is due to the location of high degree nodes within the network (around the geographic centre). This high density of nodes around the geographic centre is not apparent in the CATN and USATN, which have both been shown to display an increased resilience to small sizes of the spatial hazard. In the CATN the majority of nodes are located close to the East coast, which is a short distance from the geographic centre and causes the network to become vulnerable when these nodes are removed (when nodes within 10% of the distance from the geographic centre have been removed). In contrast, the high degree nodes in the USATN are more dispersed (Figure 3.50(a)) and it is not until the hazard reaches these high degree nodes that the network becomes vulnerable to the spatial hazard (after nodes within 30% of the distance from the geographic centre have been removed).

Both the CATN and the USATN show the same hazard tolerance as their random counterparts until nodes within 20% (CATN) or 35% (USATN) of distance is removed, after this point the CATN becomes increasingly vulnerable and the USATN increasingly resilient. The vulnerability in the CATN is due to the lack of many high degree airports close to the geographic centre; whereas the USATN shows resilience to large sizes of the central attack spatial hazard, due to the dispersion of high degree nodes throughout the network area.

Comparing the results of the random networks, using the actual nodal layouts, to the random network with random nodal locations shows that all three nodal layouts show resilience to small sizes of the spatial hazard. This is due to the lack of airports located on, and in the area immediately around, the geographic centre of the air traffic networks. However, once the areas of high density nodes in the European and China air traffic networks are removed these random networks are vulnerable, compared to the benchmark random network. The US nodal layout shows the most resilience to the spatial hazard and the random network does not become vulnerable until the area of high nodal density located on the East coast area removed. Therefore, it can be concluded that the networks show resilience to spatial hazards which affect areas of

low nodal density; however, this causes the networks to be vulnerable to hazards located over the areas of high nodal density.

This hazard location was chosen to be the 'worst case' scenario and is the case for the EATN, as previously shown in Figure 3.36; however, for the USATN the higher coastal density of airports moves the vulnerability towards the edge of the network and in the CATN the geographical centre has been 'moved' away from the area of high density due to a number of 'outlying' airports in the far West. This demonstrates that whilst the growth of links is common to all network studied, the nodal locations, which are influenced by a number of factors (including: history, geographical features and resource location) can have a significant effect on the spatial hazard tolerance.

3.3.4: APPLICATION OF NETWORK THEORY MEASURES

The hazard tolerance assessment of the CATN and the USATN has so far quantified the changes in the networks using the percentages of nodes, distance (from the geographic centre) and links removed only (assessing the proportion of affected infrastructure components for a given size of spatial hazard). In a similar manner to the EATN, the changes to the efficiency and connectivity of the network will be quantified by applying two network measures (APL and MCS). These measures will be applied to the central attack spatial hazards, for the actual air traffic networks only as it has already been established that the synthetic networks for all three air traffic networks are a good proxy for the actual networks and what is of interest is the comparison of the hazard tolerance for the three air traffic networks. The results for these measures have been plotted against the percentage of nodes removed and the percentage distance of the hazard from the geographic centre of the network (to the furthest node in the network) and can be seen in Figure 3.57.

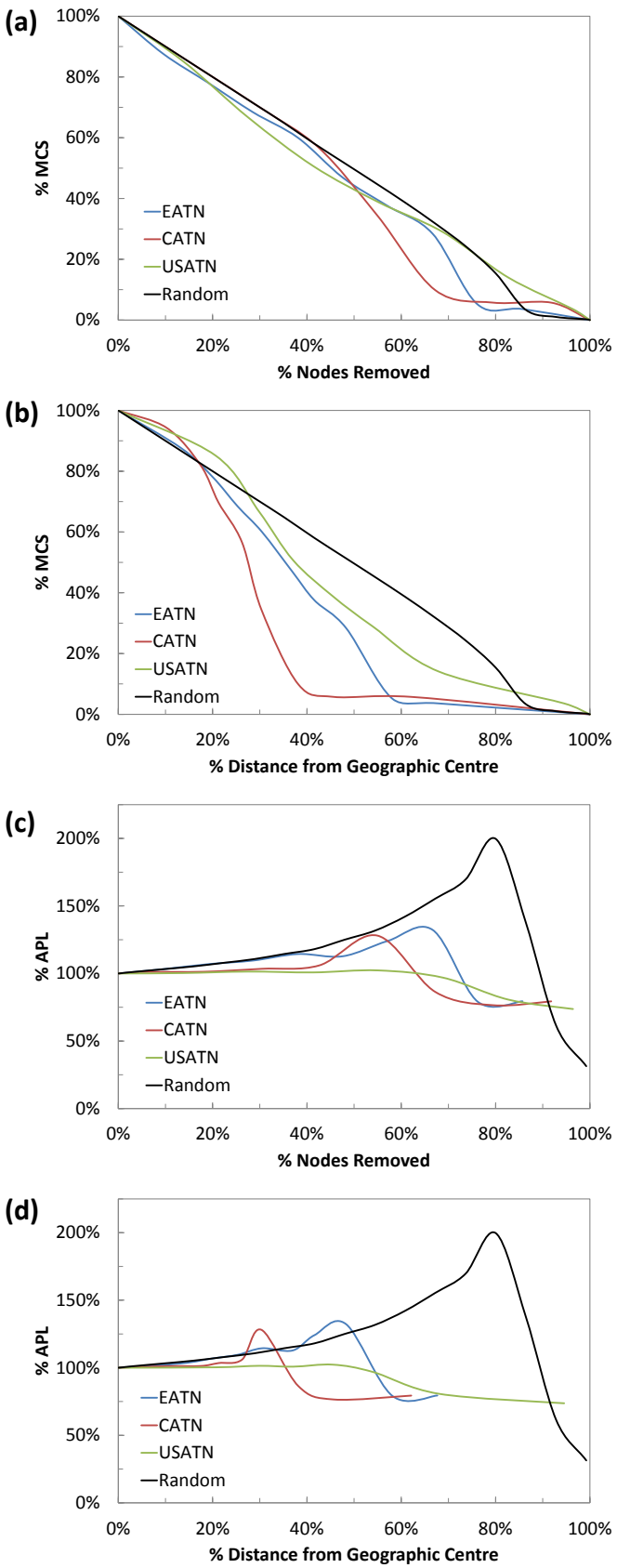


Figure 3.57: Showing (a, b) the change in MCS and (c, d) the change in APL for the European, China and US air traffic networks when subjected to the central attack spatial hazard (Figure 3.35). The percentage change in the MCS and APL has been plotted as all three networks contain a different number of nodes and links. A random network, with random nodal locations, has also been shown and is used as a benchmark for resilience.

From the results, it can be seen that the CATN becomes more weakly connected quicker than the other two air traffic networks, as it breaks into clusters and/or isolated nodes quicker than the other two networks (Figure 3.57(a, b)). This is due to the arrangement of links between the nodes in the network and as this is the most regulated network could be due to the specific arrangement of air routes in this type of air traffic network. The CATN also has an unusually large hub airport (compared to the airport with the second highest degree) unlike the EATN and USATN; therefore, the removal of this airport will have a large impact to the functioning of the remaining network, causing a decrease in both the connectivity and performance. This airport (Beijing Capital International Airport) is located at 25% of the distance from the geographic centre of the network and it can be seen from Figure 3.57(b) that this is when the MCS of the network decreases dramatically. The APL also dramatically increases when nodes within 25% of the distance from the geographic centre have been removed, therefore, it can be concluded that the removal of this high degree node not only causes the network to degrade but also causes the network to become less efficient. This result also indicates that this network is susceptible to targeted attack (e.g. terrorist attack), which will often target these high degree nodes seeking to cause maximum impact to the network.

The USATN can again be considered to be the most resilient network to the central attack spatial hazard, as it is the most robust (as it maintains the highest value of MCS as the network degrades) and maintains efficiency (with relatively constant APL values). It is interesting to note that the network initially shows resilience to the spatial hazard, having a larger MCS than the random benchmark network, until the higher density of airports around the East coast of the network are removed (when the network becomes vulnerable). However, after the removal of these airports it can be seen that the APL of the network stays approximately constant, meaning that the remaining network still functions efficiently.

Focusing on the EATN and comparing the results to those of the Eyjafjallajökull event (Figure 3.37) it can be seen that the central attack spatial hazard is more disruptive to the network, not only in terms of the increased percentage links removed (for the same percentage nodes removed, as previously discussed), but also decreases the performance and connectivity of the network. This is particularly evident when

viewing the MCS plotted against the percentage of nodes removed, where it can be seen that the central attack spatial hazard causes the MCS to dramatically decrease when around 65% of the nodes have been removed. The increased disruption can also be seen in the higher 'peak' values of APL. This therefore suggests that the nodes in the area of high nodal density around the geographic centre of the network are also vital to transferring information (or in this case passengers) around the network (i.e. this is where the 'stop over' airports are located).

From these results, for MCS and APL, it can be concluded that it is the positioning of the nodes and also the high degree nodes which can dramatically alter the hazard tolerance of a spatial network. From the CATN the effects of the removal of a high degree node to the connectivity and performance of the remaining network can be seen. Whereas, the USATN has shown that networks where the nodes are located away from the spatial hazard show an increased resilience and can be classed as tolerant to small sizes of this hazard, compared to the random benchmark network.

This chapter has assessed the hazard tolerance of three air traffic networks, namely: Europe (EATN), China (CATN) and the US (USATN). It was initially shown that the EATN was vulnerable to the Eyjafjallajökull volcanic event, contradicting previous network theory which states that this class of network should be resilient to random hazard. To determine whether this vulnerability was unique to the EATN, or was characteristic of its network class, networks with the same topological and spatial characteristics as the EATN were formed. This was achieved by developing a new network generation algorithm, based on the scale-free algorithm of Barabasi and Albert (1999). This algorithm showed that the probability of attachment must be based on degree and proximity, rather than degree alone (as for scale-free networks), to produce networks with the same topology as the EATN. It was also shown that links must also be allowed to form between pairs of existing nodes in the network as the network 'grows' in order to replicate the high degree hub nodes, present in the EATN. This network generation algorithm was combined with synthetic spatial nodal configurations, generated using an algorithm based on a cellular automata framework, to form fully synthetic proxies for the EATN, which to the best of the authors' knowledge is the first time this has been

achieved. The ability of these algorithms to generate proxies for other air traffic networks (CATN, USATN) was also assessed, finding that they form using the same 'rules' as the EATN.

The EATN synthetic networks were subjected to a simulated Eyjafjallajökull event and other spatially coherent random hazards, to which they showed the same vulnerability as the EATN. The hazard tolerances of the CATN and the USATN (and their generated synthetic networks) were also subjected to spatial hazard, finding that the CATN showed an increased vulnerability (with up to 38% more connections removed compared to a benchmark network), but the USATN showed resilience to small sizes of this hazard (with up to 12% fewer connections removed compared to a benchmark network), due to the different geographical arrangements of nodes in these networks.

To categorize all infrastructure networks into specific classes is too large a task to be practical (even if the datasets to do this existed – which is not the case) and so to cover the widest range of possible network types, the next chapter will analyse the hazard tolerance of generic networks and assess the influence of different generic combinations of spatial layout, network class and location of high degree nodes to determine which combinations are resilient and which are vulnerable. This will be used to inform strategies to increase the resilience of the EATN to spatial hazards.

CHAPTER 4: ASSESSMENT OF THE VULNERABILITY OF GENERIC SPATIAL NETWORKS

In the previous chapter it was established that traditional topological network theory models can give a false indication of the hazard tolerance of a spatially distributed network, when subjected to spatial hazards. This was demonstrated by subjecting the air traffic networks for Europe, China and the US to a range of spatial hazards (of different sizes and locations) and assessing their hazard tolerance in terms of the proportion of disrupted air routes, as well as changes to their efficiency and connectivity.

This chapter assesses the hazard tolerance of a range of spatial networks with different topological and spatial characteristics, to determine which combinations of these characteristics are resilient / vulnerable to spatial hazard. To categorise all infrastructure networks into specific classes is deemed too large a task to be practical (even if the datasets to do this existed – which is not the case) and so to cover the widest range of possible network types, synthetic networks with different generic characteristics are analysed to simulate the differing characteristics of real world systems. For example, in an air traffic network it is desirable to locate an airport close to the boundary of an area of high population density; conversely, in a power grid it is desirable to locate power stations close to the coast and away from highly populated areas. Both of these systems have been shown to have similar topological characteristics (belonging to the same network class), but will have different spatial characteristics, due to their different reasons for placing individual components (nodes). Assessing the hazard tolerance of these synthetic networks will also enable which combinations of topological and spatial characteristics produce resilient and vulnerable networks to different sizes and locations of spatial hazard. This information will be used to inform strategies to increase the resilience to the European air traffic network to spatial hazard.

4.1: SPATIAL NODAL LAYOUTS

In this thesis, it has been discussed that the majority of previous research has analysed networks where space is not an important, and governing, factor, and therefore the use of topology models has been satisfactory. However, it was shown in the previous chapter that for infrastructure networks, where space is an important factor, this analysis approach can be deficient and can lead to inaccurate assumptions regarding the hazard tolerance of a network. Real world infrastructure networks tend to form either a uniform with distance (Figure 4.1(a)) or clustered (Figure 4.1(c)) nodal distribution (as shown by analysing the three air traffic networks). Therefore, the rule set used to generate clustered nodal layouts developed in the previous chapter will again be used and a rule set to generate networks with a uniform with distance nodal layout will be created. A uniform with area nodal distribution will also be considered (Figure 4.1(b)) and will form a benchmark for comparison (see Chapter 3.1). The spatial distribution of the nodes, for each of the three layouts, has been plotted in Figure 4.1. For nodal layouts with a uniform with distance pattern, this spatial distribution is a linear relationship and for a uniform with area nodal layout the distribution follows a curved pattern. It is interesting to note the distribution for the clustered layouts, does not form the same 'smooth' line as the other two nodal layouts. This is due to the nodes being placed in clusters around the network and the spatial distribution appearing to 'jump' when each cluster is reached.

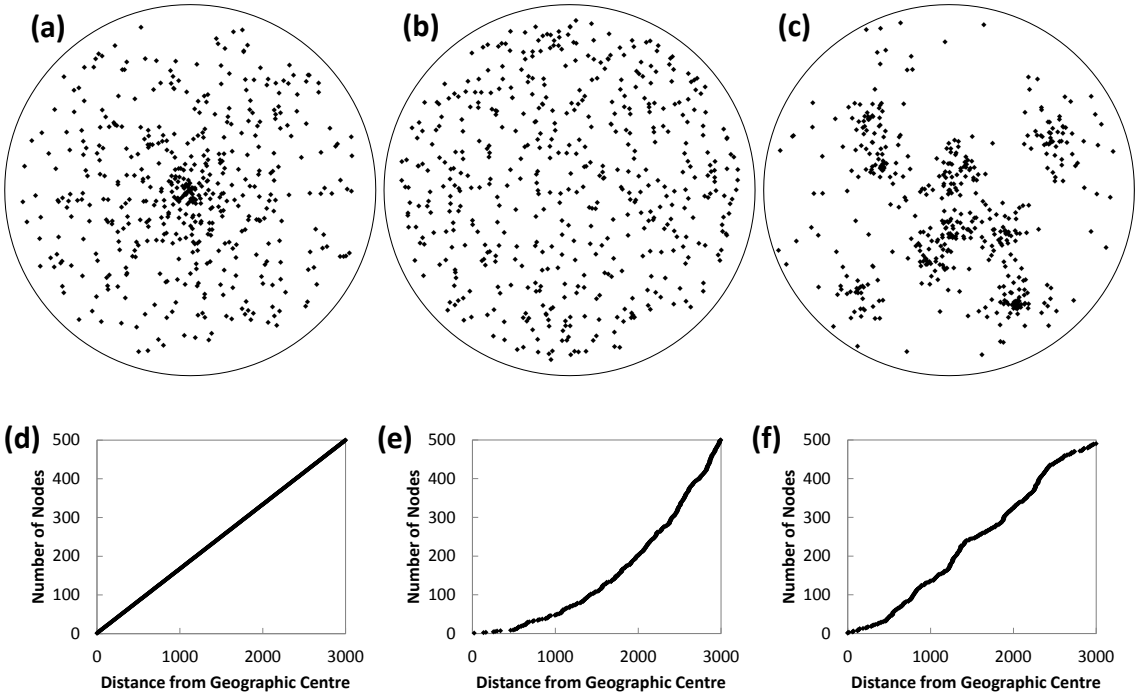


Figure 4.1: Showing three different spatial nodal layouts: (a) uniform with distance, (b) uniform with area, (c) clustered. In the three layouts, the black dots depict the nodes and the outer grey circle defines the spatial boundary of the network. Also showing the associated spatial distributions for the three nodal layouts; (d) uniform with distance, (e) uniform with area and (f) clustered.

To generate each nodal layout a different 'rule set' has been developed, governing the location of nodes within the defined spatial boundary of the network. The uniform with area and uniform with distance nodal layouts only requires the input of the extent of the spatial boundary and the number of nodes in the network; however, the clustered nodal layout requires more detailed inputs (as previously discussed in Chapter 3.2). In this chapter, all of the clustered nodal layouts have been generated using 10 seed nodes (with a random location) which have one of four starting radii values (either 10, 50, 80 or 100) to generate clusters with different densities (which can occur in infrastructure networks as shown by the three air traffic networks in the previous Chapter) and a proportion of nodes (20%) are allowed to form outside the influence of the individual clusters. Figure 4.2 shows three of the ten generated clustered nodal layouts.

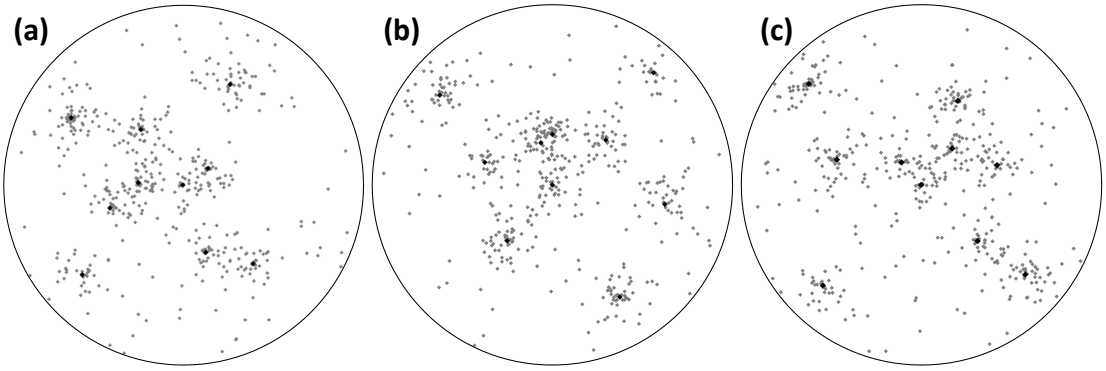


Figure 4.2: Three, of ten, clustered nodal layouts generated using the clustering algorithm (Chapter 3.2), for use in tests of hazard tolerance.

4.2: NETWORK GENERATION ALGORITHMS FOR SPATIAL NETWORKS

In order to generate generic networks belonging to the three main network classes (exponential, scale-free and random), the traditional network generation algorithms need to be modified from topological algorithms to spatial algorithms (i.e. taking into account the spatial component of the network).

The previous chapter developed a generation algorithm to generate spatial exponential networks (developed in Chapter 3.2.3). This algorithm is again used in this chapter, using a radius value of 0.25, m_0 as a constant value equal to the number of starting nodes (12 for this chapter) and allowing the GA modification. The scale-free networks used in this thesis are also generated using the algorithm developed in the previous chapter, by setting the radius value to 0 and not including the GA modification.

In the previous chapter, it was explained (and demonstrated) that the order in which nodes are introduced in the exponential and scale-free algorithms affects the location of the high degree nodes in the network and therefore the resulting spatial degree distribution (see Figure 3.14). To assess the impact that the spatial degree distribution has to the spatial hazard tolerance of these networks the three node introduction orders used in the previous chapter are again used (i.e. introducing nodes with distance from the geographic centre, proportional with distance and randomly). Although, it was shown that introducing nodes randomly to the algorithm produces the 'best fit' degree and spatial degree distribution for all three air traffic networks, all

three node introduction orders are used to demonstrate the effect that the spatial configuration of the network has to its spatial hazard tolerance (and to produce a 'complete picture' of results).

The random networks are all generated using the random graph model (detailed in Chapter 2.5.2.1) and as such do not need to be altered to create spatial networks; as the network does not 'grow' unlike the scale-free and exponential networks node introduction order does not need to be considered. This algorithm only needs to be modified, to account for the spatial component, if an optimisation problem is being considered (e.g. when the link lengths may want to be minimised).

Figure 4.3: Showing all combinations of network class (inner circle), nodal layout (centre circle) and node introduction order (outer circle) used in this chapter. In the previous chapter it was established that the exponential networks, where the nodes were introduced randomly, with a clustered nodal layout was superior at replicating the topological and spatial characteristics of the European, China and US air traffic networks.

Figure 4.3 shows all of the networks considered in this chapter, where the inner circle shows the network class, the middle circle the node introduction order and the outer circle the nodal layout. For each of the nodal layouts 10 networks have been analysed, adding to 30 networks for each node introduction order, resulting in the analysis of 90 networks for the scale-free and exponential network classes and 30 networks for the random network class (total number of networks analysed is 210). The size of the

networks are reflective of the EATN, enabling a direct comparison of the results to be made; as such, the networks consist of 500 nodes, approximately 3000 links and have a distance from the geographic centre to the spatial boundary of 3000 km.

The initial results for the hazard tolerance analysis will be presented in terms of the proportion of links removed and the proportion of nodes and area removed. It has been previously discussed that this method of displaying results is often used in studies considering the hazard tolerance of complex networks. This method can also be used to inform infrastructure owners of how many connections in their system (e.g. underground pipes, air routes) will be disrupted/damaged as a result of a particular hazard, allowing them to assess the estimated cost, repair time, etc. of the system. However, the additional time taken to transfer service around the system due to disrupted/damaged connections can be also important. This is considered later in the chapter by applying more sophisticated network graph theory measures to quantify changes in APL and MCS.

4.3: EFFECT OF NODE INTRODUCTION ORDER TO HAZARD TOLERANCE

To assess the effect that node introduction order has to the hazard tolerance of spatial scale-free and exponential networks, the uniform with area spatial nodal layout is used and networks (belonging to these two network classes) have been generated using the three node introduction orders considered. The uniform with area nodal layout has been used as it can be considered to be a benchmark case (as it is a random nodal layout) and the placement of individual nodes in the network will not affect the hazard tolerance (e.g. for each hazard the number of nodes removed will be approximately equal, however different numbers of links may be removed).

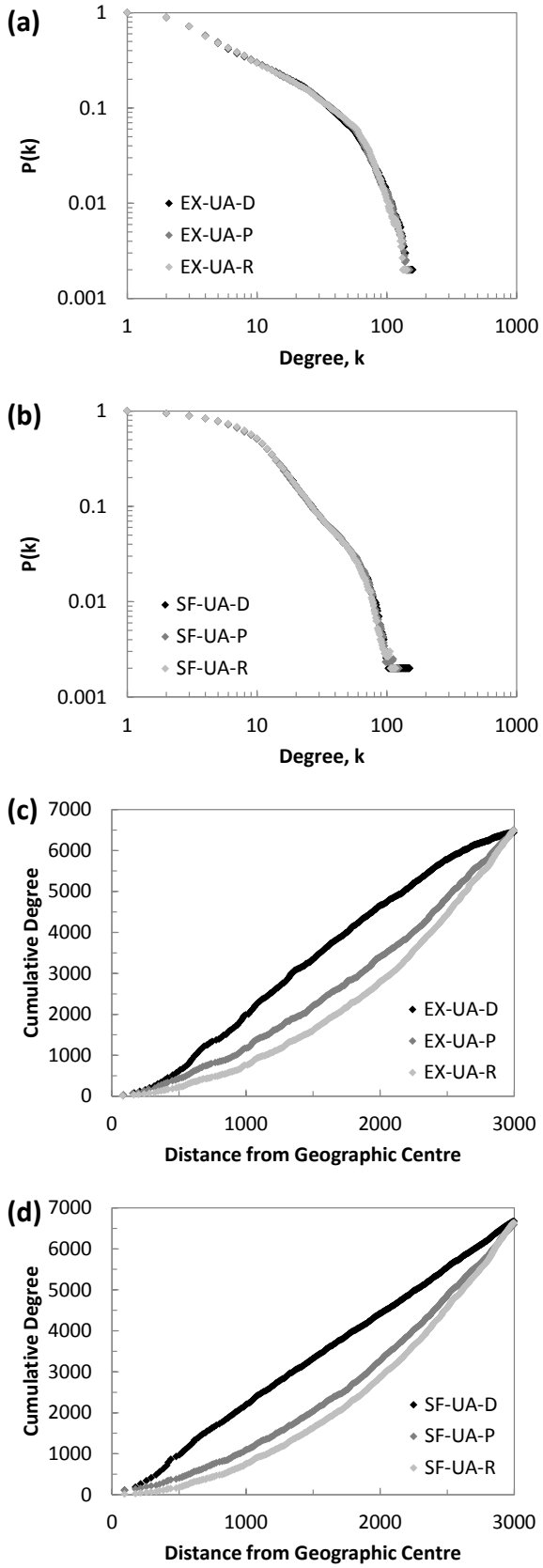


Figure 4.4: Showing the average degree distribution for (a) exponential networks and (b) scale-free networks, with a uniform with area nodal layout and three different node introduction orders; (c) the spatial degree distribution for the same exponential networks and (d) for scale-free networks[1].

The degree distribution for the exponential and scale-free networks, using a uniform with area nodal layout and three node introduction orders, can be seen in Figure 4.4. In this figure, it can be seen that the order in which nodes are introduced has no effect on the degree distribution of the network, but does affect the spatial degree distribution. This can be attributed to the length of 'time' that nodes have been present in the network, the nodes that were introduced first have a higher chance of 'attracting' links from new nodes (previously discussed in Figure 3.14). The spatial distribution of the high degree nodes in the network can be seen in Figure 4.5.

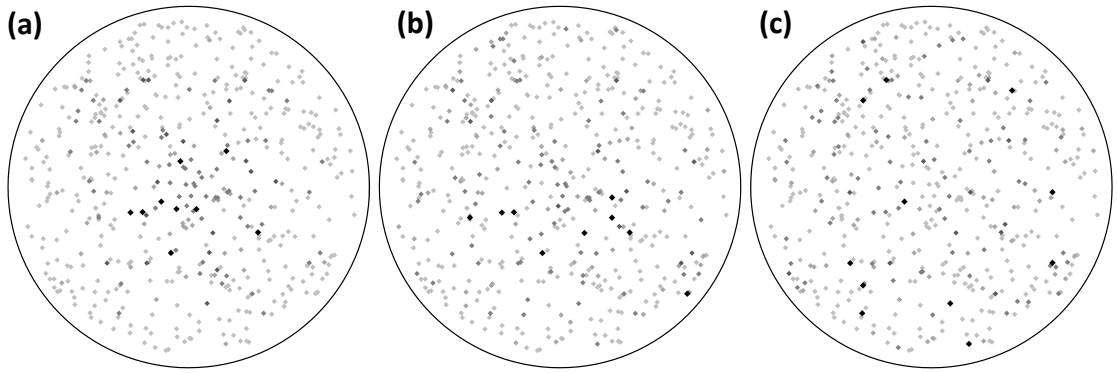


Figure 4.5: Three exponential networks with a uniform with area nodal layout, where the nodes are introduced (a) with distance, (b) proportional to distance and (c) randomly. The spatial boundary is shown as a black circle and the nodes are shown as grey-scale dots. The colour of the node indicates its degree, with black nodes having a high degree and light grey nodes a low degree.

These networks have been subjected to two different spatial hazards, which both have a fixed centre from which the hazard 'grows' outwards. The centre of the first hazard is located on the geographic centre of the network and was applied to the air traffic networks in the previous chapter (Figure 3.35) ('central attack') and the second is located on the spatial boundary of the network (Figure 4.6) ('perimeter attack'). As in previous applications of these hazards, nodes are considered to have 'failed' if they are located within the spatial hazard and the links attached to these nodes are removed from the network. Only nodes that are located within the hazard are considered to have failed and not nodes that have become isolated (due to the removal of links).

[1] To keep the key used in the figures in this Chapter to a manageable length abbreviations have been used. The key for each set of results shown refers to a different type of network and is formed of three parts for exponential and scale-free networks and two parts for random networks, separated by a hyphen. The first part of the key refers to the network class: EX refers to an exponential network, SF to a scale-free network and RND to a random network. The second part to the nodal layout of the network: UA refers to a uniform with area nodal layout, UD to a uniform with distance layout and CL to a clustered layout. The last part refers to the order in which nodes were introduced to the network: D refers to a nodal layout where nodes were introduced with distance from the geographic centre, P where nodes were introduced proportionally to distance and R introduced randomly. For example, the key EX-UA-D refers to an exponential network with a uniform with area nodal distribution where the nodes have been introduced in order of distance from the geographical centre.

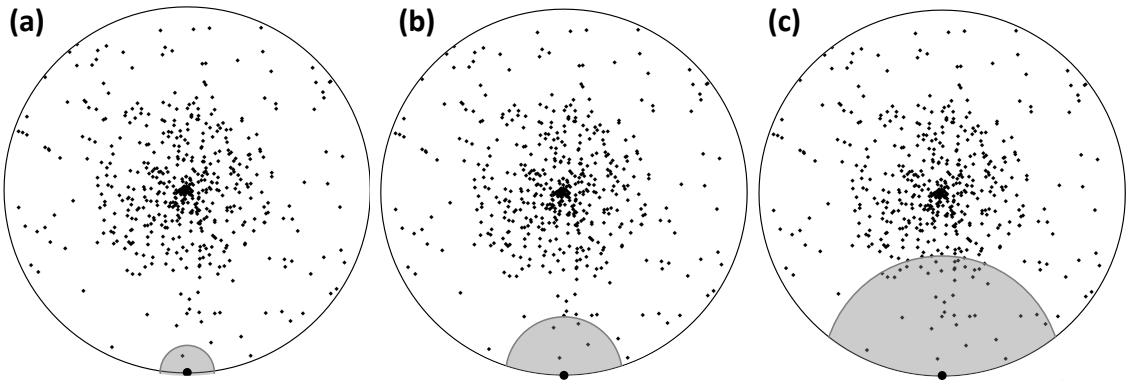


Figure 4.6: Showing three sizes of the simulated perimeter attack spatial hazard, in which the centre of the hazard is fixed on the spatial perimeter of the network and grows outwards until the whole network area is covered (i.e. from (a) to (b) to (c)).

The results for the 'central attack' spatial hazard have been plotted in Figure 4.7; for both the percentages of nodes and links removed and the percentages of area and links removed. From this figure, it can be seen that node introduction order has a significant effect on the hazard tolerance of a network. For both the exponential and scale-free networks, introducing the nodes randomly show a surprising level of resilience to this spatial hazard, having the same hazard tolerance as the random network. This can be attributed to the dispersion of the high degree nodes throughout the spatial layout of the network (Figure 4.5(c)). Therefore, as the hazard 'grows' outwards from the centre, high degree nodes are removed but a large number of small degree nodes are also removed. In contrast, networks where the nodes were introduced with distance (from the geographic centre) show an increased vulnerability to this hazard (as they have a higher percentage of removed links for a given percentage of removed nodes and area than the other two node introduction orders, Figure 4.7). This increased vulnerability is due to the high concentration of high degree nodes in the centre of the network, which is also the area of the network which is first removed by the 'central attack' spatial hazard. To quantify this difference, for the scale-free networks removing 20% of nodes results in the removal of 70% of links when introducing nodes with distance and 35% of links when removing nodes introduced randomly (35% points difference). Networks where the nodes were introduced proportional with distance, have a hazard tolerance level between the other two introduction orders (removing 45% of links in this example). This can again be attributed to the spatial dispersion of high degree nodes throughout the network,

but an increased concentration of high degree nodes close to the geographic centre unlike the randomly introduced nodes (Figure 4.5(b)).

Due to the uniform with area nodal layout, the percentage of nodes removed will be roughly equal to the percentage of area removed; therefore, there is not a significant difference in the level of hazard tolerance when plotting the percentage of links removed with the percentage of nodes compared to the percentage of area (Figure 4.7).

Comparing these results to those for the EATN, subjected to the same hazard (Figure 3.36), shows that the networks where nodes were introduced with distance show a similar hazard tolerance. This is due to the high concentration of nodes in around the geographic centre having the same effect to the remaining network, when removed by the hazard, as locating the majority of nodes in this area. Therefore, it can be seen that the hazard tolerance of a network is governed by both the spatial configuration of nodes and the spatial location of the high degree nodes (or highly connected components).

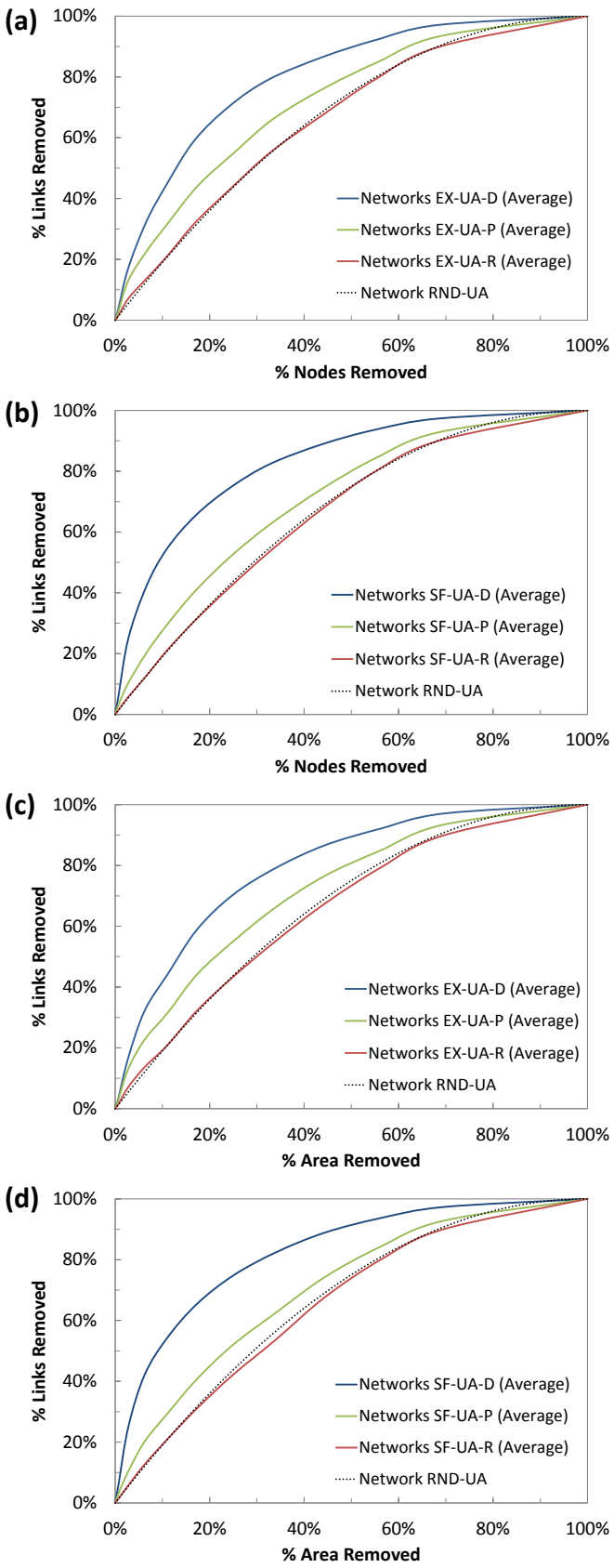


Figure 4.7: Showing the results of subjecting (a, c) the exponential networks and (b, d) the scale-free networks to the 'central attack' spatial hazard. (a, b) plot the percentage of nodes and links removed, and (c, d) plot the percentage of area and links removed. Each line of results represents an average of 10 networks. It is worth noting that there is only a small scatter in the results for each of the 10 networks.

Figure 4.8 shows the results of the same networks subjected to the 'perimeter attack' spatial hazard. From these results it can be seen that networks where the nodes were introduced proportional to distance and randomly show approximately the same resilience as the benchmark random network.

Whereas, the networks where the nodes were introduced with distance are resilient until around 35% of the network area has been removed and then become vulnerable with further expansion of the spatial hazard. This can be attributed to the location of the high degree nodes in the centre of the network. The hazard starts on the perimeter of the network, where the low degree nodes are located and therefore removes a small percentage of links compared to the percentage of nodes removed. The network becomes vulnerable after 35% of the area has been removed, as this is when the spatial centre of the network is reached, causing a dramatic increase in the percentage of removed links for only a small increase in the percentage of nodes removed. Quantifying this difference, for the scale-free networks when 20% of the nodes have been removed, results in the removal of 28% of links when introducing node with distance and 36% of links when removing nodes introduced randomly (8% points difference). However, the hazard tolerance of these two node introduction orders reverses when over 35% of the network area is removed. When 50% of the nodes have been removed, 85% of links have been removed for the nodes introduced with distance and 73% of links have been removed for nodes introduced randomly (12% points difference).

From these results it can again be seen that the EATN displays a similar hazard tolerance to the synthetic networks where the nodes are introduced with distance. Comparing the results for the Eyjafjallajökull volcanic event (Figure 3.1(d)) to those for the perimeter attack (Figure 4.8) shows that both networks display an initial resilience to small sizes of spatial hazard and then become increasingly vulnerable as the hazard grows. This again shows that locating the majority of nodes, or high degree nodes, around the geographic centre of the network has the same effect to the hazard tolerance to some sizes and location of spatial hazard.

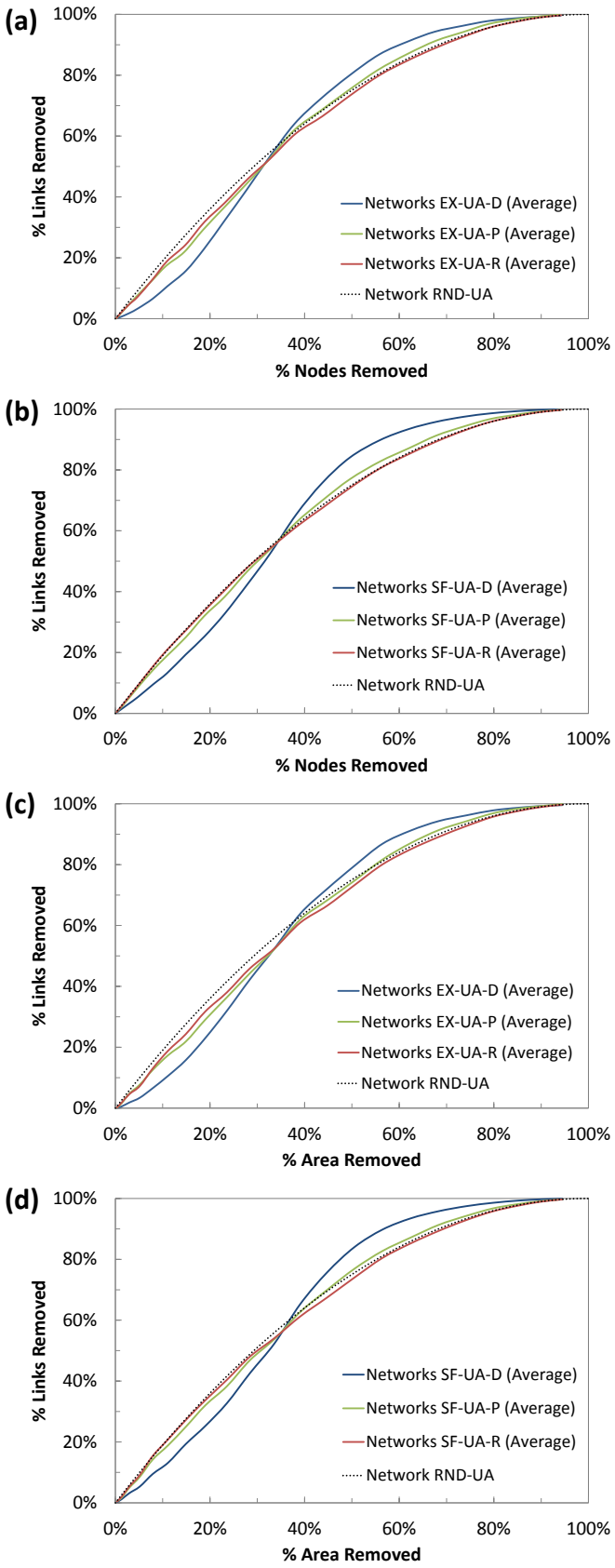


Figure 4.8: Showing the results of subjecting (a, c) the exponential networks and (b, d) the scale-free networks to the 'perimeter attack' spatial hazard. (a, b) plot the percentage of nodes and links removed, and (c, d) plot the percentage of area and links removed. Each line of results represents an average of 10 networks. It is worth noting that there is a small scatter in the results for each of the 10 networks.

It can, therefore, be concluded that the order in which nodes are introduced to 'growing' scale-free and exponential networks can have a significant effect on their spatial hazard tolerance, as it dictates the location of the high degree nodes in the network. Introducing nodes with distance causes the high degree nodes to be located close to the geographic centre of the network, rendering the network vulnerable to 'central attack' strategies; however, this also means that the network shows increased resilience to 'perimeter attack' strategies, providing that the size of the hazard is small. Introducing the nodes randomly to the network creates the most resilient network to all attack strategies (i.e. it is the best compromise), with these networks showing the same hazard tolerance as random networks.

The analysis of the three air traffic networks in the previous Chapter showed that there was a correlation between population density and the spatial configuration of airports (with a highly populated area likely to have more airports than a rural area). For example, the area around central Europe is densely populated (Figure 3.10(f)) and this is where the majority of airports are located, similarly the majority of components are located close to the East coast of China, where the main area of high population is centred (Figure 3.51(a)). These areas of high population density are also where the majority of hub airports are located, as these airports will have been opened early in the formation of the network. From the study of these synthetic networks the impact that the location of these highly connected nodes to the spatial hazard tolerance of the network can be seen. For example, the EATN shows an initial tolerance to small sizes of a 'perimeter attack' as shown by the Eyjafjallajökull event (Figure 3.1(d)) and vulnerability to all sizes of a 'central attack' (Figure 3.36), due to the location of these highly connected components around the geographic centre, which is replicated in the synthetic networks where the nodes are introduced with distance. Whereas, the CATN showed an initial resilience to the 'central attack' spatial hazard (Figure 3.56) as the geographic centre in this network is 'pulled' away from the highly populated area due to the presence of a few airports in the extreme West of the country, as previously discussed. From the results of the synthetic networks, it can be reasoned that this network will be initially resilient to small hazards located over the West coast, but will then become increasingly vulnerable as the hazard grows over the network. In contrast, the USATN should show less variability to locations of the spatial hazard, due

to the more uniform population density (particularly over the Eastern area, Figure 3.51(b)). This uniform population density causes both airports and highly connected airports to be more spatially dispersed over the network area, in contrast to Europe and China which both contain an area of high population density. Therefore, this network should display a hazard tolerance similar to the synthetic networks where the nodes are introduced with proportion to distance, with an increased vulnerability to hazards located over areas of particularly high population density (similar to the central attack spatial hazard, Figure 4.7(a, c)) and an neutral resilience to hazards located away from these areas (similar to the perimeter attack spatial hazard, Figure 4.8(a, c)).

This sub-chapter has determined that node introduction order affects the hazard tolerance of a network; however, it is also clear that the location of the spatial hazard (particularly in relation to the distance from the geographic centre) also affects the hazard tolerance. The impact of this variable to the hazard tolerance of a network will be investigated in the next sub-chapter.

4.4: EFFECT OF SPATIAL HAZARD DISTANCE TO HAZARD TOLERANCE

From the previous sub-chapter it was concluded that node introduction order has an effect to the hazard tolerance of spatial networks, as it determines the location (and concentration) of the high degree nodes. However, it was also shown that the location of the spatial hazard has an effect to the hazard tolerance. This sub-chapter will quantify the effect that the position of the centre of the hazard, in relation to the geographic centre of the network, has on the hazard tolerance of a network. In this sub-chapter both exponential and scale-free networks, all node introduction orders and the uniform with area nodal layout will be considered.

To assess the hazard tolerance of the networks, five additional positions of the hazard centre are used (from which the hazard 'grows' until the whole network area is enveloped). The additional locations of the spatial hazard have been shown in Figure 4.9 along with a graph plotting the percentage distance of the hazard from the geographic centre of the network (the locations of the 'central attack' and 'perimeter

attack' are also included in this graph with percentage distances of 0% and 100% respectively).

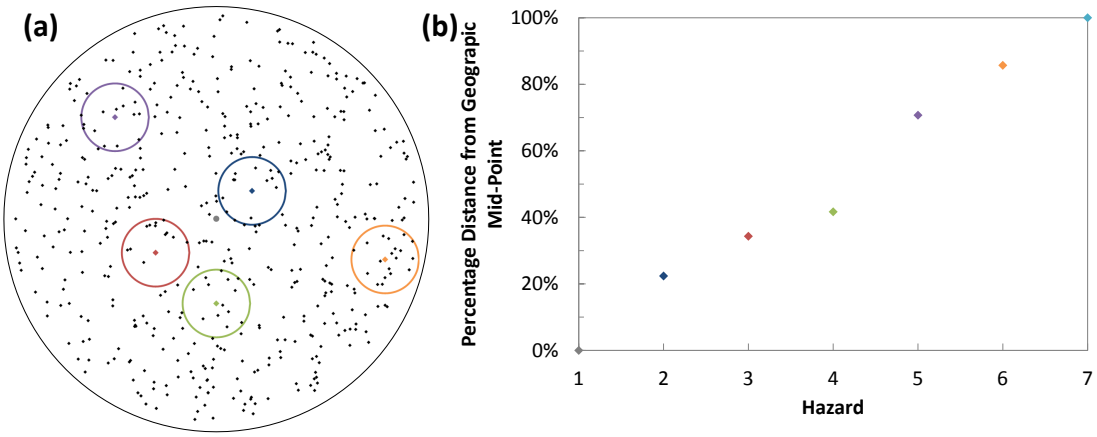
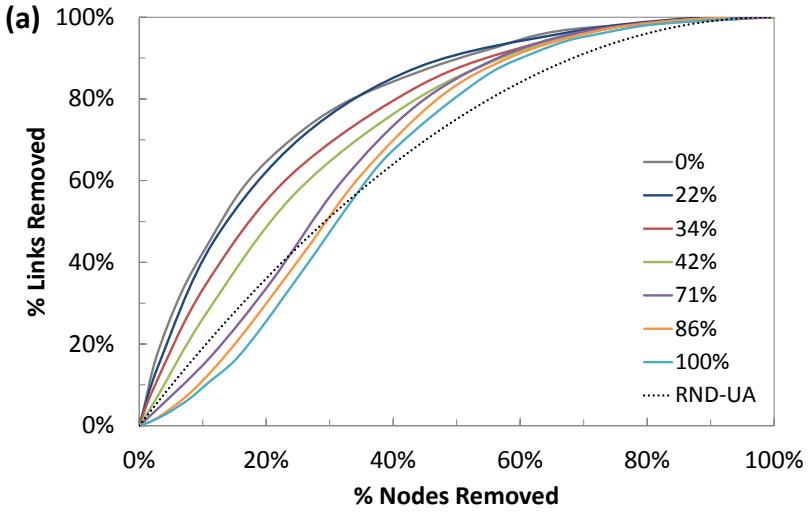
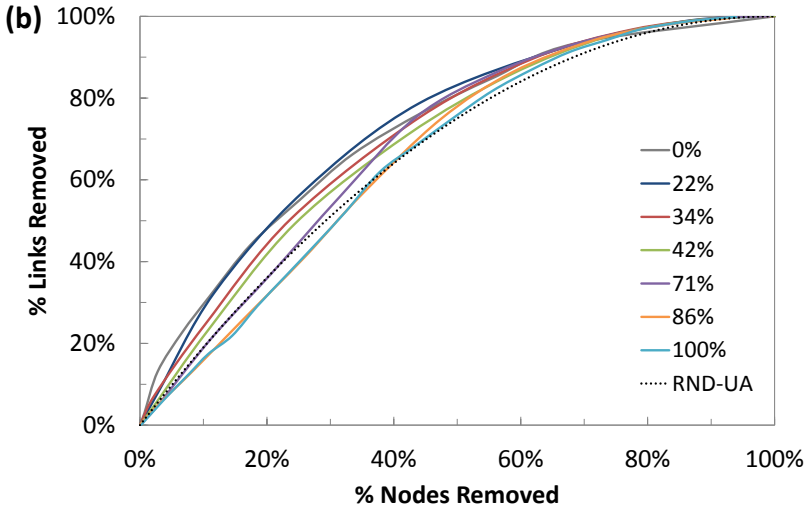
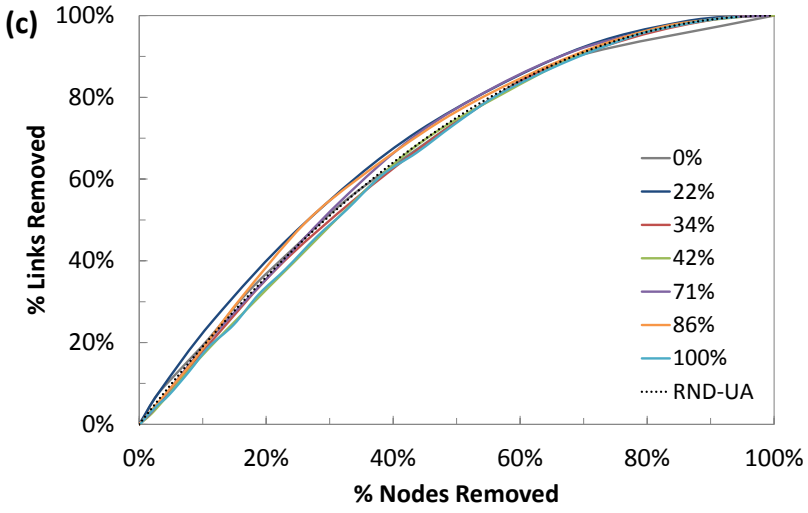


Figure 4.9: Showing (a) the locations of the five additional spatial hazards (where the black dots are the nodes, the black line the spatial boundary and the grey dot the geographic centre) and (b) plotting the percentage distance of each hazard from the geographic centre of the network (the colour of the dot on the graph is the same as that shown on the network in (a) for the five additional spatial hazards).

The results for this analysis have been shown in Figure 4.10 and Figure 4.11, where it can be seen that the hazard tolerance of both the exponential and scale-free networks are affected by the location of the spatial hazard; with the networks where the nodes are introduced with distance showing the greatest sensitivity to the spatial hazard locations.


(a)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
RND-UA


(b)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
RND-UA


(c)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
RND-UA

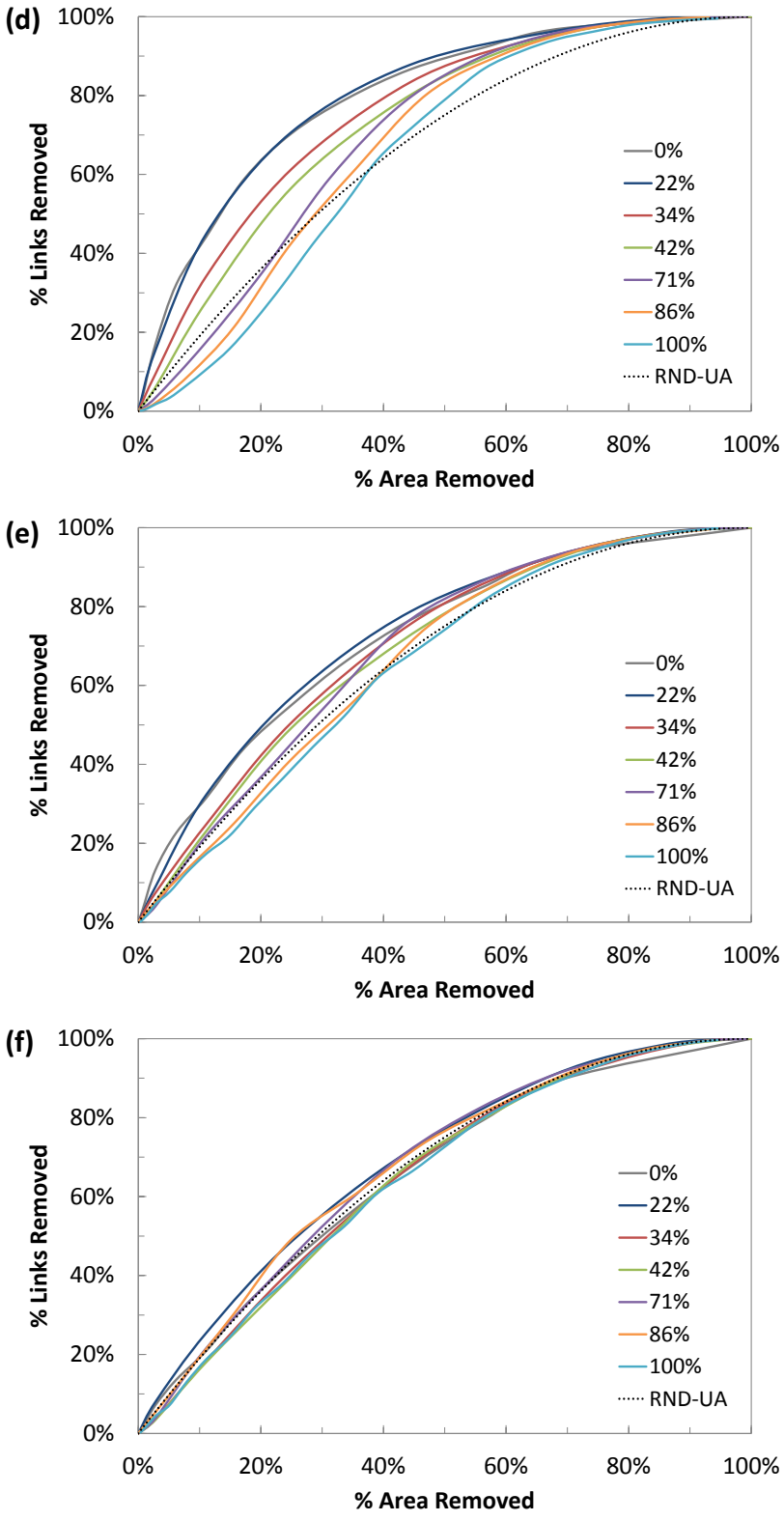
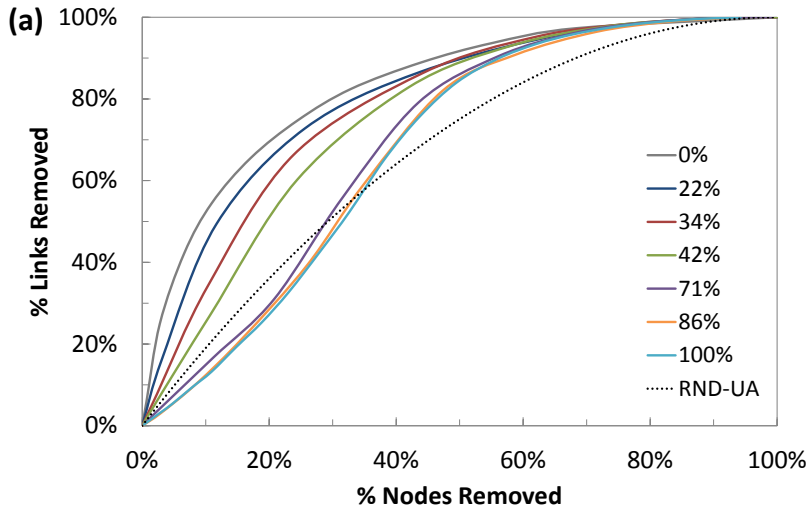
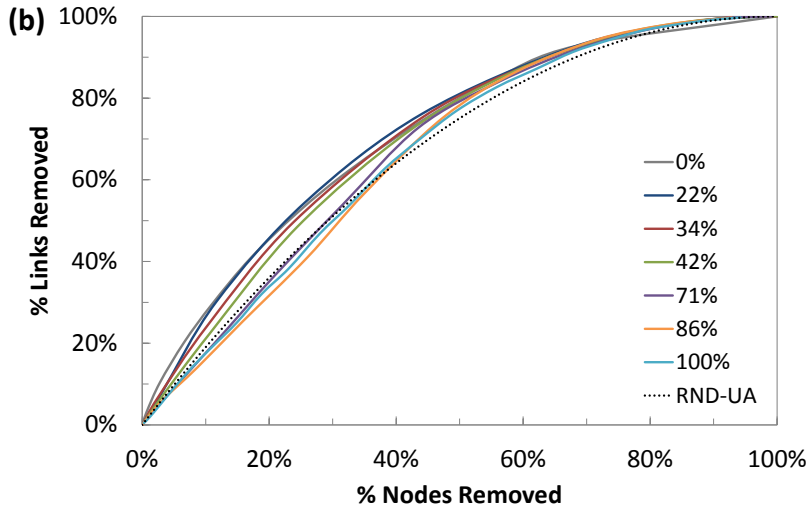
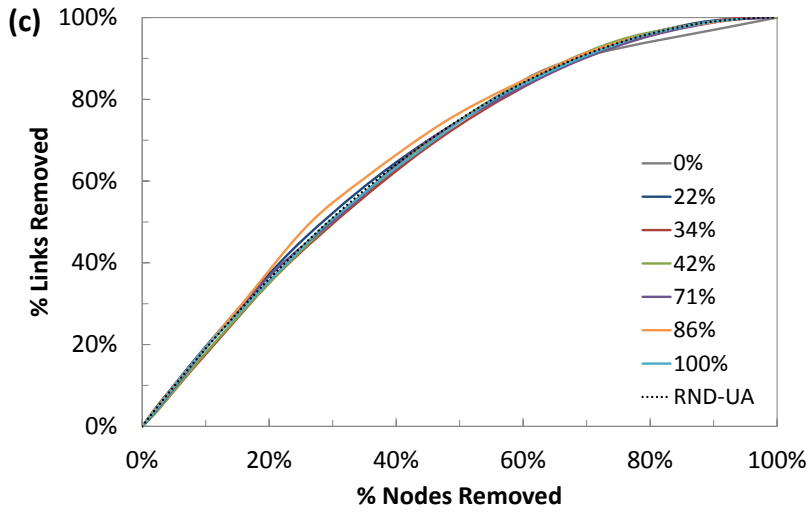


Figure 4.10: Showing the results for all locations of the spatial hazards, for an average of 10 exponential networks with a uniform with area nodal layout, where nodes are introduced (a, d) with distance, (b, e) proportional with distance and (c, f) randomly. It is worth noting that there is a small scatter in the results for each of the 10 networks.


(a)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
RND-UA


(b)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
RND-UA


(c)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
RND-UA

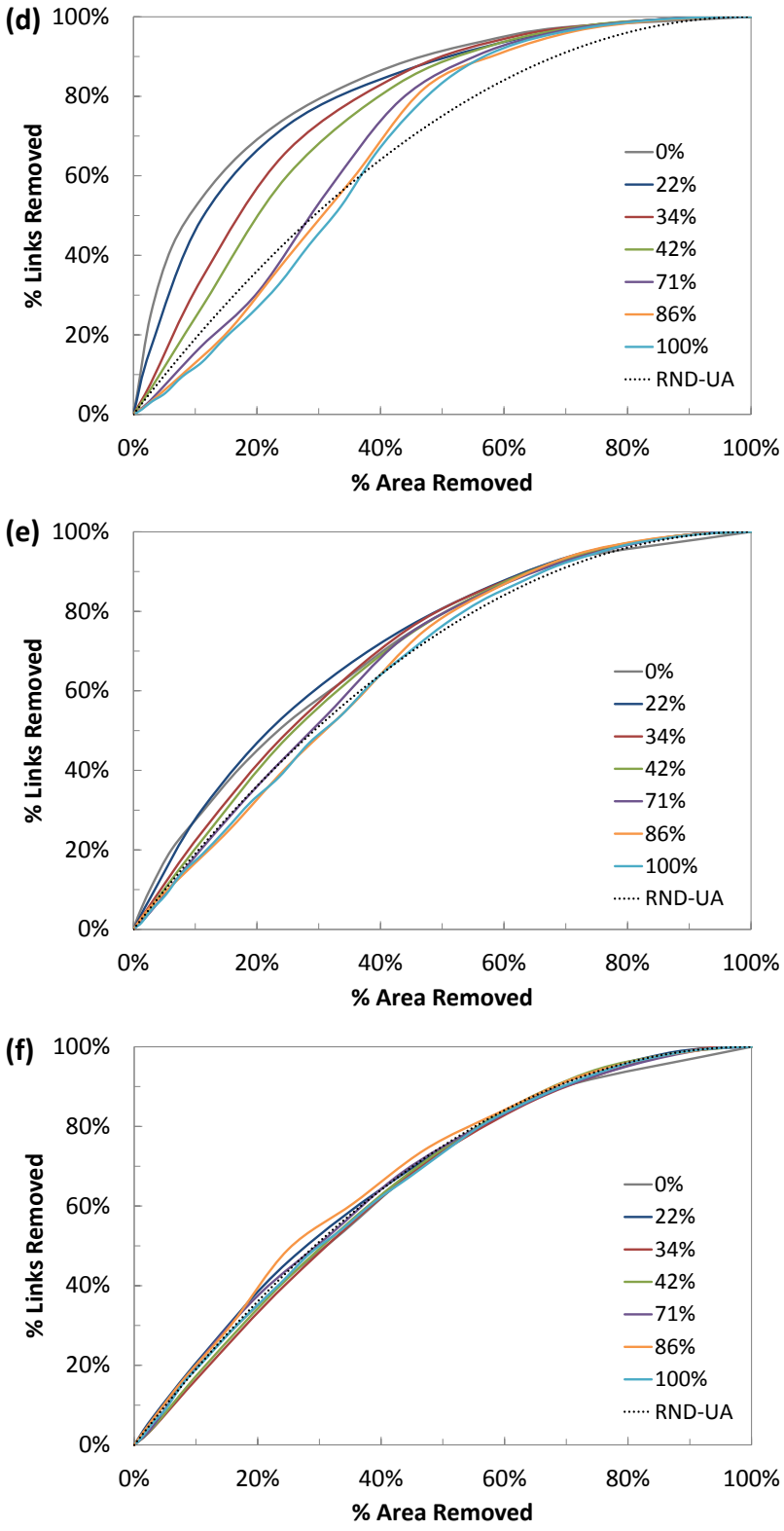


Figure 4.11: Showing the results for all locations of the spatial hazards, for an average of 10 scale-free networks with a uniform with area nodal layout, where nodes are introduced (a, d) with distance, (b, e) proportional with distance and (c, f) randomly. It is worth noting that there is a small scatter in the results for each of the 10 networks.

For the networks where the nodes are introduced with distance, it can be seen that as the centre of the hazard 'moves' from being located on the geographical centre of the network towards the spatial boundary (perimeter) the network becomes increasingly resilient to the spatial hazard. It can also be seen that there is a significant difference in the hazard tolerance results between the 0% and 100% hazards (i.e. the 'central attack' and 'perimeter attack' strategies). For the exponential networks this difference can be quantified as a 43% point different between the percentage of links removed when 20% of nodes have been removed (also a 43% point difference for scale-free networks). This difference, in the percentage of links removed, reduces to 16% points for exponential networks (and 13% points for scale-free networks) when the nodes are introduced proportional with distance and to an 8% point difference for exponential networks (5% points for scale-free networks) where nodes introduced randomly. This demonstrates that the location of the spatial hazard has the greatest effect to the hazard tolerance of the networks where the nodes are introduced with distance and, conversely, has very little effect to the hazard tolerance of the networks when the nodes are introduced randomly. This sensitivity to the spatial hazard location is due to the location, and concentration, of the high degree nodes in the networks. For the networks where the nodes are introduced with distance, the high degree nodes tend towards the centre of the network (Figure 4.5); therefore a hazard located in the centre of the network will remove more links per node removed compared to hazards located on the perimeter of the network. Plotting the results in terms of the percentages of area and links removed shows the same trend in results (as the nodes are dispersed uniformly throughout the network area, therefore approximately the same percentage of nodes as percentage of area will be removed by a spatial hazard of a given size).

Comparing the hazard tolerance of the exponential and scale-free networks to the benchmark random networks (Figure 4.10, Figure 4.11), shows that both of these more sophisticated network models are more vulnerable to the spatial hazard located on, or close to, the geographic centre of the network. There is a 29% point difference between the percentages of links removed for the exponential networks (35% points for the scale-free networks) between the 0% hazard and the random network, when 20% of nodes have been removed. This difference reduces to 12% points for

exponential networks (10% for scale-free networks) when the nodes are introduced proportional with distance and to 4% for exponential networks (and 3% for scale-free networks) when nodes are introduced randomly (for the same percentage of nodes removed). This reduction in percentage of links removed, compared to the random network, is again due to the location of the high degree nodes in the network.

There are three positions of the spatial hazard which result in both the exponential and scale-free networks showing an increased resilience compared to the random network. This is only for networks where the nodes are introduced with distance and for small sizes of the spatial hazard. These three spatial hazards are located on, or close to, the spatial boundary of the network (the 71%, 86% and 100% hazards in Figure 4.10 and Figure 4.11). The exponential networks are resilient until between 25-34% of nodes (29-35% for scale-free networks) or 23-38% of area has been removed (28-37% for scale-free networks). Introducing the nodes proportional with distance also results in the exponential and scale-free networks showing an increased resilience compared to the random network for two locations of the spatial hazard (86% and 100%). In this case, the exponential networks are resilient until 35% of nodes (the same for scale-free networks) or 40% of area (the same for scale-free networks) has been removed. This increased resilience, for these two node introduction orders, is due to the location of the majority of the high degree nodes close to the geographic centre of the network and therefore the location of mainly low degree nodes close to the spatial boundary of the network. The networks are resilient to only small sizes of the spatial hazard and then become increasingly vulnerable when these high degree nodes are removed (i.e. when the spatial hazard reaches the centre of the network).

It can be concluded that networks where the nodes are introduced with distance show the greatest sensitivity to locations of the spatial hazard, when the results are plotted in terms of percentage of links and percentage of nodes or area. These networks show an increased resilience to hazards located close to the spatial boundary of the network, but an increased vulnerability to hazards located close to the geographic centre of the network, compared to the benchmark random networks. Therefore, networks with a similar spatial configuration as the EATN will not only display an increased vulnerability to a spatial hazard which extends from the perimeter of the network towards the geographic centre (as previously discussed), but also to smaller spatial hazards which

move from the perimeter towards the geographic centre. Whereas this analysis has shown that the hazard tolerance of networks with a similar spatial configuration as the USATN are less affected by the location of spatial hazard.

The next sub-chapter will investigate the effects of different nodal locations (uniform with distance and clustered) to the hazard tolerance of these networks (again considering scale-free, exponential and random networks with one of the three node introduction orders).

4.5: COMPARISON OF HAZARD TOLERANCE FOR DIFFERENT NODAL LAYOUTS

To assess the effect of nodal location to the hazard tolerance of the networks, the two additional nodal layouts (uniform with distance, Figure 4.1(a), and clustered, Figure 4.1(c)) are used. These nodal layouts are combined with the three network classes (exponential, scale-free and random) and the three node introduction orders (random, proportional with distance and with distance from the geographic centre). The resulting networks have been subjected to the seven positions of the spatial hazard (shown in Figure 4.9).

4.5.1: UNIFORM WITH DISTANCE NODAL LAYOUT

The hazard tolerance for the networks with a uniform with distance nodal distribution, show the same trends as those with a uniform with area distribution when plotting the percentages of nodes and links removed (Figure 4.12). However, the hazard tolerance changes when plotted in terms of the percentage of area and links removed, due to the different nodal distributions.

The uniform with distance nodal layout has a higher density of nodes located close to the geographic centre of the network, and therefore a smaller density of nodes located close to the spatial boundary of the network, than the uniform with area nodal layout (this can be seen visually in Figure 4.1(a, b)). Consequently, hazards located close to the geographic centre of the network will remove a higher proportion of nodes than hazards located close to the spatial boundary of the network. This ultimately changes

the hazard tolerance of the networks when the results are plotted in terms of the percentage of links and area removed (rather than plotting the percentage of links and nodes removed).

The networks where the nodes are introduced with distance still show the most sensitivity to the locations of the spatial hazard (for both the scale-free and exponential networks) and are highly vulnerable to hazards located over the geographic centre of the network. For the exponential networks there is a 76% point difference (the same for the scale-free networks) between the percentages of links removed for the 0% ('central attack') and 100% ('perimeter attack') spatial hazards when 20% of area has been removed. This compares to a 40% point difference for exponential networks (and 43% point difference for scale-free networks) with a uniform with area nodal layout and the same node introduction order (again when 20% of the area has been removed). Therefore, it can be seen that the nodal layout of the network also affects the sensitivity of the network to spatial hazard location.

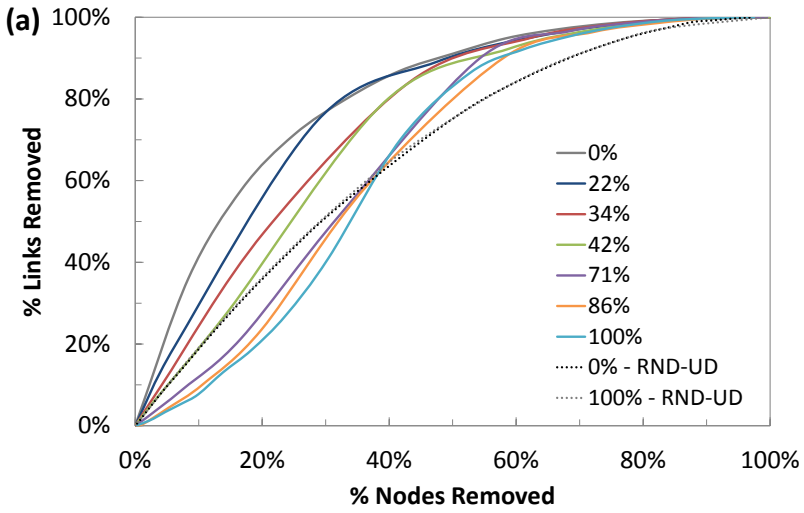
For the networks where the nodes are introduced proportional with distance, there is also a greater variability in the hazard tolerance results, compared to the uniform with area layout. There is a 66% point for exponential networks (65% point for scale-free networks) between the 0% and 100% spatial hazards when 20% of the area has been removed. Networks where nodes are introduced randomly to the network also show a sensitivity to the location of the spatial hazard, unlike networks with a uniform with area distribution. There is a 43% point difference for exponential networks (and a 44% point difference for scale-free networks) between the two 'extreme' spatial hazard locations (when 20% of the area has been removed). This can again be attributed to the spatial distribution of nodes throughout the spatial area of the network.

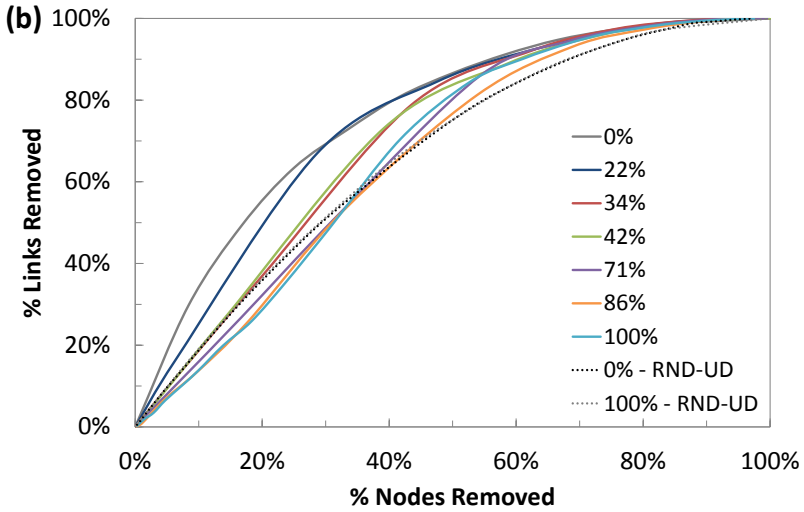
The random networks, with a uniform with distance nodal layout, also show sensitivity to the location of the spatial hazards, when plotting the results in terms of percentage area removed. Due to increase in density of nodes in the centre of the network, hazards close to the centre will remove a higher proportion of nodes (and consequently more links) than those on the perimeter of the network, where there is a lower density of nodes. For this reason, the hazard tolerance of the random networks has been assessed for these two 'extreme' locations of the spatial hazard (Figure 4.12,

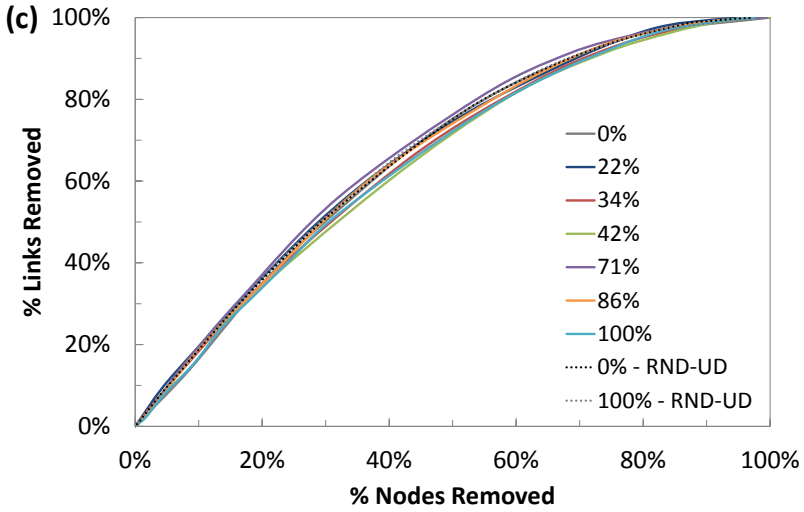
Figure 4.13). This enables a comparison with the exponential and scale-free networks to be made, although for these two locations of the spatial hazard only.

Similarly to the previous nodal layout, the networks where the nodes are introduced with distance show the greatest resilience / vulnerability compared to the random network, due to the concentration location of the high degree nodes around the geographic centre of the network. The exponential networks are 20% points more resilient (the same for scale-free networks) than the random networks to the central hazard (0%), when 20% of the area has been removed and are 13% points (14% points for scale-free) more resilient to the perimeter hazard (100%) for the same percentage area removed.

Therefore, it can be concluded that a network with a uniform with distance nodal layout can show more sensitivity to locations of the spatial hazard, than networks with a uniform with area nodal layout. This has important implications for infrastructure owners, who must carefully consider the location / distribution of highly connected and important components within their system. If all of these components are located close to the geographic centre then the resulting system will be extremely vulnerable to hazards located on, or close to, this area. Not only will the highly connected components be removed but many other nodes will be removed, having potentially devastating effects for the system (due to a significant proportion of components and connections removed, leading to a potentially extended period of repair and loss of service provision).


(a)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
0% - RND-UD
100% - RND-UD


(b)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
0% - RND-UD
100% - RND-UD


(c)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
0% - RND-UD
100% - RND-UD

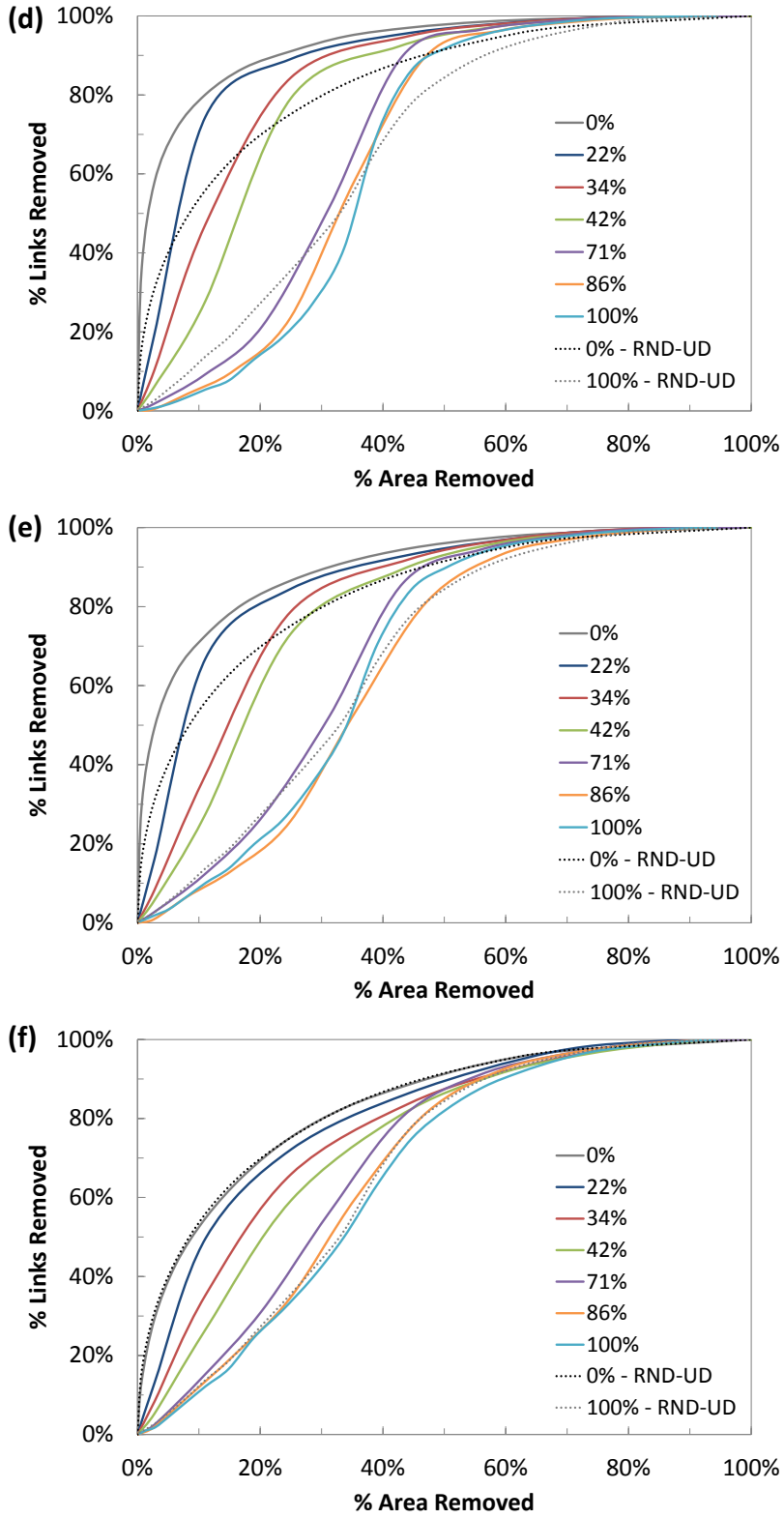
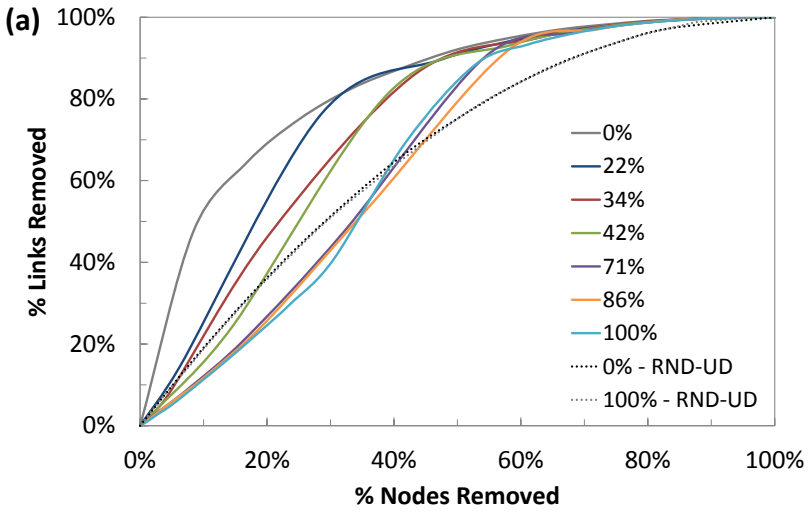
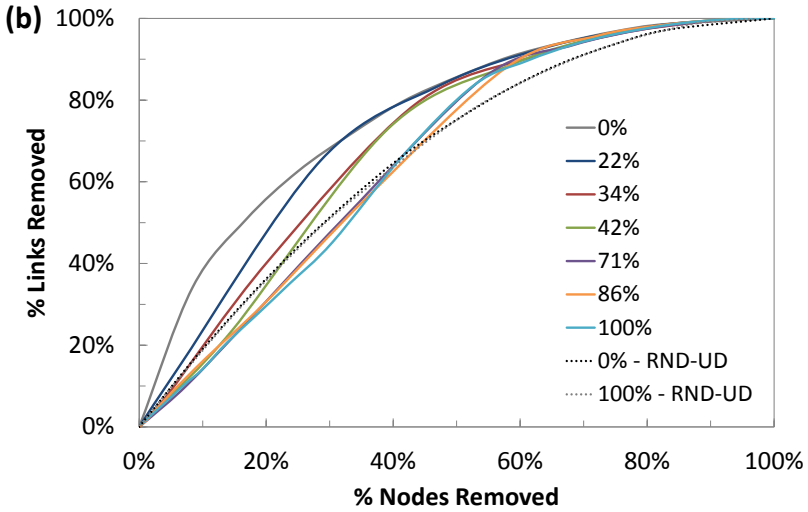
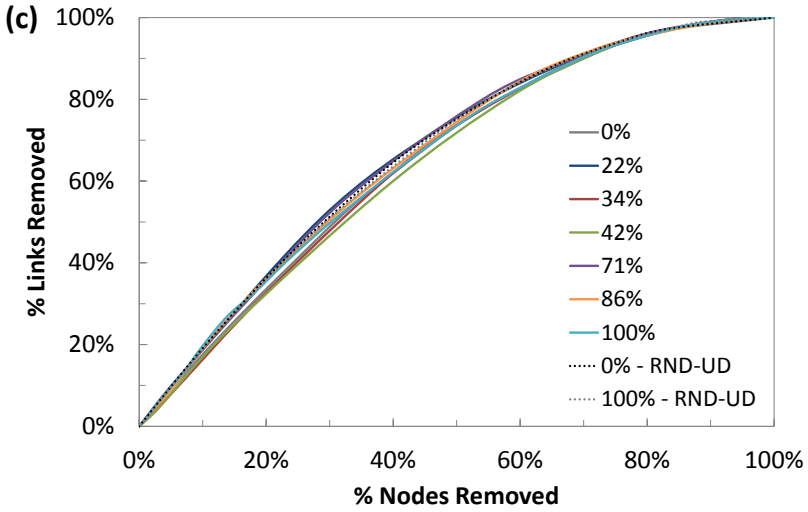


Figure 4.12: Showing the results for all locations of the spatial hazards, for an average of 10 exponential networks with a uniform with distance nodal layout, where nodes are introduced (a, d) with distance, (b, e) proportional with distance and (c, f) randomly. It is worth noting that there is a small scatter in the results for each of the 10 networks.


(a)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
0% - RND-UD
100% - RND-UD


(b)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
0% - RND-UD
100% - RND-UD


(c)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
0% - RND-UD
100% - RND-UD

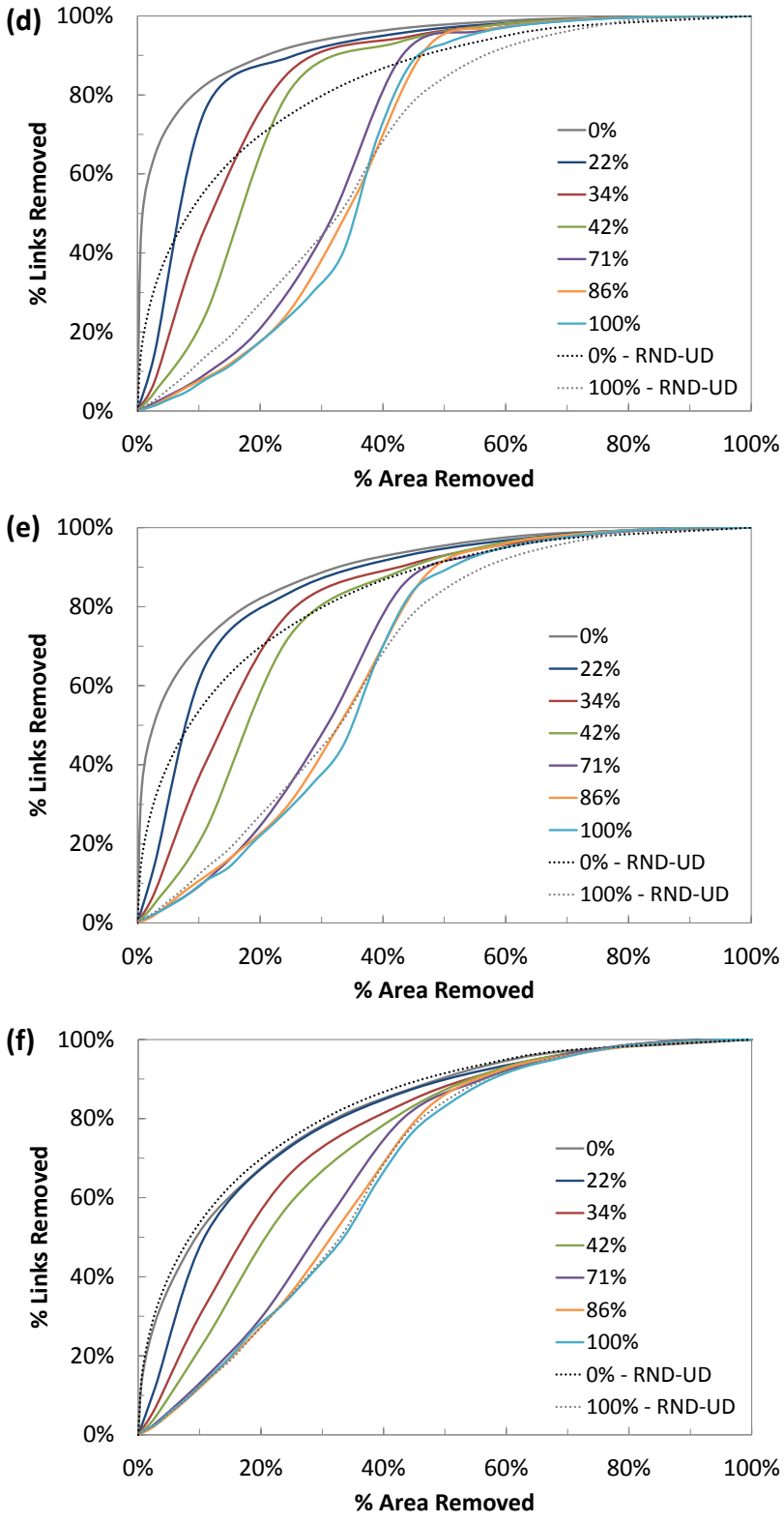


Figure 4.13: Showing the results for all locations of the spatial hazards, for an average of 10 scale-free networks with a uniform with distance nodal layout, where nodes are introduced (a, d) with distance, (b, e) proportional with distance and (c, f) randomly. It is worth noting that there is a small scatter in the results for each of the 10 networks.

4.5.2: CLUSTERED NODAL LAYOUT

The networks with a clustered nodal layout show the same trends in results as both the uniform with area and uniform with distance nodal layouts, when plotting the percentages of nodes and links removed by each location of the spatial hazard (Figure 4.15, Figure 4.16). Although, in a similar manner to the uniform with distance nodal layout, plotting the results in terms of the percentages of area and links removed changes the hazard tolerance compared to the uniform with area nodal layout.

However, the plotted results do not form 'smooth' curves for the increasing spatial hazard size unlike the previous two nodal layouts; as they can show sharp increases in results for a small change in the size of the spatial hazard. This is caused by the removal of a whole cluster of nodes in the network (causing a sharp increase in the proportion of nodes/links removed for a small increase in the size of the hazard). Figure 4.14 shows the results for 10 clustered networks, with different nodal layouts, the same node introduction order and subjected to the same spatial hazard. From this figure, the 'jump' in results for some networks can be easily seen. However, as the results shown in Figure 4.15 and Figure 4.16 are an average of the results achieved for 10 networks (with different 'cluster' locations) and therefore the impact of removing one cluster of nodes in one of the networks has been reduced (i.e. the 'jump' in results is not as obvious compared to considering one network in isolation).

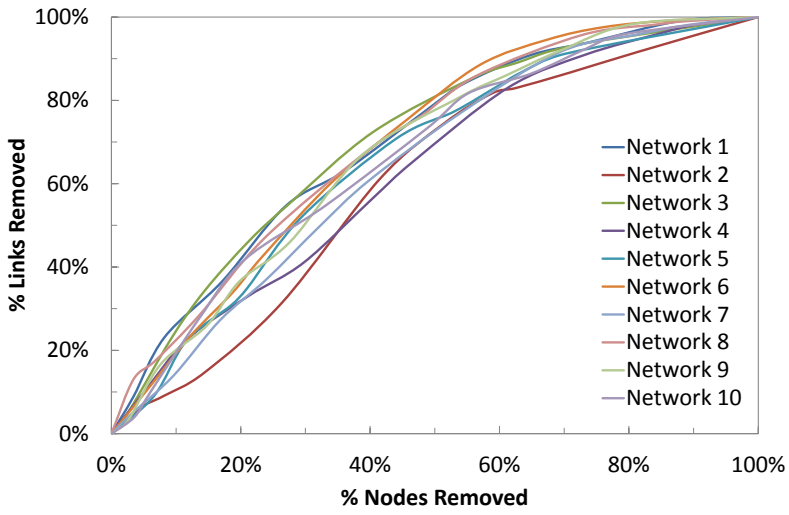


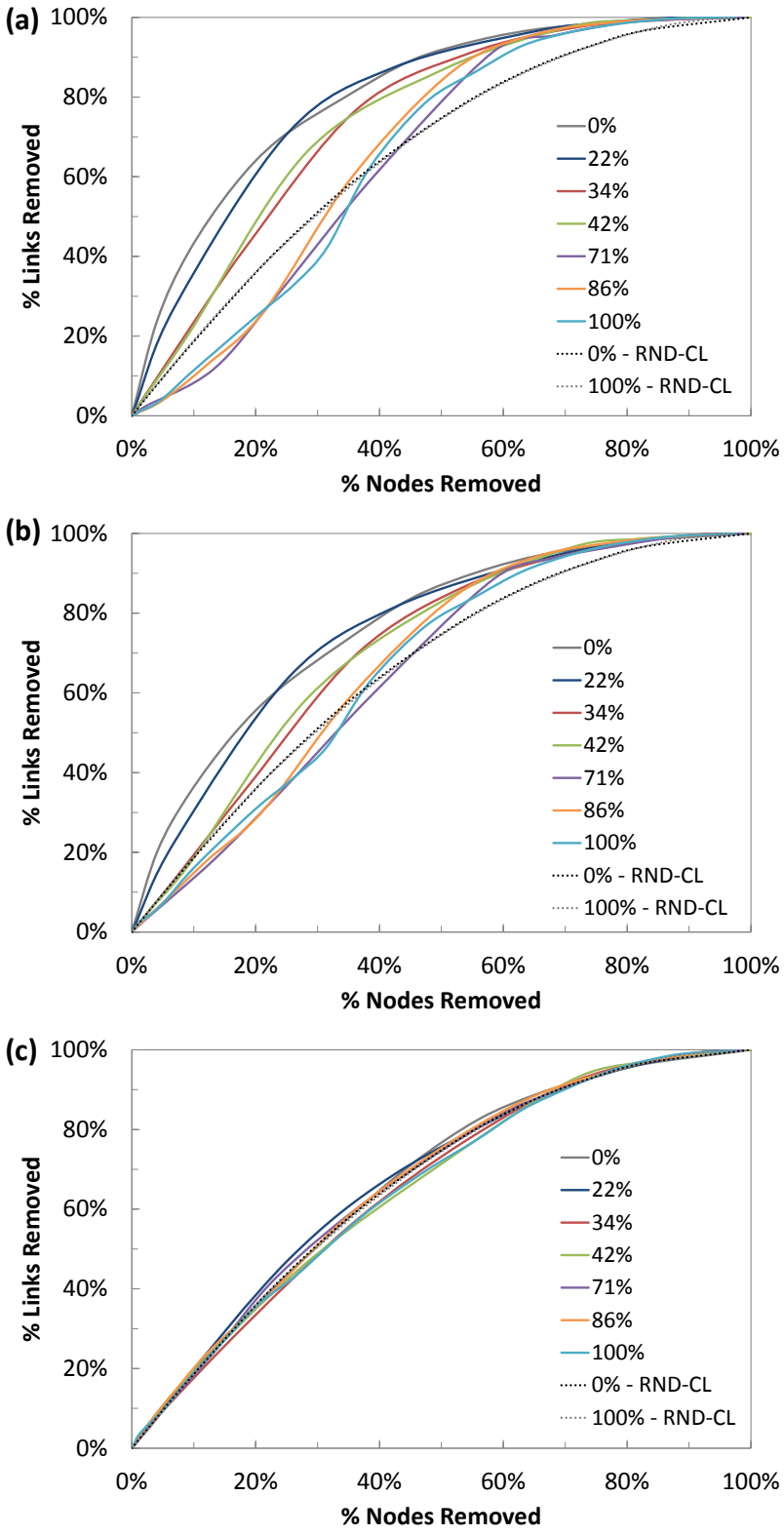
Figure 4.14: Showing the results for 10 exponential networks with a clustered layout, where the nodes were introduced randomly subjected to the 'central' attack. These results are averaged to produce the 0% result line in Figure 4.15. The amount of scatter in the results is due to the positions of the different clusters of nodes.

Similarly to the two previous nodal layouts, networks where the nodes are introduced with distance show the greatest sensitivity to locations of the spatial hazard. There is a 67% point difference for the exponential networks (68% points for the scale-free networks) between the two 'extreme' locations of the spatial hazard (i.e. 0% and 100%), when 20% of the area has been removed. This reduces to 53% points for exponential networks (51% points for the scale-free networks) when the nodes are introduced proportional to distance and to 36% points (and 36% for scale-free networks) when the nodes are introduced randomly, for the same percentage area removed. Compared to the uniform with area nodal layout this is an increase in the variability of results, but a decrease in the variability compared to the uniform with distance nodal layout. This is due to the spatial distribution of the nodes in the network (Figure 4.1). The uniform with area nodal layout gives a linear relationship between the distance from the centre of the network and the number of nodes, this relationship changes to that distinctive of a squared function for the uniform with area nodal layout. The spatial distribution of nodes for the clustered nodal layout is between these two relationships; therefore, it is logical that the variability in the hazard location (when plotted in terms of the percentage area removed) is between these two nodal layouts (for the same node introduction order).

Comparing the results to the random network, again show that networks where the nodes are introduced with distance show the greatest resilience / vulnerability compared to the random network, due to the location of the high degree nodes. The exponential networks are 23% points more resilient (24% points for scale-free networks) than the random networks to the central hazard (0%), when 20% of the area has been removed and are 10% points (10% points for scale-free) more resilient to the perimeter hazard (100%) for the same percentage area removed.

These results may have important implications for infrastructure owners, as many infrastructure systems display a clustered nodal layout (as they are 'drawn' to areas of high population). If a spatial hazard is located over one of these clusters then a high proportion of nodes (and potentially links) will be removed, for a small and otherwise inconsequential spatial hazard. However, the connectivity of the network is also important, particularly when the network becomes 'degraded', as this governs the supply of service around the system. This will be considered in the next sub-chapter,

which applies various network measures to the degraded networks to quantify their change in performance.



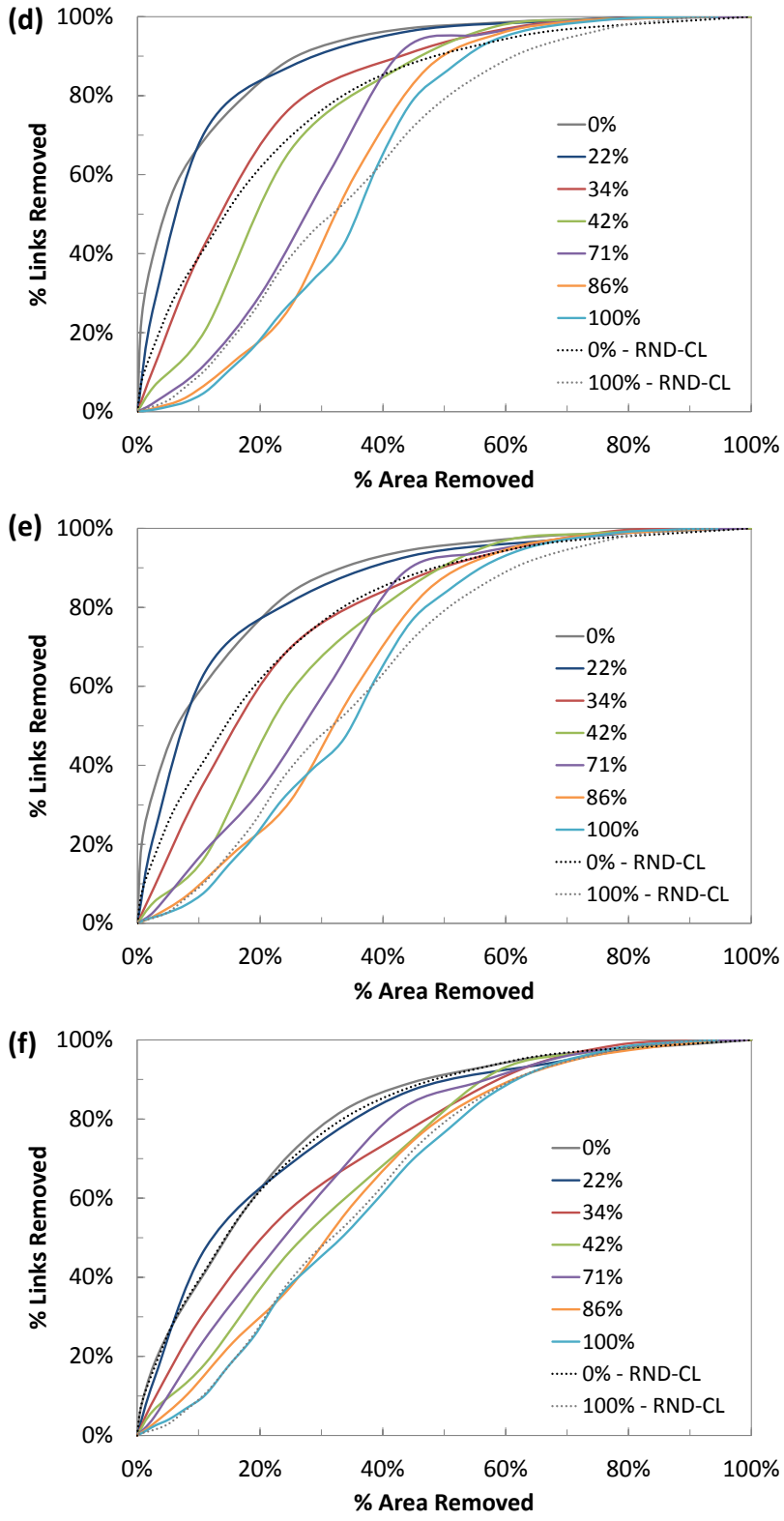
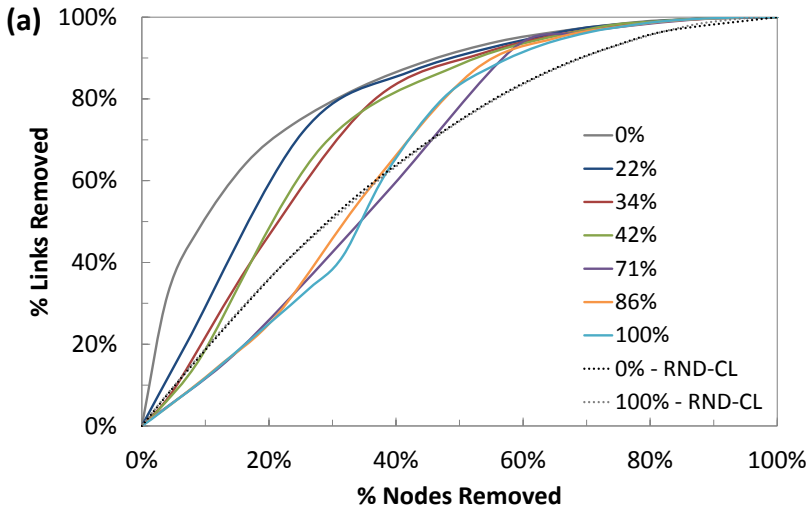
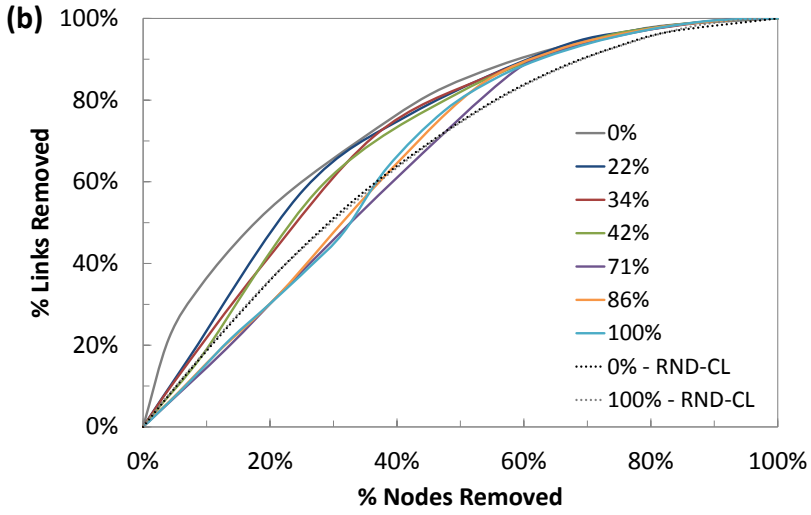
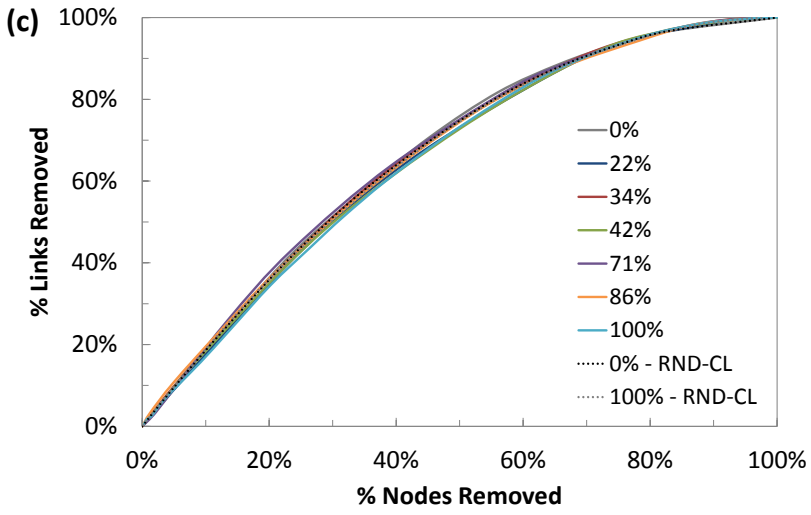


Figure 4.15: Showing the results for all locations of the spatial hazards, for an average of 10 exponential networks with a clustered nodal layout, where nodes are introduced (a, d) with distance, (b, e) proportional with distance and (c, f) randomly.


(a)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
0% - RND-CL
100% - RND-CL


(b)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
0% - RND-CL
100% - RND-CL


(c)
100%
80%
60%
40%
20%
0%
% Links Removed
0%
20%
40%
60%
80%
100%
% Nodes Removed
0%
22%
34%
42%
71%
86%
100%
0% - RND-CL
100% - RND-CL

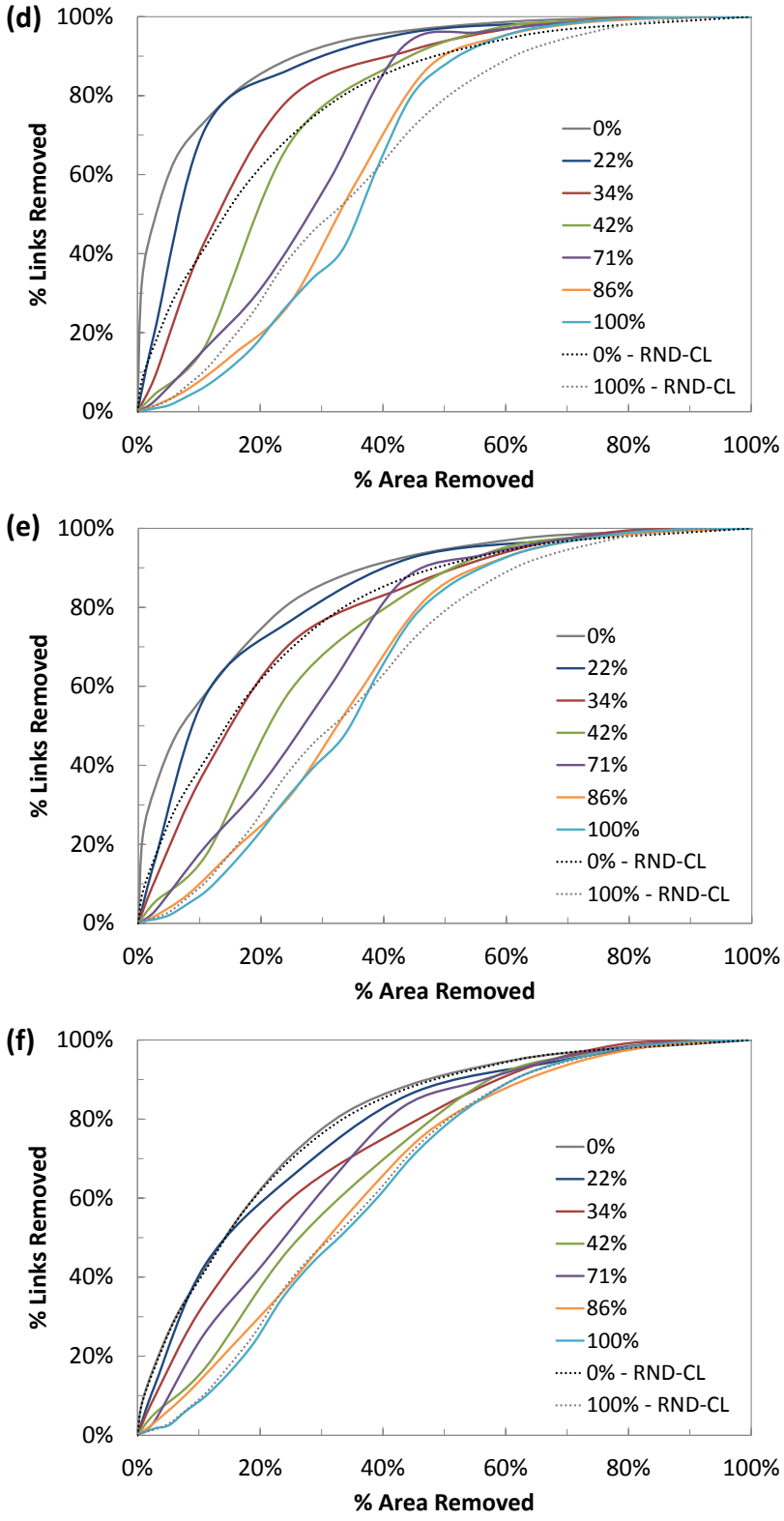


Figure 4.16: Showing the results for all locations of the spatial hazards, for an average of 10 scale-free networks with a clustered nodal layout, where nodes are introduced (a, d) with distance, (b, e) proportional with distance and (c, f) randomly.

4.5.2.1: EFFECT INDIVIDUAL CLUSTER DENSITY ON THE HAZARD TOLERANCE OF THE NETWORK

All of the networks with a clustered nodal layout analysed, so far, in this Chapter have used one value of C_D (equal to 200). This value is now varied to determine its effects to the hazard tolerance of the resulting network, when subjected to the central attack (Figure 3.35) and perimeter attack spatial hazards (Figure 4.6). To keep to number of results to a manageable, and presentable, only the random network class has been used (as using the more sophisticated exponential and/or scale-free network class would mean that sets of results for the three node introduction orders would need to be analysed, tripling the number of results). In this analysis, seven different C_D values (which are equally dispersed from C_D = 50 to C_D = 350) have been used and a random network generated for each, the resulting distribution of nodes in three of these networks is shown in Figure 4.17. These networks all have the same initial conditions, with the exception of the C_D value, and the probability that a node will not be located inside the influence of a cluster is 0.2 (the same as the previous clustered nodal layouts in this chapter).

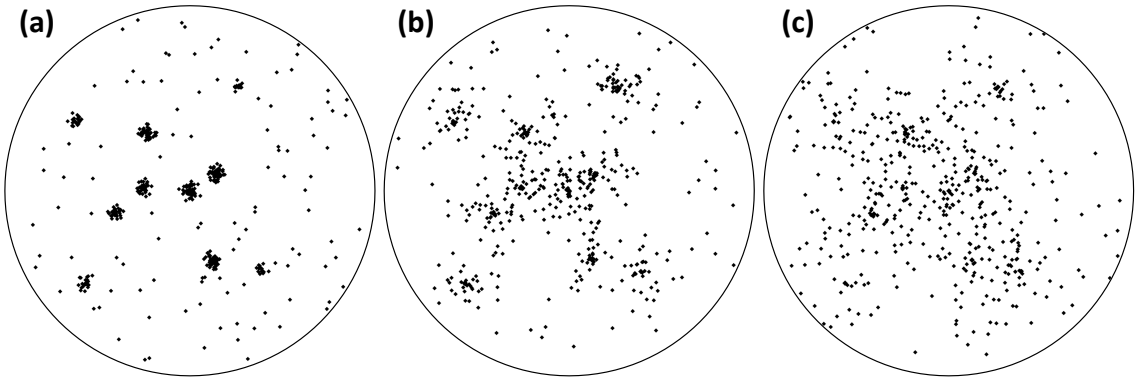


Figure 4.17: Three of the seven clustered layouts used to demonstrate the hazard tolerance of generated clustered nodal layouts generated with the same seed locations and radii, but using different C_D values: (a) C_D = 50, (b) C_D = 200, (c) C_D = 350.

The degree distribution, spatial distribution and spatial degree distribution for the seven generated networks has been shown in Figure 4.18. From this figure it can be seen that the degree distribution for all networks is approximately equal and that, for networks with a higher C_D value the spatial distributions are 'smoother' than those with small C_D values. This is due to the higher C_D value causing the individual clusters of nodes to be less dense and also overlap (which can be seen visually in Figure 4.17), resulting in a more spatially dispersed nodal configuration. This is reflected in the spatial distributions, as they show a sharp increase in the number of nodes, for a small

increase in the distance, for networks with a small C_D value (and therefore dense clusters) but not for networks with a high C_D value.

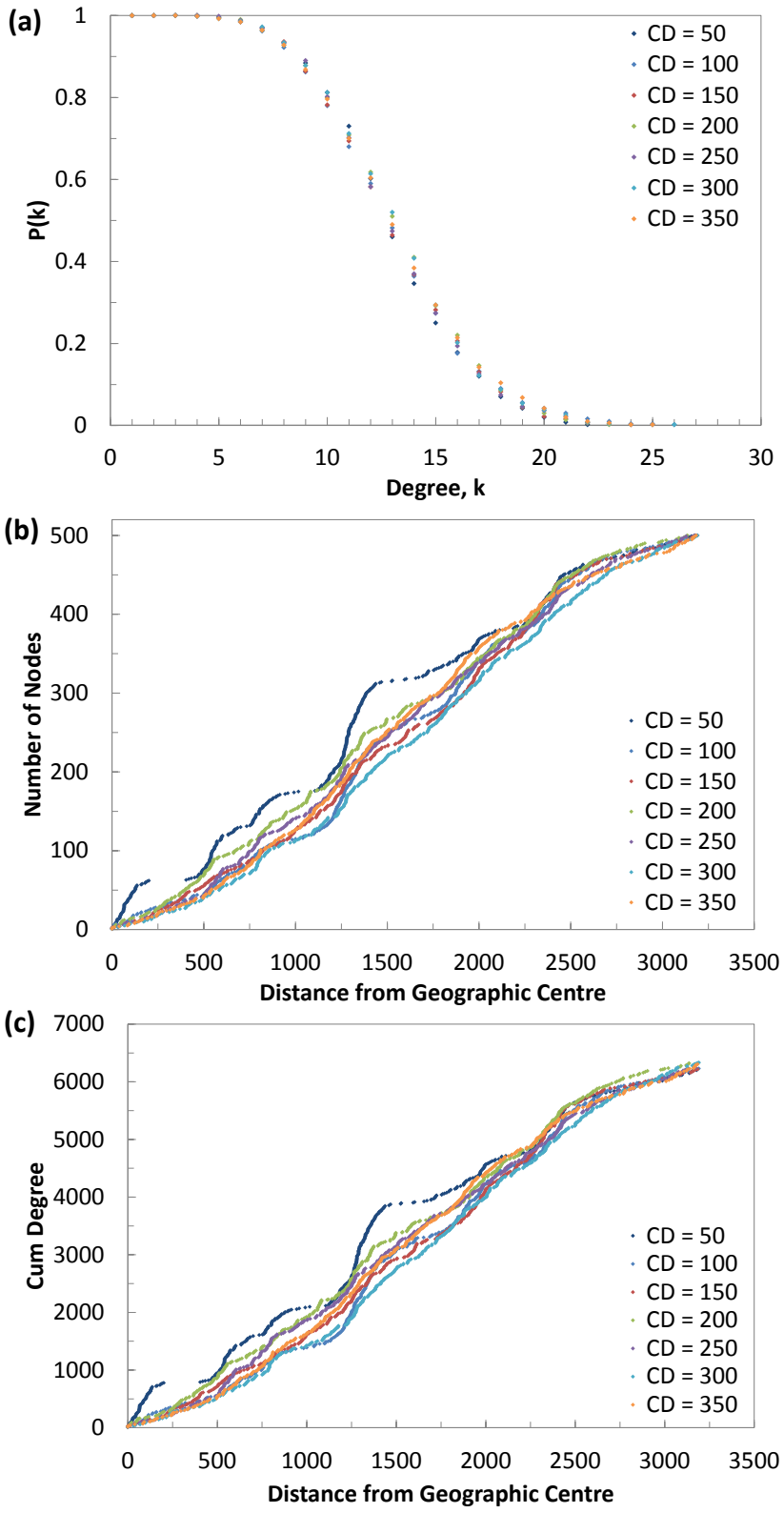


Figure 4.18: The (a) degree distribution, (b) spatial distribution and (c) spatial degree distribution for seven random networks, with different clustered nodal layouts. As all nodes in a random network have approximately the same degree, the degree distribution (shown in (a)) has not been presented on a log scale.

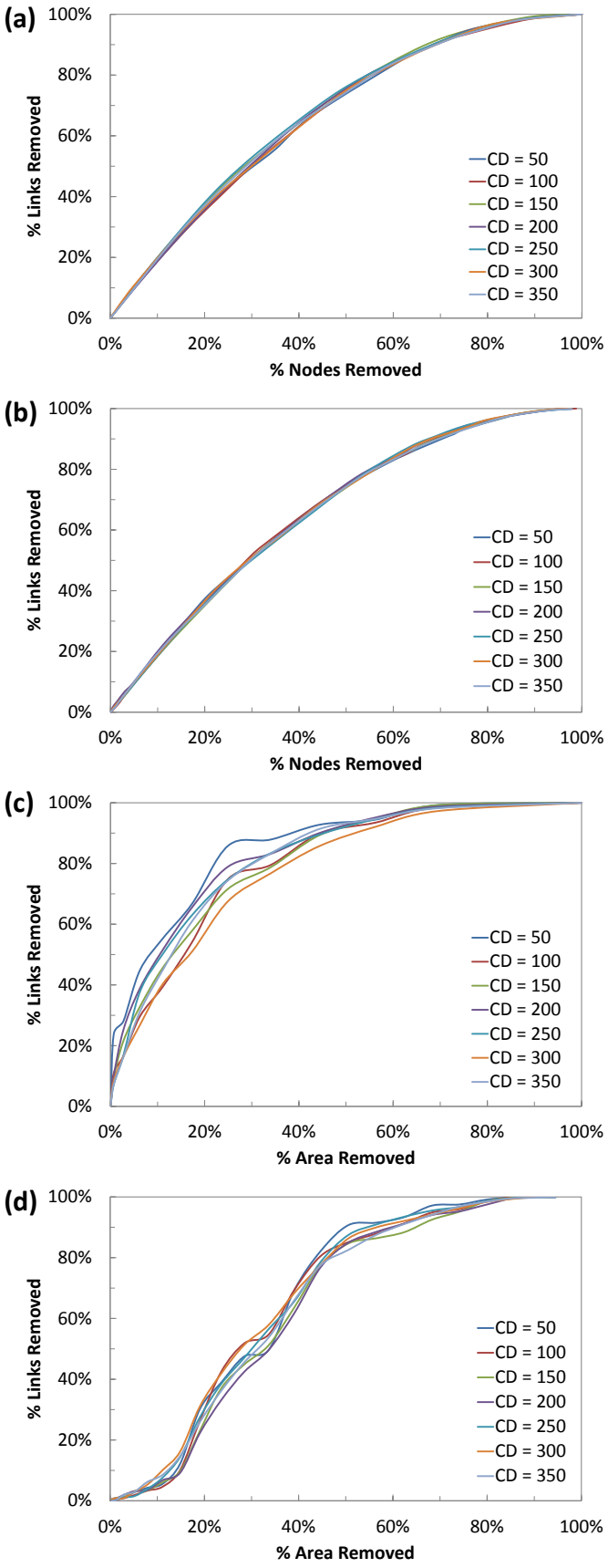


Figure 4.19: Hazard tolerance of seven random networks with different clustering layouts, showing (a, c) tolerance to central attack spatial hazard and (b, d) tolerance to perimeter spatial hazard.

The results of the hazard tolerance analysis, shown in Figure 4.19, show that all of the networks have the same hazard tolerance when the results are plotted in terms of the proportion of nodes and links removed, for both spatial hazards. This result is expected as the spatial layout of nodes is not considered in this method of presenting the results and random networks are homogeneous (so for the same proportion of nodes removed there should be the same proportion of links removed). However, including a spatial element in the presentation of the results shows that there is a small amount of scatter between the seven networks; but more apparent, is the effect that cluster density has to the hazard tolerance. For the networks with a small C_D value the removal of one of the dense clusters causes a sharp increase in the proportion of links removed for a small increase in hazard size (this is particularly evident for the perimeter spatial hazard when between 30-35% of the network area is removed (Figure 4.19(d))). From these results it can also be seen that the networks do not become progressively resilient, or vulnerable, with an increasing C_D value. Although, these seven networks show a similar hazard tolerance to the two applied spatial hazards, their hazard tolerance to randomly placed hazards will be different, due to the specific placement of clusters in the layout.

It can therefore, be concluded that the hazard tolerance is dependent on the location, and density, of the individual clusters in the network in relation to the spatial hazard size and location. For networks with tight clusters (e.g. C_D = 50) the placement of these dense clusters must be considered when planning the spatial layout of the network, relative to that of any potential spatial hazards, and also in the placement of the high degree nodes in more structured network classes (e.g. placing all of the high degree nodes in one cluster will render the network highly vulnerable to the removal of this small spatial area). Whereas, the placement of clusters in networks with more dispersed nodes (e.g. C_D = 350) is less important, as a larger spatial area must be covered by the hazard to remove the whole of the cluster.

4.6: QUANTIFYING CHANGE IN PERFORMANCE / CONNECTIVITY USING NETWORK MEASURES

The results in this chapter have, so far, focused on quantifying the proportion of links (connections) removed for a given proportion of nodes or area removed. This provides infrastructure owners with information regarding the number links (representing pipelines, transmission lines, for example) which may need to be replaced or repaired following a disaster (from which impacts such as costs or down time can be estimated). However, for some infrastructure systems it is the efficiency (e.g. the time taken to transfer a flow of service around the system) that can also be considered to be important. For these systems, plotting the results in terms of proportion links removed does not give an insight into the efficiency of the system. For example, a high percentage of pipelines may have been removed from a water distribution system, but if these pipelines were not trunk mains then the resulting impact to the efficiency of the network may be negligible. However, if these links were trunk mains then high disruption may be caused.

This sub-chapter applies the MCS and APL network measures (defined in Chapter 2.5.4) to the networks used in the previous sub-chapter, allowing the efficiency of the networks to be quantified. To enable a 'manageable' number of results to be presented, only the central attack and perimeter attack strategies (Figure 3.35, Figure 4.6) will be considered, as these have been shown to be the best and worst case scenarios. The efficiency and resilience of both the exponential and scale-free networks will be considered, as will all three nodal layouts and node introduction orders. The results of the analysis are plotted in terms of the proportion of nodes removed (to establish if node introduction order and/or network class affects the efficiency and resilience of the network) and also in terms of the proportion of area removed (to determine the effect that nodal layout has on the hazard tolerance / efficiency).

4.6.1: CONNECTIVITY AND EFFICIENCY OF BENCHMARK RANDOM NETWORKS

The change in connectivity and efficiency of the benchmark random networks is initially established (before comparisons with the exponential and scale-free networks are made), for all three nodal configurations and for both locations of spatial hazard.

Figure 4.20 plots the change in connectivity (MCS) for the random networks when subjected to the central and perimeter attack strategies. From this figure, it can be seen that all of the random networks maintain a highly connected structure for both locations of the spatial hazard when the results are plotted in terms of the proportion of nodes removed, due to the homogeneous nature of a random network. However, plotting the results in terms of the proportion of area removed shows that the nodal configuration of a network affects its connectivity as the hazard grows. The random networks with a uniform with area nodal configuration show the greatest resilience to the central attack spatial hazard, as these networks maintain connectivity as the hazard expands (e.g. for each node removed by the hazard, the MCS drops by approximately one). Whereas, the networks with a uniform with distance or clustered nodal layout show vulnerability to this spatial hazard, as the MCS drops quickly for small sizes of spatial hazard (with a reduction in MCS of 83 for a spatial hazard covering 5% of the network area for a uniform with distance layout and 48 for a clustered layout, compared to the uniform with area nodal configuration). This is due to the high density of nodes around the geographic centre of the network for both of these nodal configurations and not because to the topology of the network. In contrast, these two nodal configurations show resilience to small sizes of the perimeter attack spatial hazard, compared to the uniform with area configuration, due to the presence of a smaller number of nodes close to the perimeter of these networks, but become less connected after 35-45% of the network area has been removed (when the high density of nodes around the geographic centre is reached by the hazard).

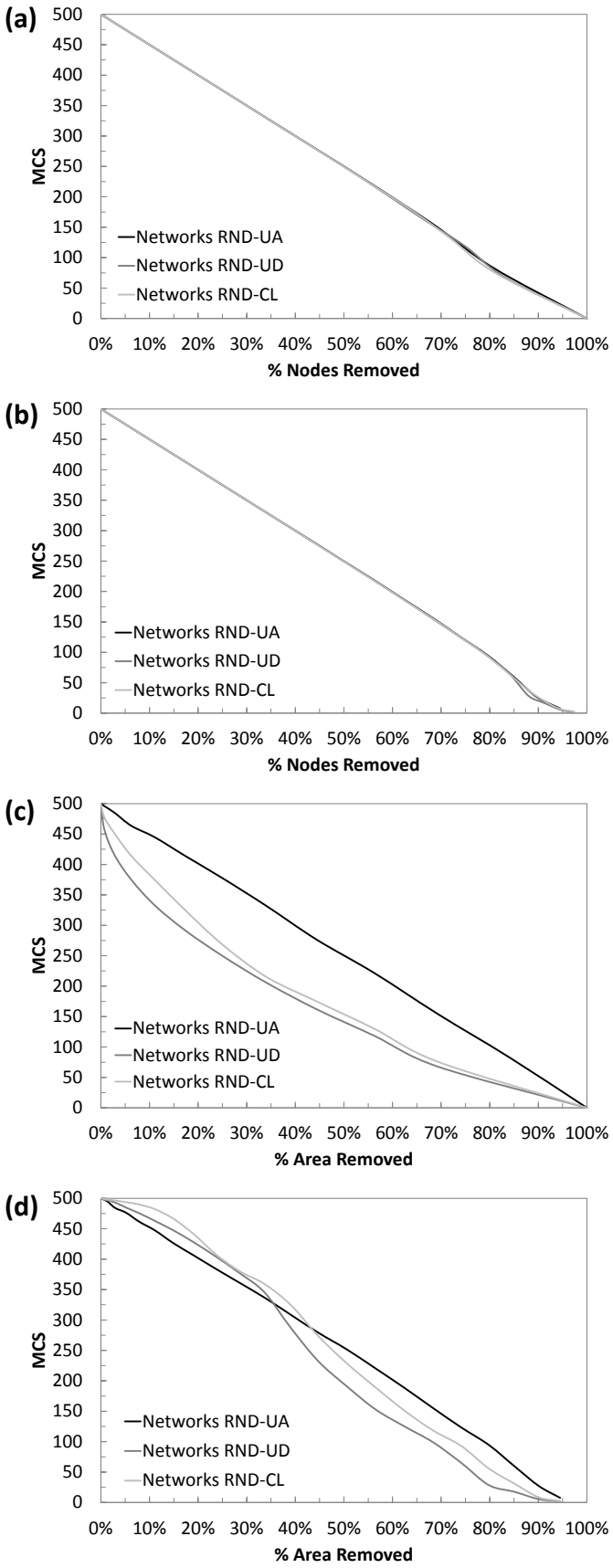


Figure 4.20: Showing how the maximum cluster size (MCS) changes for the random networks when subjected to (a, c) central attack and (b, d) perimeter attack spatial hazards. Each line shown in the graphs is the average of ten networks.

The change in APL (which is indicative of the efficiency of a network) for the same networks due to the expansion of both the central attack and perimeter attack spatial hazards are shown in Figure 4.21. It should again be noted that APL is only a valid measure until the results show a dramatic increase in efficiency (a drop in APL), for reasons previously discussed. From this figure it can be seen that all of the random networks have approximately the same efficiency and become increasingly inefficient (displaying higher values of APL) to both locations of the spatial hazard as the hazards grow, until 70% of the nodes have been removed. Further expansion of the spatial hazard causes the efficiencies of the networks to diverge by a small but noticeable amount. However, plotting the results in terms of the proportion of area removed shows that there are differences in the efficiencies of the three nodal layouts for all sizes of the spatial hazards. The random network with a uniform with area nodal configuration is the most efficient for all sizes of the central attack spatial hazard, due to the spatial dispersion of nodes throughout the network area. Both the uniform with distance and clustered nodal layouts have a higher proportion of nodes closer to the geographic centre of the network, meaning that for hazards located over this area a higher proportion of nodes will be removed, ultimately causing the networks to become more inefficient than the uniform with area configuration.

However, it is interesting to note that whilst a smaller proportion of nodes are removed from the random networks with the uniform with distance and clustered nodal configurations by small sizes of the perimeter attack spatial hazard (until 35% of the network are has been removed), their efficiency is approximately the same as the networks with a uniform with area nodal layout. This can be attributed to the approximately equal efficiency of all random networks under normal operational conditions and the number of nodes needed to noticeably change the APL of a network. Unlike the MCS, the APL is not affected by the removal of a small proportion of nodes in a random network (as they all have approximately the same degree). The APL considers the shortest path length between all pairs of nodes in the network and the removal of a small proportion of nodes (and therefore a small proportion of links) will not significantly affect this value, consequently, causing all networks to show an approximately equal efficiency for small sizes of the perimeter attack spatial hazard.

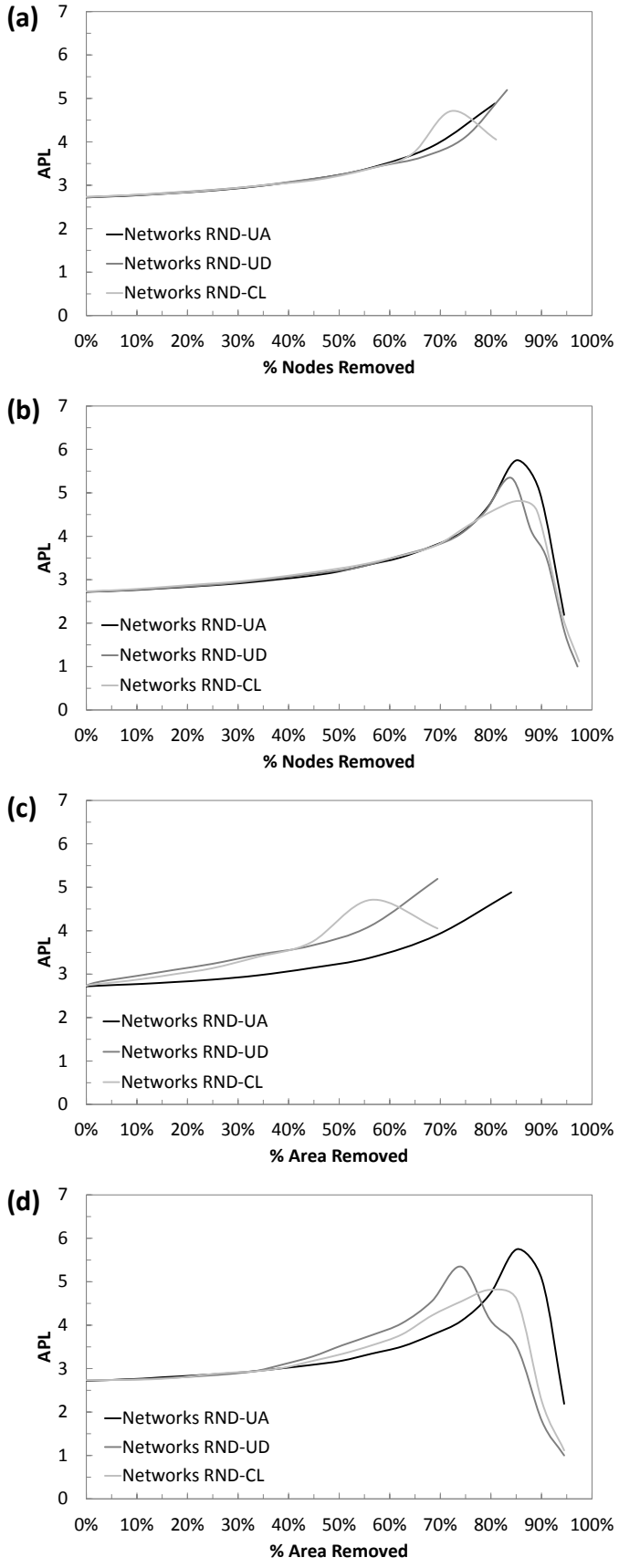


Figure 4.21: Showing how the shortest average path length (APL) changes for the random networks when subjected to (a, c) central attack and (b, d) perimeter attack spatial hazards. Each line shown in the graphs is the average of ten networks.

4.6.2: EFFECTS OF NODE INTRODUCTION ORDER AND NETWORK CLASS

The results for the scale-free networks, plotted in Figure 4.22, shows that networks with different nodal configurations show approximately the same MCS values when the networks are subjected to spatial hazard, but the order in which nodes are introduced to a network does effects the network connectivity. Networks where the nodes are introduced randomly (red lines) show the greatest resilience to both locations of spatial hazard (maintaining a higher APL value) than the networks where the nodes are introduced proportional to distance (green lines) and with distance from the geographic centre (blue lines). This trend is more noticeable when the networks are subjected to the central attack spatial hazard (Figure 4.22(a)), but can also be seen in the results for the perimeter attack, after 40% of the nodes have been removed (Figure 4.22(b)) and is due to the location of the high degree nodes within these networks. For the networks where the nodes are introduced proportional to distance and with distance, the majority of highly connected components are located around the geographic centre of the network. It has already been shown that when this area is removed by spatial hazard the network shows an increased number of removed links compared to a random benchmark network, rendering the network vulnerable to this hazard.

From Figure 4.22 it can be seen that the removal of these high degree nodes causes a disproportionate decrease in the MCS, which is due to the topological characteristics of a scale-free network. Many of the low degree nodes (which may only have one connection) are attached to a high degree node (as a result of the network generation algorithm); therefore when these high degree nodes are removed by the hazard a number of low degree nodes can be left without a connection to the remaining network (causing a disproportionate reduction in the MCS). This trend can also be observed in the exponential networks, shown in Figure 4.23, and is again caused by the location of the high degree nodes and the topological structure of the network.

The results achieved for the exponential networks (Figure 4.23(a)) are similar to those previously shown for the three real world air traffic networks (Figure 3.57(a)). In these networks introducing nodes randomly to the network created the best fit proxy network (considering both the topological and spatial characteristics) and it can be seen from Figure 3.57(a) that the USATN maintains a similar connectivity as the

random network and the CATN and EATN maintain this connectivity until 45% and 65% of nodes have been removed, respectively. This decrease in connectivity of the CATN and EATN has been previously explained and they do not display a similar behaviour in connectivity to the synthetic exponential networks due to their different topological and spatial characteristics.

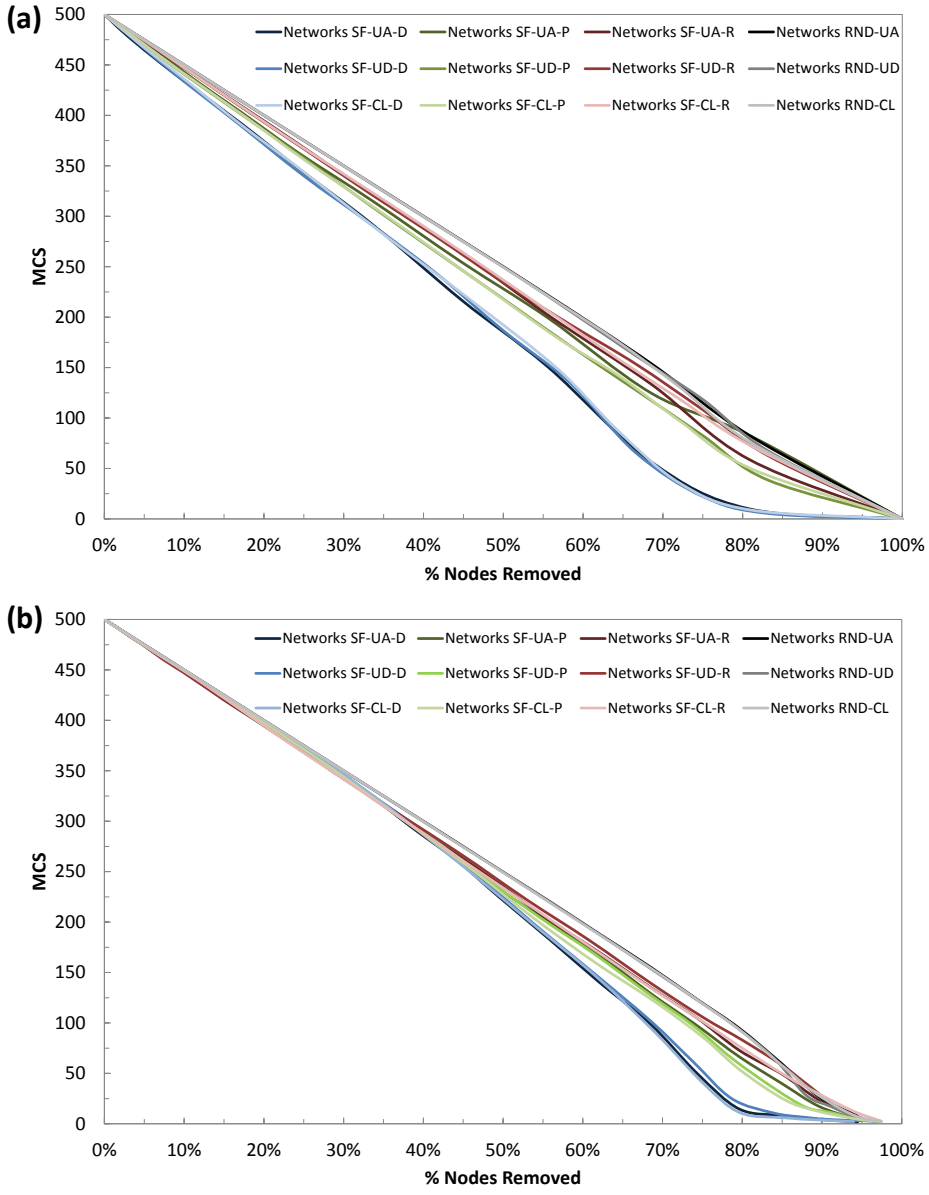


Figure 4.22: Showing how maximum cluster size (MCS) changes with node removal for scale-free networks subjected to (a) central attack and (b) perimeter attack spatial hazards. Each line of results shown is the average of ten networks. The networks where the nodes are introduced with distance are shown in shades of blue, nodes introduced proportional with distance are shown in shades of green and nodes introduced randomly are shown in shades of red. The average results for the random networks are shown in shades of grey.

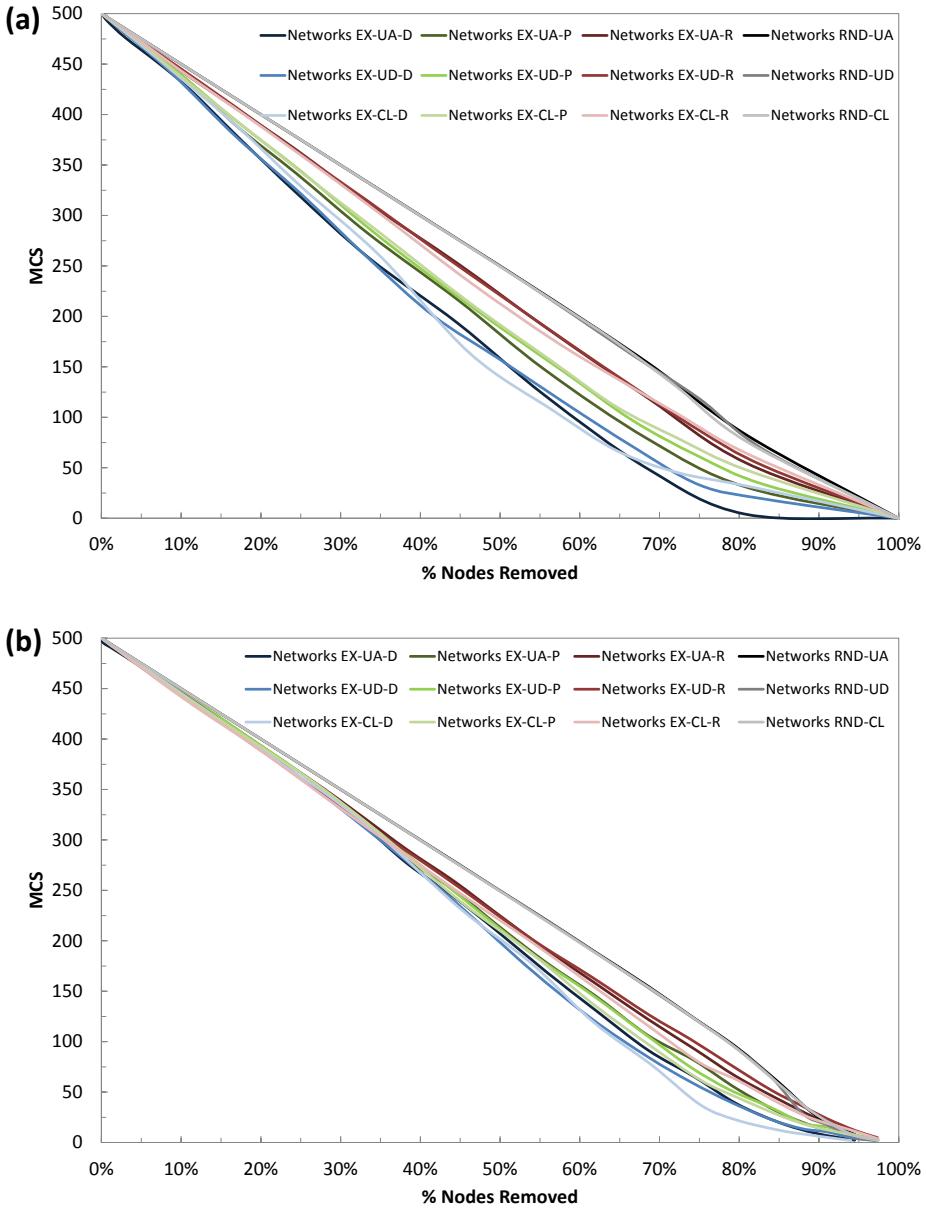


Figure 4.23: Showing how maximum cluster size (MCS) changes with node removal for exponential networks subjected to (a) central attack and (b) perimeter attack spatial hazards. Each line of results shown is the average of ten networks. The networks where the nodes are introduced with distance are shown in shades of blue, nodes introduced proportional with distance are shown in shades of green and nodes introduced randomly are shown in shades of red. The average results for the random networks are shown in shades of grey.

In the case of the air traffic networks, the MCS can determine if it is possible to travel around the network, but does not give an indication to the ease of this travel (efficiency), for this the change in APL of the networks must be considered.

The changes in APL of the scale-free and exponential networks are shown in Figure 4.24 and Figure 4.25 respectively, for both the central attack and perimeter attack spatial hazards. The results for the scale-free networks, plotted in Figure 4.25, show that all node introduction orders and nodal layouts have very similar values of APL,

when subjected to both the central attack and perimeter attack spatial hazards. However, there are large differences in the results for the different node introduction orders, particularly when subjected to the central attack spatial hazard (Figure 4.24(a)). Networks where nodes are introduced randomly to the network (red lines) show the most robust APL values and therefore the network maintains high efficiency. In contrast, networks where the nodes are introduced in order of distance (blue lines) show the greatest increase in APL and are therefore become the most inefficient and are more susceptible to disruption. This difference can be attributed to the location of the high degree nodes within the network. Locating the majority of highly connected components close to the geographic centre causes these nodes to be removed first by the central attack spatial hazard, resulting in a disproportionate effect to the proportion of links removed (as previously discussed). However, this also causes a decrease in the efficiency of the network due to the topological connectivity of a scale-free network. These networks are efficient under normal operational conditions as the numerous weakly connected nodes tend to be directly connected to one, or more, of the few highly connected nodes and can exploit this connection to quickly transfer information to other weakly connected nodes in the network. However when these highly connected nodes are removed, the network becomes increasingly inefficient as the remaining low degree nodes cannot move information quickly around the network by transferring it through a high degree node and must rely on their connections to other low degree nodes in order to transfer information (increasing their shortest path length and therefore the APL of the whole network).

Figure 4.24 also shows that the scale-free networks, where the nodes are introduced randomly, maintain a higher efficiency than the random benchmark networks to both locations of the spatial hazard. This increase in efficiency is not apparent in the networks where the nodes are introduced with distance or proportional to distance and can therefore be attributed to the spatial dispersion of high degree nodes in the network. In these scale-free networks the removal of a high degree node by the spatial hazard also causes a large number of weakly connected nodes to be removed; and it is the removal of many of these low degree nodes which causes the network to maintain efficiency (for reasons previously discussed).

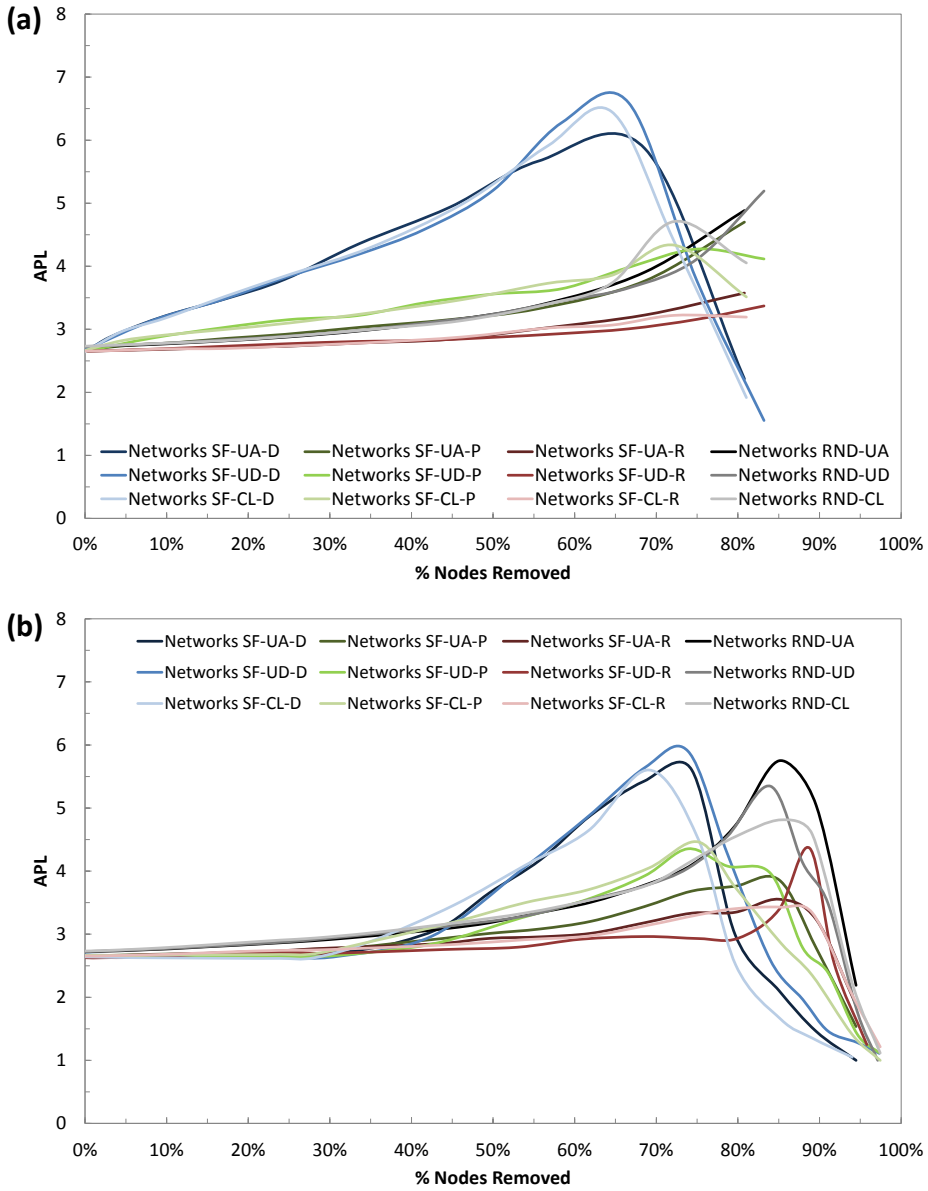


Figure 4.24: Showing how the shortest average path length (APL) changes with node removal for scale-free networks subjected to (a) central attack and (b) perimeter attack spatial hazards. Each line of results shown is the average of ten networks. The networks where the nodes are introduced with distance are shown in shades of blue, nodes introduced proportional with distance are shown in shades of green and nodes introduced randomly are shown in shades of red. The average results for the random networks are shown in shades of grey.

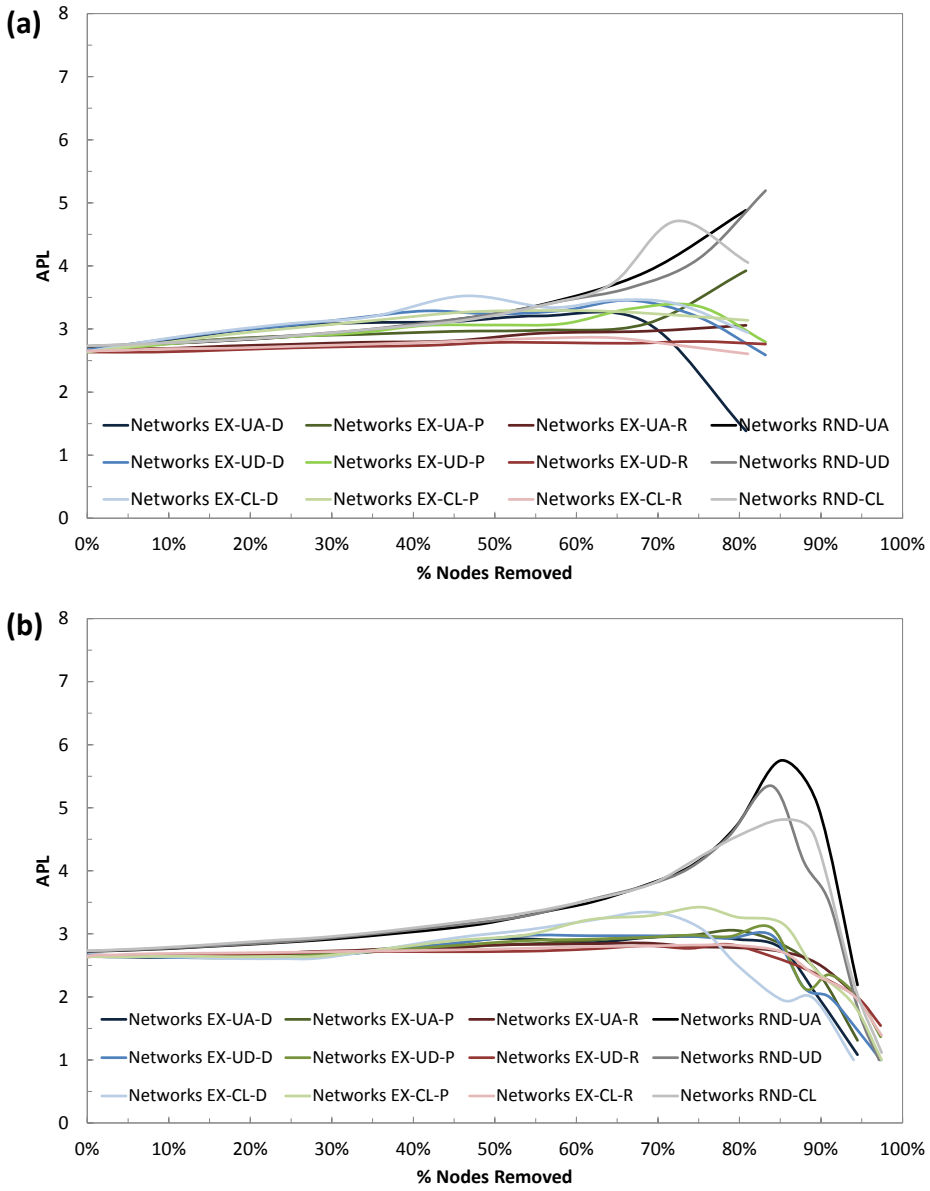


Figure 4.25: Showing how the shortest average path length (APL) changes with node removal for exponential networks subjected to (a) central attack and (b) perimeter attack spatial hazards. Each line shown in the graphs is the average of ten networks. The networks where the nodes are introduced with distance are shown in shades of blue, nodes introduced proportional with distance are shown in shades of green and nodes introduced randomly are shown in shades of red. The average results for the random networks are shown in shades of grey.

The APL of the exponential networks (Figure 4.25) follow the same trend as those for the scale-free networks when considering the order in which nodes were introduced to the network (with networks where the nodes were introduced with distance showing the greatest reduction in efficiency). However, from Figure 4.25 it can be seen that all of the exponential networks maintain efficiency compared to the random benchmark networks, unlike the scale-free networks. For example, the APL for the random networks peaks at 5.75 for the perimeter attack spatial hazard, and for the same

proportion of nodes removed the most inefficient exponential network has an APL value of 2.46. This increase in efficiency can be explained by considering the neighbourhood value which was used to generate the exponential networks. The neighbourhood size affects the probability of attachment which is used by a new node when deciding to connect links from a new node to existing nodes in the network (see Figure 3.4) and for the air traffic networks generated in Chapter 3 this neighbourhood value represents the distance that people were prepared to travel overland to reach an airport. If this value is set low enough the probability of attachment will be based on degree alone, as no other nodes will be found in the neighbourhood of each existing node (resulting in a scale-free network); whilst a high value of neighbourhood causes each existing node to have an equal probability of attachment (as the neighbourhood of each node covers the whole network area). This value therefore alters the connectivity and topological characteristics of the generated network, which can be seen when viewing the degree distribution of six networks generated with different neighbourhood values shown in Figure 4.26. These networks all have a uniform with area nodal configuration and nodes were introduced in order of distance from the geographic centre.

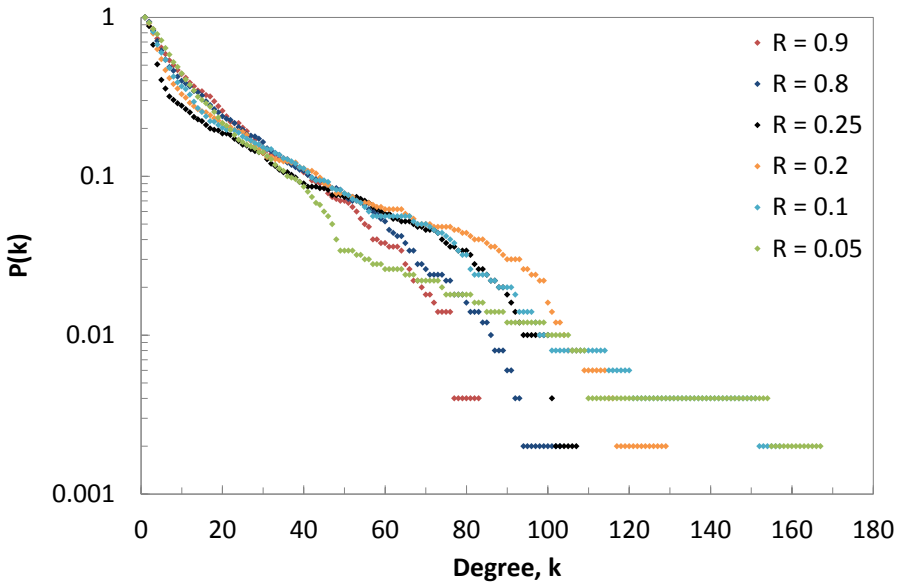


Figure 4.26: The degree distribution of six networks generated with different neighbourhood values.

From Figure 4.26 it can be seen that the network generated with the smallest value of neighbourhood (R = 0.05) has the highest degree node (with a degree of 167) and the number of connections attached to the highest degree node reduces with each

increase of neighbourhood value. This is because for a small value of neighbourhood the probability of attachment is based on degree alone meaning that the highest degree node is most likely to attract new links (causing a large degree node); whilst for a large neighbourhood all nodes have equal probability of attachment (meaning that this high degree node is now less likely to form). The effect that this neighbourhood value has to the efficiency of a network has been assessed by subjecting these six networks to the central attack spatial hazard, shown in Figure 4.27.

From Figure 4.27 it can be seen that the neighbourhood value does affect the efficiency of the generated network, particularly for large sizes of spatial hazard (after 40% of the nodes have been removed). The networks generated with a small neighbourhood value (R = 0.05) quickly become the most inefficient (with the highest values of APL) when 65% of the nodes have been removed. This neighbourhood value should cause these networks to behave in a similar manner to the scale-free networks and comparing the results to those for the scale-free networks, in Figure 4.24(a), it can be seen that this is the case. Although, these networks do not become as inefficient as the scale-free networks, with a maximum APL value of 4.51, compared to the APL value of 5.86 for a scale-free network (with the same nodal configuration and node introduction order), due to the presence of a small neighbourhood value meaning that the probability of attachment is not solely based upon degree. As the neighbourhood value increases (to R = 0.1 and R = 0.2) the generated networks are able to maintain a higher efficiency when nodes are removed by spatial hazard, with a neighbourhood value of 0.25 forming the most efficient network (this value was used to generate all of the exponential networks previously used in this Chapter). These relatively constant APL values are due to the probability of attachment of new connections being based on both degree and proximity, which causes a number of links that were bound for a high degree hub to be 'shifted' to nearby lower degree nodes. Therefore, as the hazard removes these high degree nodes there still exists a connection between many of the lower degree nodes due to this 'shift', causing the efficiency of the network to be maintained. However, with further increase of this neighbourhood value, to R = 0.8 and R = 0.9, the network no longer maintains efficiency as the hazard expands. This is due to the topological structure of these networks becoming similar to that of an unstructured random network, due to the random probability of attachment (as

previously discussed). It is worth noting that an equal probability of attachment (due to a high neighbourhood value) does not result in a generated network with the same topological structure as a random network, due to the *growth* element in this network generation algorithm.

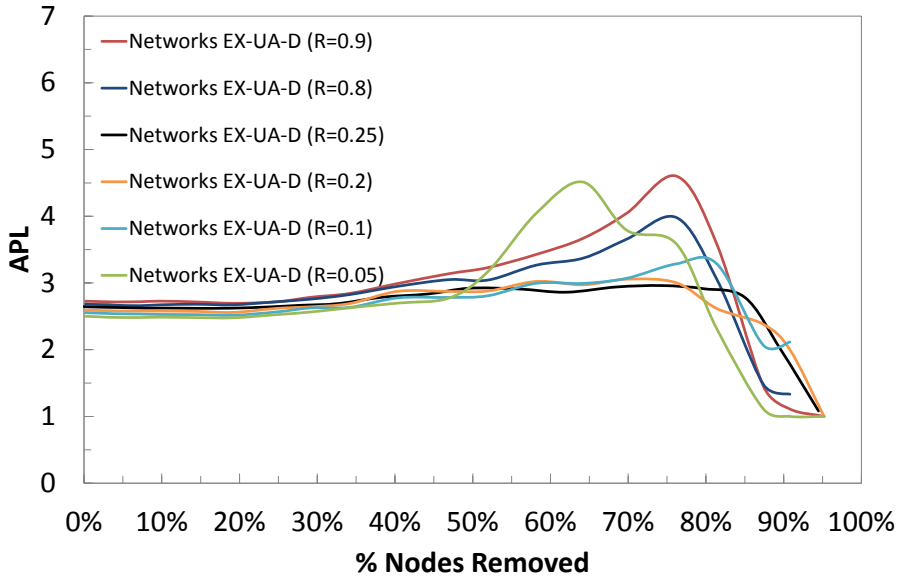


Figure 4.27: Showing how the shortest average path length (APL) changes for six exponential networks, with a uniform with area nodal configuration, when subjected to the perimeter attack spatial hazard. These networks were all generated with a different neighbourhood size (R) which is shown in the key and the nodes in all six networks were introduced in order of distance from the geographic centre.

Therefore, for the air traffic networks (and other real world infrastructure networks with a similar topology) this suggests that there is an optimal value of neighbourhood which will cause the network to maintain efficiency when subject to, in this example, the worst case location of spatial hazard (as nodes were introduced with distance and the central attack spatial hazard was used). However, this may compromise the efficiency of these networks under normal operational conditions. Table 4.1 shows the APL values for all six generated networks under normal operational conditions. From this table it can be seen that networks with a small neighbourhood size have a smaller APL than networks with a larger neighbourhood, meaning that they are more efficient under normal operational conditions. The APL value which causes the network to maintain efficiency when subjected to the worst case hazard scenario (R = 0.25) is 5.2% less efficient than the network with the smallest neighbourhood (R = 0.05) under normal operational conditions. Therefore for a real world infrastructure network it should be carefully considered whether this reduction in efficiency under normal

operational conditions is worth the maintenance of this efficiency under hazard scenario.

Table 4.1: Showing the APL of the six networks generated with different neighbourhood values under normal operational conditions.

Neighbourhood Value	APL
0.05	2.50
0.10	2.55
0.20	2.59
0.25	2.63
0.80	2.68
0.90	2.73

The results shown in this sub-chapter have been plotted in terms of the percentage of nodes removed, giving an indication of how the connectivity and efficiency of the system is affected by network class and node introduction order.

It can be concluded that exponential networks maintain a higher efficiency when degraded by hazard than both scale-free and random networks, and that this higher efficiency is caused by the topology of the network which is a result of the neighbourhood value used to generate the network. For these synthetic exponential networks a neighbourhood value of 0.25 results in the optimal efficiency of the system when subjected to the worst case central attack spatial hazard, but does slightly compromise the efficiency of the network under normal operational conditions. This research has also shown that the placement of high degree nodes affects both the connectivity and efficiency of a network. Placing the majority of high degree nodes around the geographic centre of the network (i.e. introducing nodes with distance) renders the network vulnerable to the central attack spatial hazard. This was shown to be the case in the previous sub-chapter when the results were plotted in terms of the proportions of removed nodes and links, but has also been shown to cause a disproportionate impact to the connectivity and efficiency of the networks. Whereas, spatially dispersing these high degree nodes (i.e. introducing nodes in randomly) creates a network that is the best compromise for all locations of the spatial hazard (i.e. it is not susceptible to specific location of the spatial hazard).

4.6.3: EFFECTS OF SPATIAL NODAL CONFIGURATION

The MCS has been plotted against the proportion of area removed by the central attack and perimeter attack spatial hazards for the scale-free (Figure 4.28) and exponential networks (Figure 4.29). From these results it can be seen that the nodal layout does have an effect on the connectivity of the scale-free and exponential networks, when plotting the results in terms of the percentage area removed, rather than percentage nodes removed. This again can be attributed to the high density of nodes in the centre of the uniform with distance and clustered nodal layouts and therefore the low density of nodes around the spatial boundary of the network. For the central spatial hazard, the results show that both of these nodal layouts degrade quicker (i.e. have a lower value of MCS) than the uniform with area nodal layout, meaning that the network has either broken into many smaller clusters or a large proportion of nodes have been removed. Considering the previous results plotting the MCS against the proportion of nodes removed and the MCS (shown in Figure 4.22 for scale-free networks and in Figure 4.23 for exponential networks) it can be seen that the latter of these is correct; this can also be determined by visualising the three nodal layouts (Figure 4.1). Comparing these results to the benchmark random networks, for each nodal layout, shows that both the scale-free and exponential networks are vulnerable to all sizes of the central attack spatial hazard (with a consistently lower value of MCS).

For small sizes of the perimeter hazard (until 35% of the area has been removed) both the scale-free and exponential networks with a uniform with distance and clustered nodal configuration have a higher MCS value than those with a uniform with area configuration. This can be expected as there are fewer nodes around the perimeter of the network for these two nodal configurations, therefore fewer nodes will be removed, resulting in a larger value of MCS for the same hazard size. However, when the hazard reaches the geographic centre of the network (when between 30-40% of the network area has been removed), these two nodal layouts become increasingly vulnerable. This is due to the removal of the high density of nodes around the geographic centre of the network in these two nodal configurations. Comparing these results to the random networks again shows that the random networks are more

resilient (i.e. have a consistently larger MCS value) than the scale-free networks, for the same nodal configuration.

It is also worth noting that the order in which nodes are introduced to the network also has an effect on the connectivity (MCS) of the network. Networks where the nodes are introduced with distance show lower values of MCS and are therefore less connected than networks where the nodes are introduced randomly to the network; this can be attributed to the spatial dispersion of high degree nodes in the randomly introduced nodal networks.

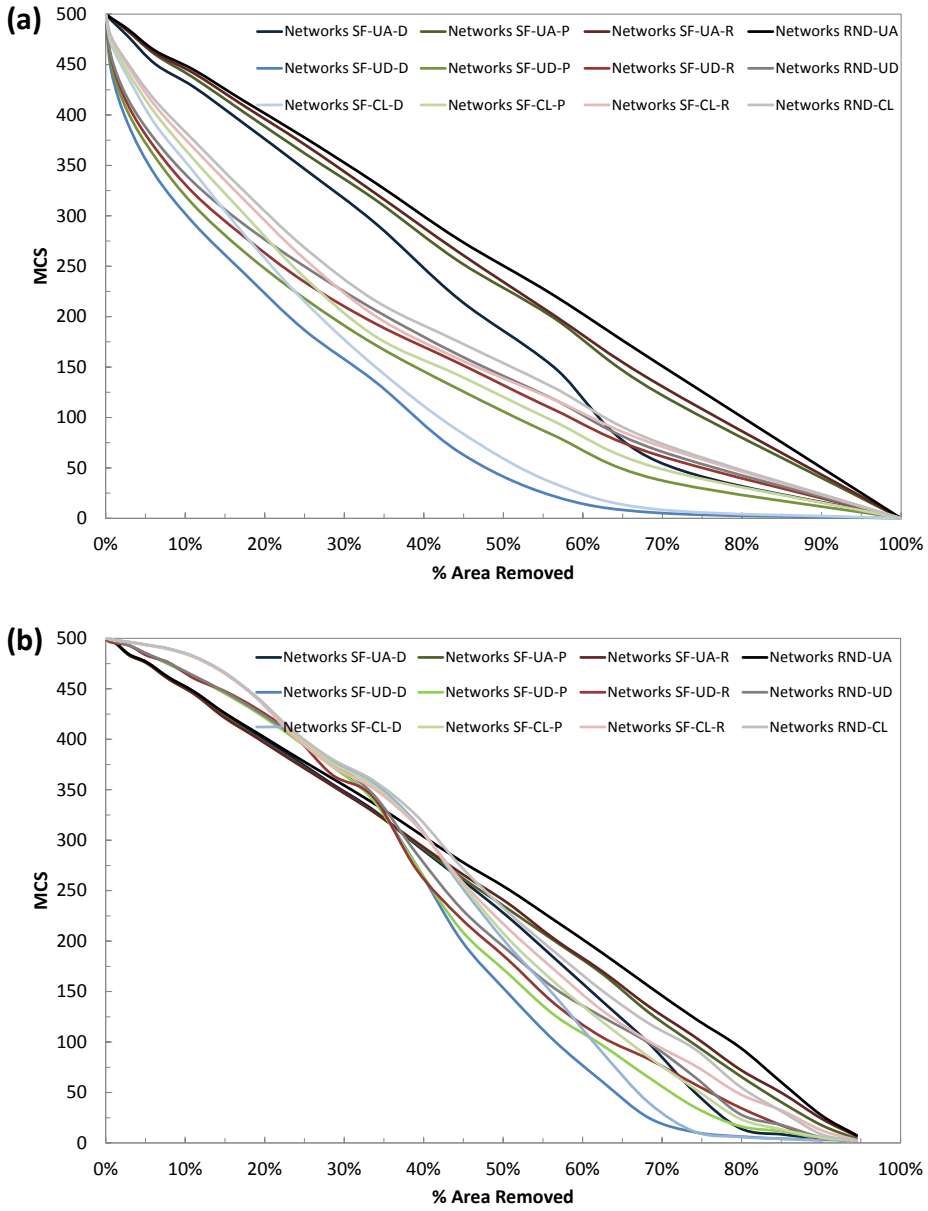


Figure 4.28: Showing how maximum cluster size (MCS) changes with area removal for scale-free networks subjected to (a) central attack and (b) perimeter attack spatial hazards. Each line of results shown is the average of ten networks. The networks where the nodes are introduced with distance are shown in shades of blue, nodes introduced proportional with distance are shown in shades of green and nodes introduced randomly are shown in shades of red. The average results for the random networks are shown in shades of grey.

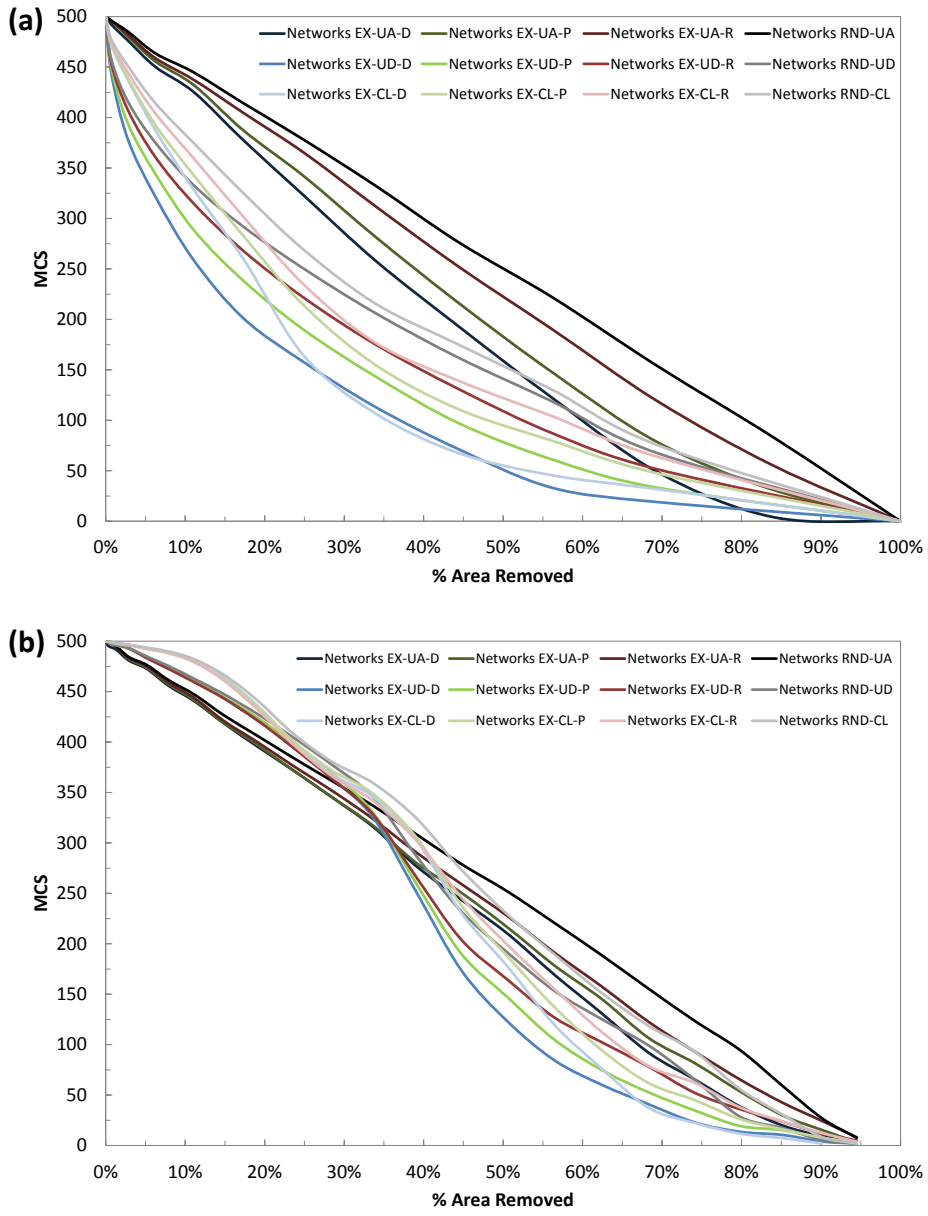


Figure 4.29: Showing how maximum cluster size (MCS) changes with area removal for exponential networks subjected to (a) central attack and (b) perimeter attack spatial hazards. Each line of results shown is the average of ten networks. The networks where the nodes are introduced with distance are shown in shades of blue, nodes introduced proportional with distance are shown in shades of green and nodes introduced randomly are shown in shades of red. The average results for the random networks are shown in shades of grey.

The change in APL with area removed by the central and perimeter attack spatial hazards have been plotted in Figure 4.30 for scale-free networks and in Figure 4.31 for exponential networks. From these figures it can be seen that the nodal configuration of a network all affects its efficiency when subjected to a hazard scenario. This is particularly evident in the scale-free networks subjected to the central attack spatial hazard (Figure 4.30(a)), where it can be seen that, for the same node introduction order, the efficiency of the networks with a uniform with distance or clustered nodal

configuration reduces at a quicker rate than the networks with a uniform with area nodal layout. This is due to the concentration of nodes around the geographic centres of these configurations, which causes the peak APL values to occur with a smaller proportion of area removed than proportion of nodes removed. From Figure 4.30(a) it can also be seen that networks with the uniform with distance nodal configuration quickly become the most inefficient (and therefore the most vulnerable) to the central attack spatial hazard as they have the highest proportion of nodes close to the geographic centre.

From Figure 4.31, it can be seen that the nodal configuration has a negligible impact to the efficiency of an exponential network, when subjected to both the central attack and perimeter attack spatial hazards and that these networks are still more efficient than the random benchmark networks. This is due to the topological characteristics of these networks, as previously discussed.

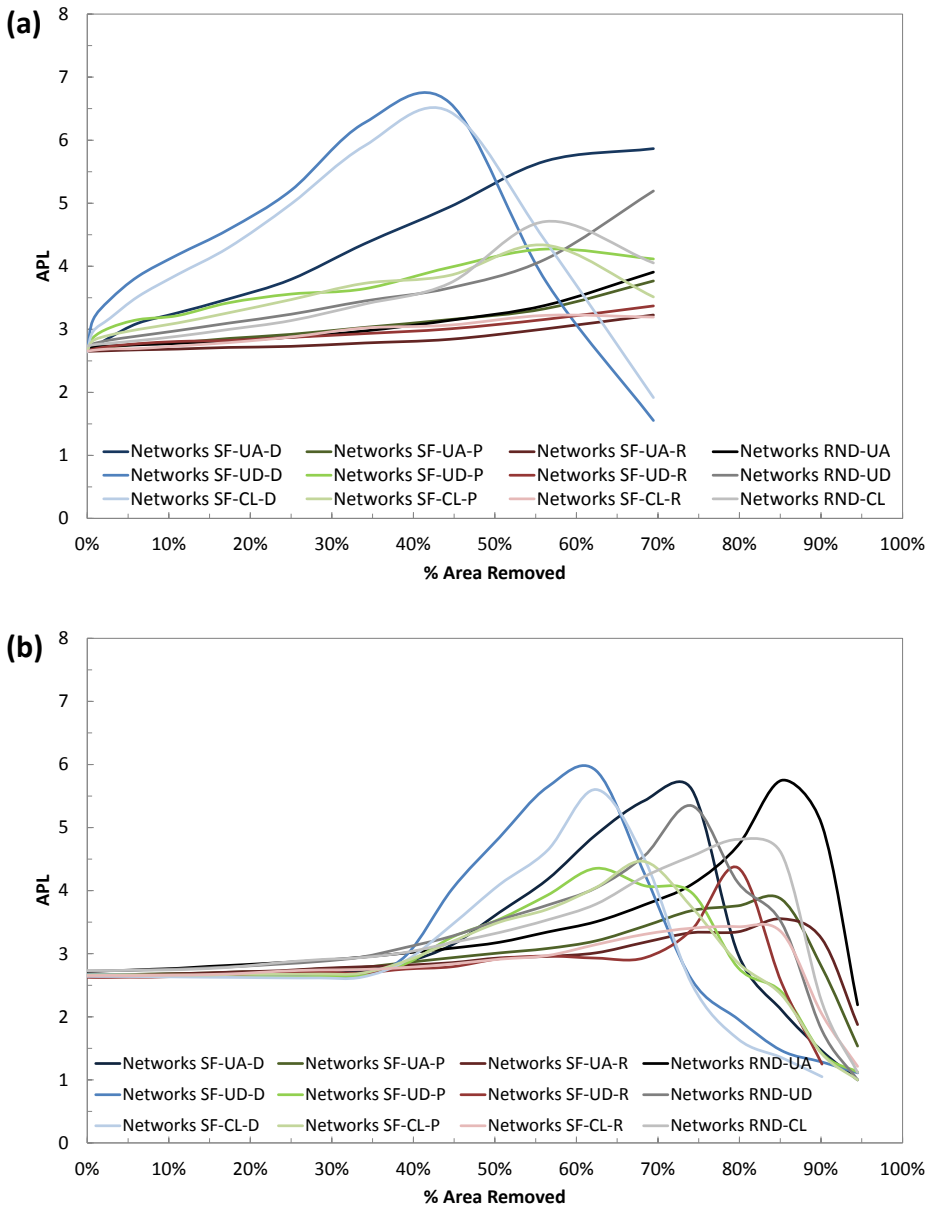


Figure 4.30: Showing how the average path length (APL) changes with area removal for scale-free networks subjected to (a) central attack and (b) perimeter attack spatial hazards. Each line of results shown is the average of ten networks. The networks where the nodes are introduced with distance are shown in shades of blue, nodes introduced proportional with distance are shown in shades of green and nodes introduced randomly are shown in shades of red. The average results for the random networks are shown in shades of grey.

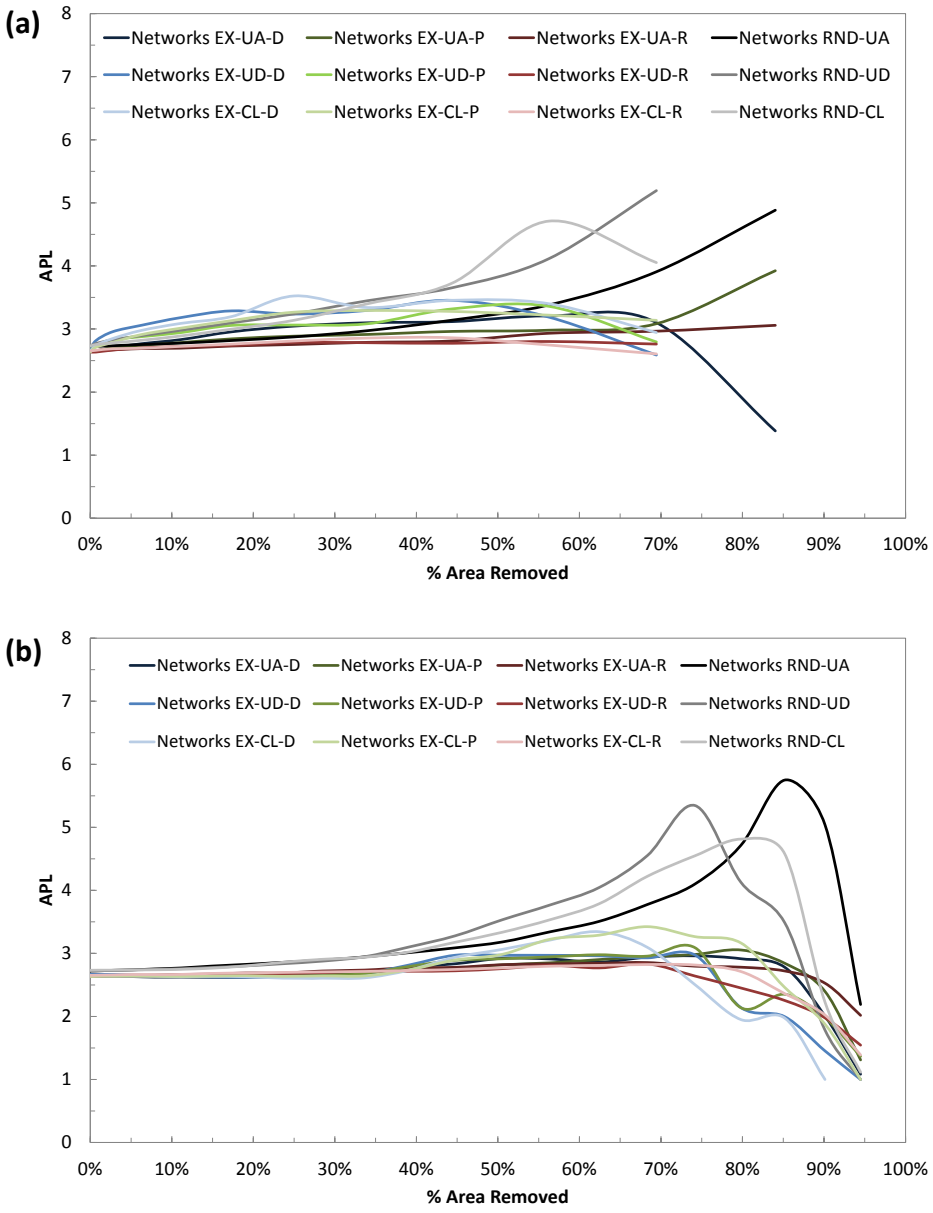


Figure 4.31: Showing how the shortest average path length (APL) changes with area removal for exponential networks subjected to (a) central attack and (b) perimeter attack spatial hazards. Each line of results shown is the average of ten networks. The networks where the nodes are introduced with distance are shown in shades of blue, nodes introduced proportional with distance are shown in shades of green and nodes introduced randomly are shown in shades of red. The average results for the random networks are shown in shades of grey.

The results shown in this sub-chapter are the same as those in the previous sub-chapter, but have been plotted terms of the percentage of area removed rather than the percentage of nodes removed. This gives an indication of how the connectivity and efficiency of the system are affected by the nodal layout.

From these results it can be seen that the nodal configuration and location of high degree nodes can dramatically affect the connectivity and efficiency of a network when subjected to spatial hazard. Locating the majority of components in one area

(uniform with distance nodal configuration) renders the network vulnerable to locations of the spatial hazard over this area and causes a fragmented network (reducing MCS) and also a significant drop in efficiency (increasing APL). Therefore, for networks such as the EATN and CATN (which have formed around an area of high population density) hazards located over the area of high nodal density will not only remove a disproportionate number of links, but will also cause the network to become fragmented and increasingly inefficient. However, this configuration causes these networks show an increased resilience (maintaining both MCS and APL) to spatial hazards located away from this area of high nodal density, which has been shown by the EATN when subjected to the Eyjafjallajökull volcanic event. The EATN maintained connectivity for small sizes of the hazard (until 20% of the network area was removed) and maintained efficiency for all sizes of this hazard (as shown in Figure 3.37). Whereas, spatially dispersing all infrastructure components throughout the network area (uniform with area) creates a network which is the best compromise to all locations of the spatial hazard.

4.7: BEST / WORST CASE COMBINATIONS FOR HAZARD TOLERANCE

This chapter has investigated the hazard tolerance of a range of synthetic networks to different sizes and locations of spatial hazard. All possible combinations of network class (random, scale-free and exponential), nodal layout (uniform with area, uniform with distance and clustered) and node introduction order (random, proportional with distance and with distance) have been considered. This sub-chapter concludes the results in this chapter, initially summarising the main findings for each different network class and then discussing the relevance of these findings for infrastructure systems. The next section of this chapter will then use this data to inform strategies to increase the resilience of the EATN to spatial hazard.

Chapter 4.6 initially analysed the changes in MCS and APL for the random networks, to establish a benchmark for resilience from which to compare the two more sophisticated network classes (scale-free and exponential). Analysis of these random networks showed that they maintained connectivity when subjected to both the central attack and perimeter attack spatial hazards (Figure 4.20(a, b)). However, these

networks also showed a decreasing efficiency with an increase in hazards size (Figure 4.21(a, b)). Through this analysis, it was also shown that the nodal configuration of a random network affects its hazard tolerance. Networks with a uniform with area nodal configuration showed the same response, in terms of both connectivity and efficiency, to both locations of spatial hazard (Figure 4.20(c, d), Figure 4.21(c, d)); whereas, the uniform with distance and clustered nodal configurations showed an increased vulnerability to the central attack spatial hazard (with a decreased efficiency and connectivity) and an increased resilience to small sizes of the perimeter attack spatial hazard. This was attributed to the high concentration of nodes around the geographic centre in these two nodal configurations.

The analysis of the scale-free networks showed that they displayed an increased vulnerability to many sizes and locations of spatial hazard compared to the random networks, with the order in which nodes were introduced to the network significantly affecting their hazard tolerance. For example, networks where the nodes were introduction proportional to distance and randomly showed a lower value of MCS than the random networks for all sizes of the central attack spatial hazard, but it was the networks where nodes were introduced with distance which showed the lowest MCS values and therefore the greatest vulnerability (Figure 4.22(a)). Networks where the nodes were introduced with distance also showed the greatest reduction in MCS for larger sizes of the perimeter attack spatial hazard (after 40% of nodes were removed, Figure 4.22(b)). This decreased connectivity was attributed to the location of high degree nodes within these networks, as previously explained. Networks where the nodes were introduced with distance also showed the greatest decrease in efficiency for all sizes of the central attack spatial hazard, and for larger sizes of the perimeter attack spatial hazard (when more than 40% of nodes were removed, Figure 4.24). Whereas, networks where the nodes were introduced proportional to distance showed a similar efficiency as the random networks and introducing nodes randomly formed a more efficient network. This was attributed to both the location of high degree nodes and the topology of a scale-free network, compared to a random network. Finally, it was shown that, in a similar manner to the random networks, the nodal configuration of scale-free networks affects both their connectivity and efficiency when the results are plotted in terms of the proportion of area removed by

the spatial hazard (Figure 4.28, Figure 4.30). It was again shown that the uniform with distance nodal layout formed the weakest connected and most inefficient network for all sizes of the central attack spatial hazard, due to the large proportion of nodes around the geographic centre of the network (Figure 4.28(a), Figure 4.30(a)). However, this high concentration of nodes also caused this nodal layout to show resilience (a higher MCS and lower APL value) to small sizes of the perimeter attack spatial hazard (until 35% of the area is removed) (Figure 4.28(b), Figure 4.30(b)).

The exponential networks showed a similar change in MCS, as the scale-free networks, for both spatial hazards (Figure 4.23). These networks again showed that the order in which nodes are introduced to a network affects the change in connectivity for an increase in spatial hazard size, due to the location of the high degree nodes. For the central attack spatial hazard, introducing nodes in order of distance (and therefore placing the high degree nodes around the geographic centre) caused a disproportionate impact to the connectivity of the network (Figure 4.23(a)), with this introduction order forming the most weakly connected network. Whereas, introducing nodes randomly formed the most resilient exponential network, as it maintained a higher connectivity; although, these networks were still vulnerable when compared to the random benchmark networks. However, it was shown that the exponential networks were able to maintain efficiency when subjected to both locations of spatial hazard, unlike the scale-free and random networks. This was attributed to the topology of these networks, as a result of the neighbourhood parameter used in the network generation (which enables the decision to attach a link from an introduced node to be based on degree and proximity, rather than degree alone as for scale-free networks). Further analysis of networks generated using different values of this neighbourhood parameter, showed that for small values the efficiency of the networks was similar to that of scale-free networks (as the probability of attachment is more likely to be based on degree alone, forming a topology similar to a scale-free network) and for large values the efficiency was similar to that shown by random networks (as each node has an equal value of probability, therefore inhibiting the formation of high degree nodes) (Figure 4.27). This analysis revealed that there was an 'optimum' value of neighbourhood which resulted in the efficiency of a network being unaffected by spatial hazard. However, it was also shown that this

optimisation compromised the efficiency of the network under normal operational conditions. In a similar manner to both the random and scale-free networks it was also shown that the nodal configuration affects the hazard tolerance of an exponential network. Exponential networks with a uniform with distance nodal configuration showed the greatest vulnerability to the central attack spatial hazard (Figure 4.29(a)), but were the most resilient to small sizes of the perimeter attack spatial hazard (Figure 4.29(b)), due to the high concentration of nodes around the geographic centre as previously discussed.

Whilst, this Chapter has focused on the analysis of synthetic networks, the results have important implications for real world systems. Infrastructure systems which have formed around a more uniform population density (for example, the USATN) are likely to be spatially dispersed and will therefore have a similar resilience to all locations of spatial hazard, as shown by the uniform with area nodal configuration. Infrastructure owners of these systems can therefore estimate the expected damage caused by a spatial hazard based on the hazard size alone (rather than considering both hazard and location). However, infrastructure systems which have formed around a single area of high population density (for example, the EATN and the CATN) are likely to form either a uniform with distance or clustered nodal layout (centred around this area of high density), with the majority of highly connected components also located in this area. This research has shown that these networks are particularly vulnerable to hazards located over this high density area, causing not only a disproportionally large number of connections to be removed (up to 22% points more links removed, when 20% of the area is removed, than a uniform with area nodal layout), but also a disproportionate drop in the connectivity of the network and potentially a decrease in the efficiency of the network, depending on its topological characteristics. However, this nodal configuration can also cause these networks to show an increased resilience to hazards located away from this high density area (similar to the effect that a small size of the Eyjafjallajökull volcanic event caused to the EATN, Figure 3.1(d)), with up to 7% fewer connections removed than the uniform with area configuration for a hazard removing 20% of the network area. Therefore, infrastructure owners with systems that have formed around one area of high population density should be aware of both the potential location and size of any spatial hazards in relation to this area. For example,

the EATN has formed around the area of high population density around central Europe rendering it vulnerable to spatial hazard covering this region (e.g. winter storms, volcanic ash clouds). For these systems, if the majority of known spatial hazards are likely to affect this area of high density, infrastructure owners are advised to relocate a number of their system components (particularly highly connected components) away from this area of high density, to reduce the vulnerability (and increase connectivity and efficiency) of the network under hazard scenario. However, this may not be possible for all infrastructure systems, due to the economic cost involved and the demand for this infrastructure within the area of high population density. For these systems, the infrastructure owners are advised to have a robust adaptation strategy which can be used in the event of spatial hazard to minimise disruption.

It can be concluded that infrastructure owners should take note of the spatial location of both their components and highly connected components when determining the hazard tolerance of their system(s). However, this should not be considered in isolation. This chapter has shown that both scale-free and exponential networks can have the same hazard tolerance as benchmark random networks, but that this is dependent on the spatial configuration of the network. However, the topological resilience of these networks must not be forgotten; in this case the scale-free and exponential networks are vulnerable to targeted attacks. Therefore, to fully assess the hazard tolerance of their system infrastructure owners need to be aware of the consequences of both the spatial distribution and network class of their system.

4.8: HOW CAN THE RESILIENCE OF EXISTING REAL WORLD INFRASTRUCTURE SYSTEMS BE IMPROVED?

In this sub-chapter two strategies to increase the resilience of the EATN are developed, applied and finally tested to determine their ability to reduce the vulnerability shown by the EATN to the central attack spatial hazard (Figure 3.36) (this hazard is used, rather than the perimeter attack, as this hazard was deemed to be the 'worst case' for the EATN). These strategies are both informed by the resilience shown by the random network class, spatial dispersion of high degree nodes (i.e. the random node

introduction order) and the spatial dispersion of nodes (i.e. the uniform with area nodal layout) in the previous sub-chapters.

Two strategies to increase the resilience of the EATN have been formed by considering the conclusions from the previous data gathered from the synthetic networks. The first strategy can be considered to be 'adaptive' as it dictates how the EATN responds to a spatial hazard, by allowing air routes to reroute to other airports if one of their connected airports is enveloped by the hazard. Whilst the second strategy is 'permanent' and re-generates the EATN using the network generation algorithm (developed in Chapter 3) but sets a limit for the maximum number of connections that a node can have (to limit the size of the hub airports). It is worth noting that in both of these strategies it is the connectivity of the network that is of interest and not the capacity of the network (i.e. the ability to move around the network, not the capacity of each air route).

To ensure that these strategies are realistic and could be used as a basis for informing more sophisticated methods (which account for social and economic elements) to increase the resilience of the EATN several assumptions have been made. It is assumed that the location of airports cannot be altered and that existing airports cannot be removed, nor additional airports introduced. Similarly, it is assumed that links cannot be added to the network (creating a homogenous network where every airport is connected to every other airport would no doubt create the most resilient network, but conversely would also be the most economically unviable). In the ‘adaptive’ strategy it is assumed that under normal operational conditions the EATN is optimally configured to maximise social and economic benefits. It is also assumed that the capacity of airports can change, particularly at short notice in the event of a hazard scenario (e.g. as air routes become diverted, potentially whilst the aircraft is in flight) and that each airport has infinite capacity and can cope with added air traffic of a rerouted air route.

4.8.1: 'ADAPTIVE' STRATEGY FOR IMPROVING RESILIENCE

The first strategy aims to increase the resilience of the EATN by 'adapting' the network to a spatial hazard. In this strategy, air routes are 'rewired' from airports that are located in the hazard to the closet operational airport (i.e. the closest airport outside the hazard).

To determine the improvement that this 'adaptive' strategy has to the EATN, the central attack spatial hazard is used and 10 airports at a time are removed as the hazard grows. The network is analysed after the removal of 10 airports, rather than removing airports individually, to reduce the computational effort of the analysis. If an air route is connected to two airports that are both enclosed in the spatial hazard, then the air route has failed and it is assumed that it is a short overland distance between these two airports and that is now the quickest mode of travel between the two. However, if an air route is connected to one airport inside the boundary of the spatial hazard and one outside the hazard, then the air route is 'redirected' to the closest airport located outside the spatial hazard; provided that these two airports are not already connected.

Using this method, two simulations are undertaken; one includes parallel edges (where two, or more, links connect the same two nodes) and the other removes parallel air routes. In this thesis, weighted networks and parallel edges are outside the scope; however, they are used in this instance purely to show the increase in expected air traffic at airports outside the influence of the spatial hazard. Figure 4.32(a, b) shows the adaptive rewiring strategy when parallel edges have been removed from the network and Figure 4.32(c, d) shows the strategy when these parallel edges have been retained.

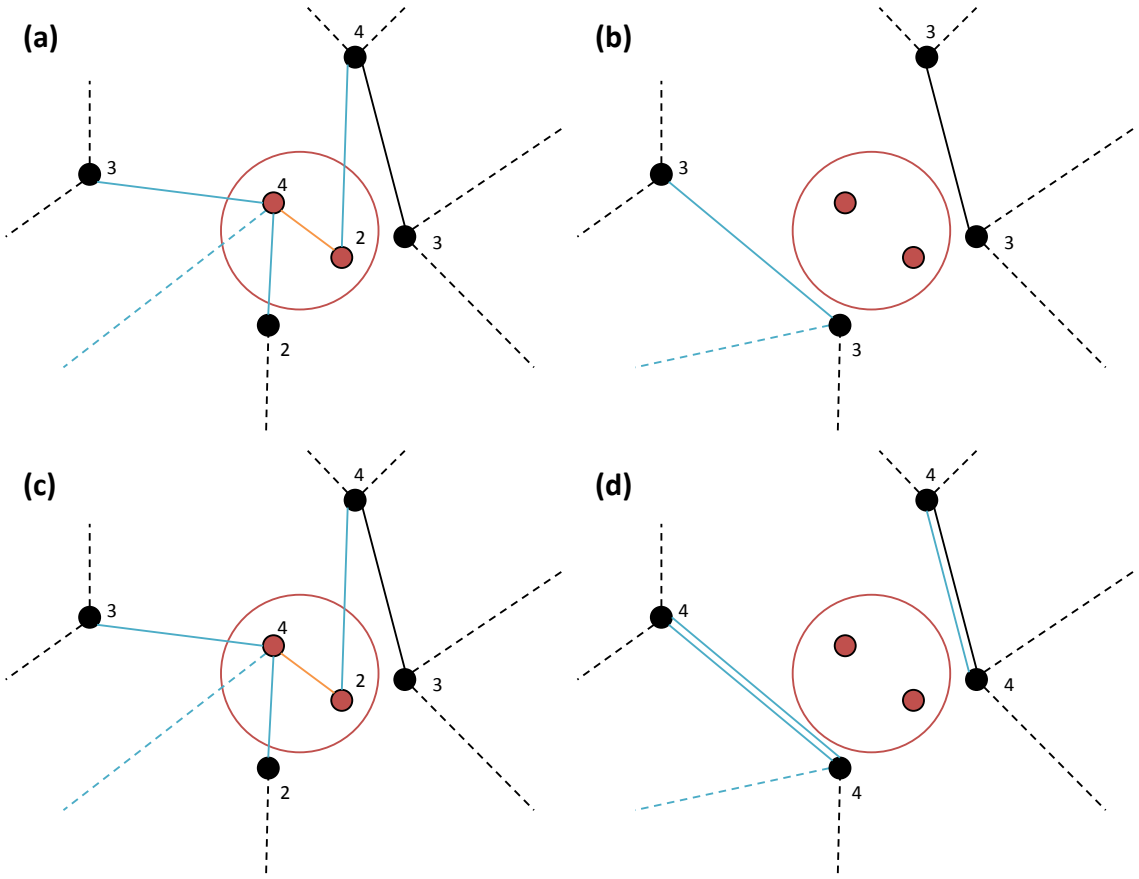


Figure 4.32: Showing the strategy used to rewire links (air routes) in the event of a spatial hazard. In all parts of the figure a section of the EATN is shown and the nodes are indicated by dots and the links by the connecting lines (solid lines indicate a link between two shown nodes and a dotted line between two nodes where one has been omitted for clarity). In (a) it can be seen that two airports (red dots) have been enveloped by a spatial hazard (red circle). The orange air route is failed (as both origin and destination airports are enveloped by the spatial hazard) and the blue air routes are 'rewired' to the closest airport and any parallel edges are removed, the result of this can be seen in (b). The same starting network is shown in (c) and is rewired in (d) using the same 'rules', but in this case parallel edges are allowed to form.

The results for this strategy have been shown in Figure 4.33, for both the networks where the parallel edges have been included / removed. In this figure, the results have also been compared to that of the original EATN and two random networks, one with the same nodal locations as the EATN and the other with random nodal locations. It can be seen that by 'rewiring' the air routes around the spatial hazard that the resilience of the network increases by 30% points when the parallel air routes are removed and by 45% points when the parallel air routes are included, for the removal of 20% of the airports, compared to the EATN with no rewiring strategy. Adaptively 'rewiring' the air routes also increases the resilience of the EATN when compared to the random network (with random nodal locations) and indeed makes the network resilient when compared to the random network. The adaptively rewired network that removes parallel edges is 8% points more resilient than the random network and

increases to 26% points more resilient when parallel edges are included, for a hazard that closes 20% of the airports.

Plotting the results in terms of the proportion of closed area shows that only the rewired EATN where the parallel edges have been included is resilient when compared to the random network with random nodal locations. Although, the resilience of the rewired EATN with removed parallel edges does increase by 12% points compared to the EATN with no rewiring, it is still 41% points more vulnerable than the random network for a hazard size covering 20% of the network area. This is due to the location of a large proportion of airports around the geographic centre of the network (Figure 3.7). These airports are removed by the spatial hazard and their air routes can only be rewired if they do not form a parallel edge. From this graph, it can also be seen that the rewired EATN where the parallel edges are not removed shows a significantly increased resilience until around 80% of the network area is removed. This is due to the failure of fewer air routes as a result of the inclusion of these parallel edges. Using this method, air routes are only failed when they connect to airports within the expanding spatial hazard.

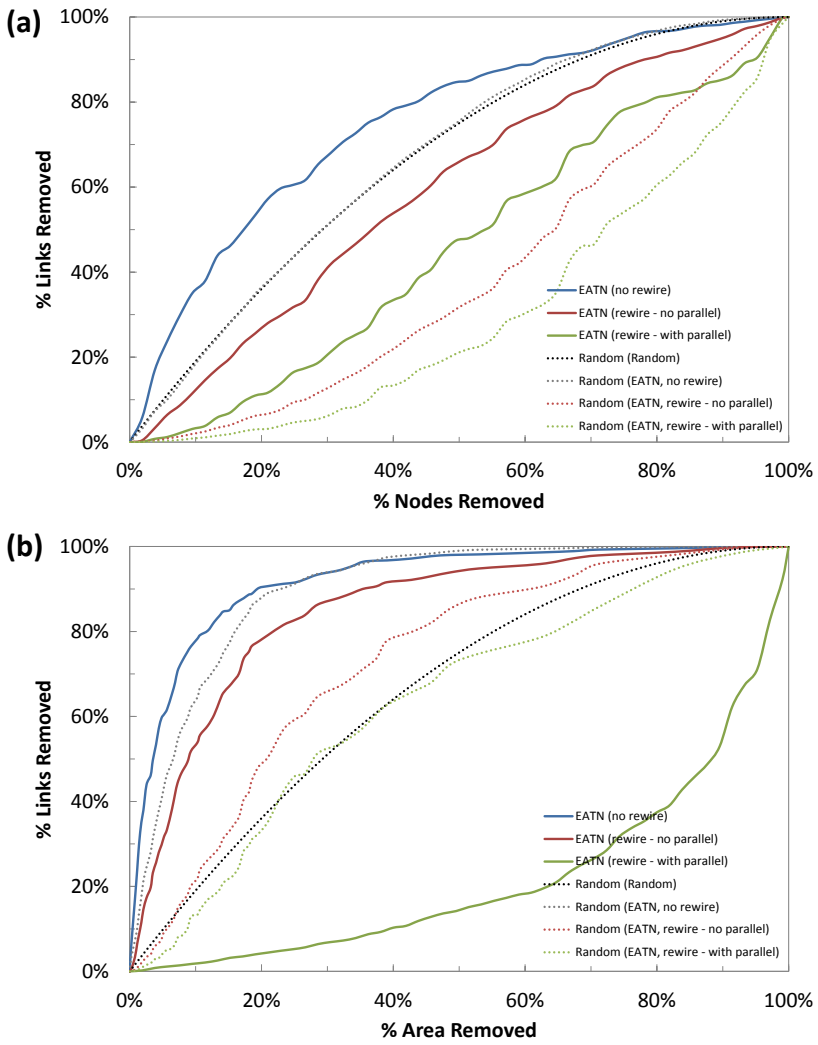


Figure 4.33: The results of the 'adaptive' rewiring strategy for the EATN subjected to the central attack spatial hazard. The hazard tolerance of the EATN with no rewiring (where links are removed if one (or both) of their connecting airports are enveloped by the hazard) (blue line) is compared to the EATN when the links have been rewired and parallel edges removed (red line) and not removed (green line). The random benchmark network, with random nodal locations, and three random networks with the same nodal configuration as the EATN have also been shown (dotted lines).

The random network, with the same nodal locations as the EATN, has also been rewired to form a benchmark for comparison with the EATN. It can be seen from Figure 4.33(a) that the rewiring improves the resilience of the random networks (compared to those that have not been rewired) when the results are plotted in terms of the proportion of nodes removed; however, plotting the results for the proportion of closed area shows that the rewired random networks, with the same nodal layout as the EATN, are still not as resilient as the random network, with random nodal locations, that has not been rewired (Figure 4.33(b)). From these results, it can therefore be concluded, that the airport locations play a significant role in the vulnerability shown by the EATN to spatial hazards located close to the geographic centre of the network.

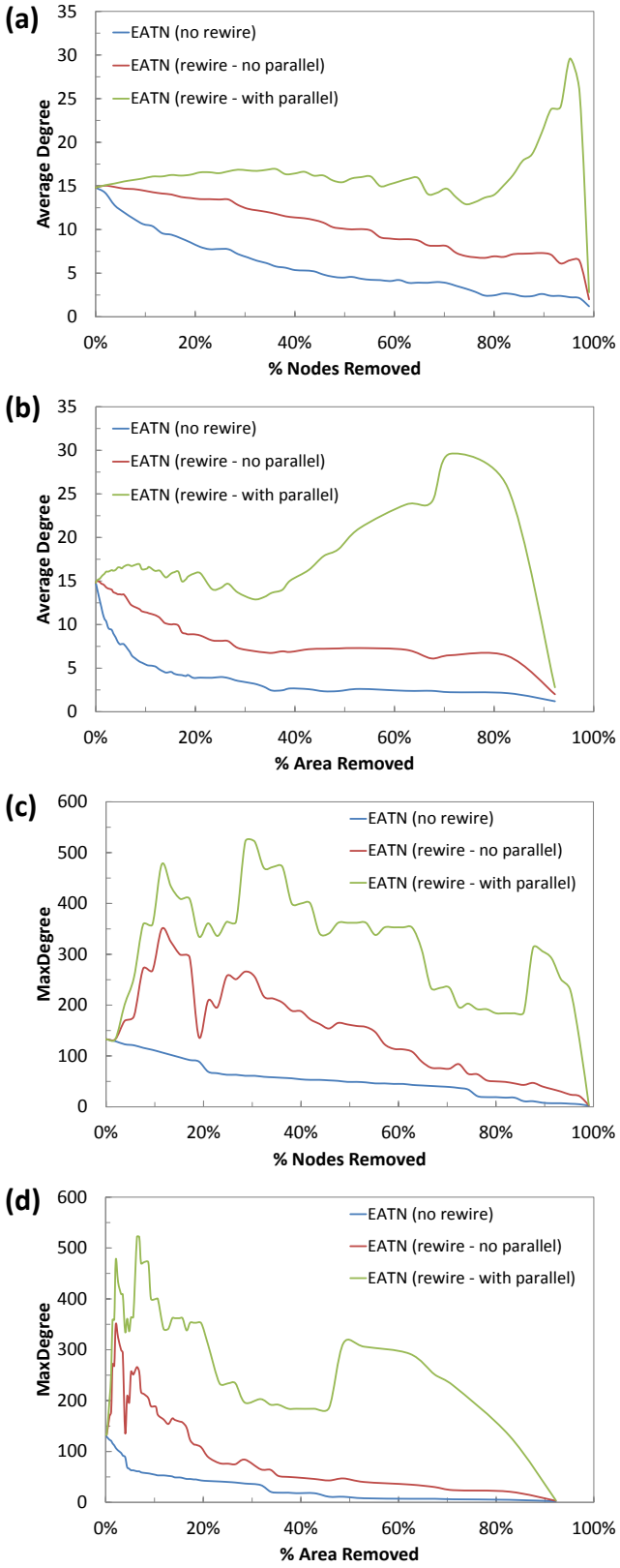


Figure 4.34: Observing the changes in (a, b) average degree of the remaining nodes for the EATN and two adaptively rewired networks (one with parallel edges, one without) and (c, d) maximum degree for the same three networks. The results in (a, c) have been plotted with respect to the proportion of nodes removed and in (b, d) with respect to the proportion of area removed.

To observe the changes that the rewiring strategy has to the degree of the airports, the maximum and average degree (recalculated after the removal of 10 airports) are plotted against the proportion of nodes and area removed by the spatial hazard (Figure 4.34). For the 'adaptive' strategy where parallel edges are removed the average degree of airports slowly decreases, but not as quickly as the EATN where this strategy is not implemented (Figure 4.34(a, b)); however, when the parallel edges remain in the network the average degree of airports increases and reaches a peak of 29.60 (compared to the original average of 14.80) when around 95% of airports or 70% of airspace is closed. This is due to the presence of only a few airports which are all interconnected by multiple air routes.

Considering the maximum degree of the same three networks, it can be seen that for both of the rewired networks the maximum degree increases dramatically with only a small proportion of the airspace closed (Figure 4.34(c, d)). The maximum degree airport has a degree of 133 in the EATN (with no airports removed) and increases to 350 when the 'adaptation' strategy which removes parallel edges is implemented and to 522 when parallel edges remain in the network. Therefore, for small spatial hazards, these high degree airports will experience a significant increase in the number of expected aircraft and passengers. It was assumed that all airports have infinite capacity and can therefore cope with any increase in aircraft and passengers; however, it is likely that for an actual air traffic network (where the capacity of the airports is restricted) that some of these air routes may need to divert to another nearby airport.

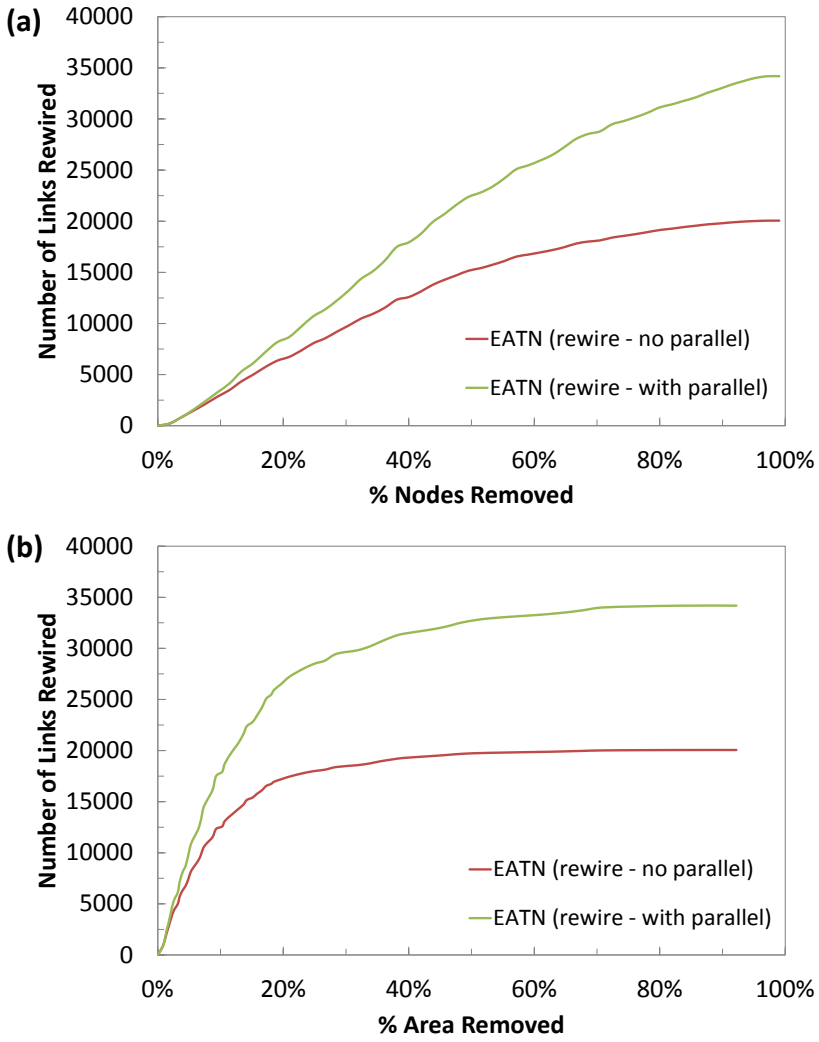


Figure 4.35: Observing the changes in the number of links rewired in the EATN for the rewired networks with parallel edges (green line) and without parallel edges removed (red line). The results in (a) are plotted with respect to the proportion of nodes removed and in (b) with respect to the proportion of area removed.

The number of air routes rewired in the 'adaptation' strategy for both the inclusion and exclusion of parallel edges is shown in Figure 4.35. In this figure, it can be seen that the number of rewired air routes gradually increases when plotted in terms of the proportion of airports closed and fairly sharply when plotted in terms of the proportion of airspace closed. The network where the parallel edges have not been removed (green) shows that a higher number of air routes have been rewired (a total of 20,057) compared to the network where these multiple edges have been removed (red) (a total of 34,178), this is due to the increase in the number of air routes in this network. Therefore, it can be seen that small sizes of spatial hazard, the size of the hazard has a disproportionate effect to the number 'displaced' passengers (until 20% of the network area is removed).

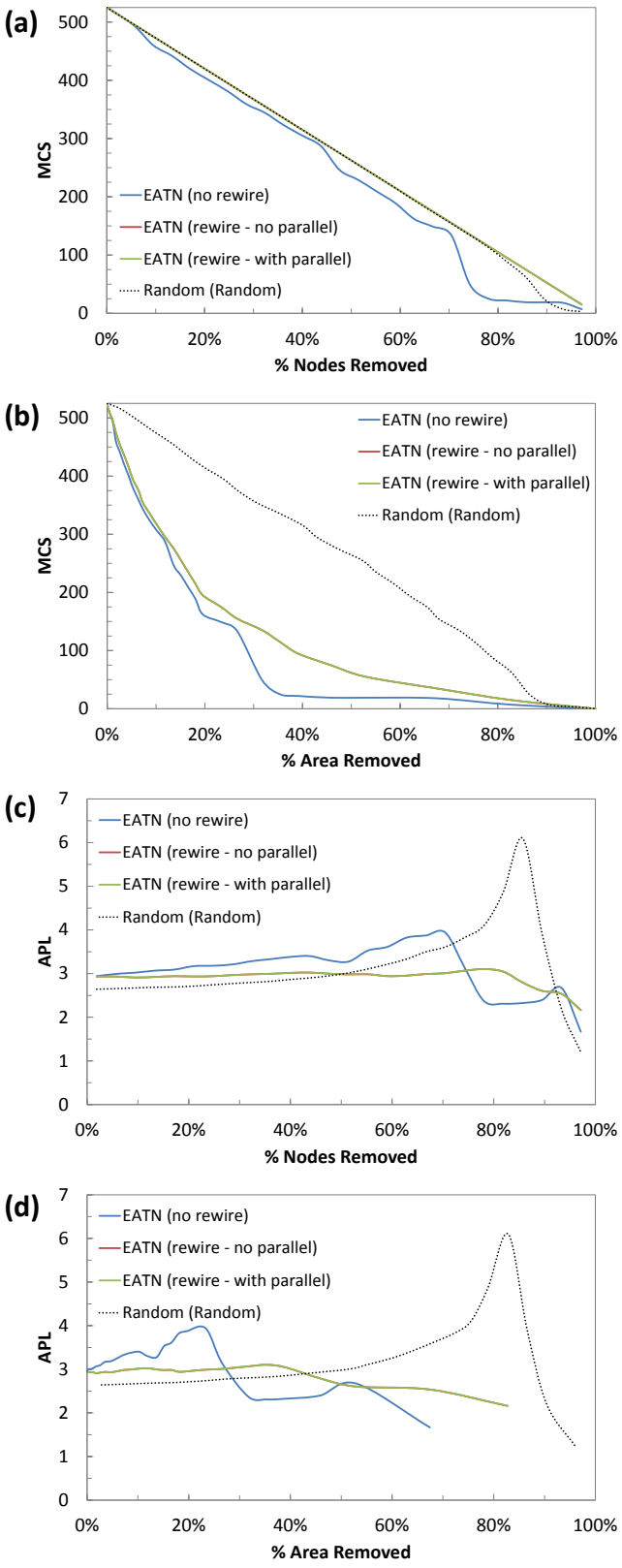


Figure 4.36: Showing the changes in (a, b) maximum cluster size and (c, d) average path length for the EATN, two rewired networks and a random network subjected to the central attack spatial hazard. The results in (a, c) are plotted with respect to the proportion of nodes removed and in (b, d) with respect to the network area removed by the spatial hazard. It appears that the results for the rewired EATN with no parallel edges (red line) is missing from this figure, however, it has the same results as the rewired EATN with parallel edges (green) and appears under this line.

The MCS and APL of these networks have also been calculated, and compared to the MCS and APL of the EATN without rewiring and to the random benchmark network (shown in Figure 4.36). Considering the results of the MCS, the rewired networks show a slight increased resilience compared to the EATN with no rewiring, but still do not show the same resilience as the random network, with random nodal locations (Figure 4.36(a, b)). Therefore, it can be concluded that although there are more air routes in the network, these do not connect the remaining airports in one coherent cluster and travel between some parts of the network still needs to be achieved using other forms of transportation. The APL for the same networks shows that travel around the 'rewired' networks is easier than for the EATN when there is no rewiring (as there is a lower value of APL) (Figure 4.36(c, d)); peaking at a value of 3.10 compared to the EATN at 3.94. These networks also show a smaller APL value than the random networks (which peak at an APL value of 6.10).

4.8.2: 'PERMANENT' STRATEGY FOR IMPROVING RESILIENCE

The second strategy implemented to increase the resilience of the EATN focuses on the permanent rewiring of the network and in so doing proposes a 'trade off' or compromise between the optimised social and economic factors (assumed in the actual EATN) and the resilience of the network. In this strategy the EATN is generated using the algorithm previously developed (in Chapter 3) and also uses the same node introduction order as in Figure 3.8(g, h) (i.e. the 'best fit' for the EATN using actual nodal locations). However, in this generation the maximum degree of an airport is limited and a range of networks are generated with different values of maximum degree, to gauge the impact on resilience. The degree of a node is limited in the algorithm by setting the probability of attachment to zero for a node when it reaches the maximum permitted degree, thereby eliminating the possibility that links introduced from new nodes will connect to this existing node. This strategy has been informed by the resilience shown in random networks, which do not include high degree nodes, and so in preventing the formation of these hub airports it is argued that the network should show more resilience (as these nodes will have a lesser impact when removed).

The degree distribution and spatial degree distribution for four generated networks where the maximum degree has been limited are shown in Figure 4.37. From these distributions it can be seen that limiting the size of the highest degree node does not cause a noticeable effect to the shape of the degree distribution (Figure 4.37(a)) or to the spatial degree distribution (Figure 4.37(b)), until the maximum degree is limited to 20. Limiting the maximum degree by this amount results in all nodes having an approximately equal degree (similar to a random network) and therefore causes the proportion of links around the geographic centre of the network to reduce (as this is where the majority of high degree nodes in the EATN are located).

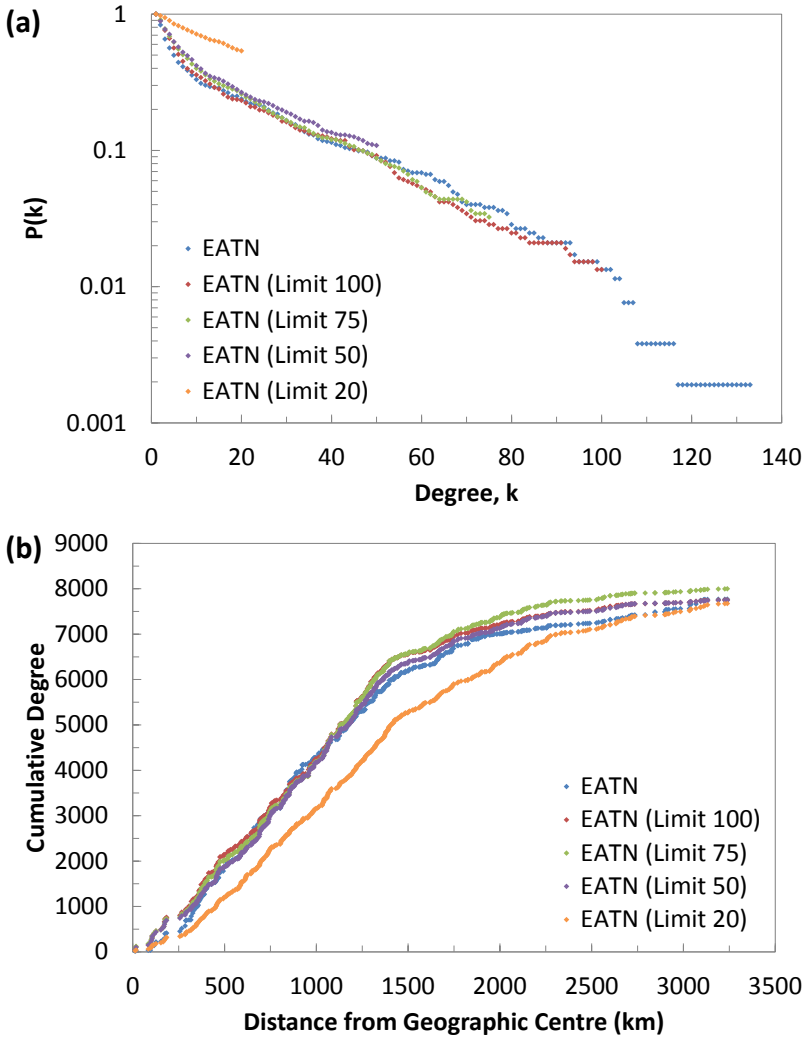


Figure 4.37: The (a) degree distribution and (b) spatial degree distribution for the EATN and four networks generated using the same algorithm as the EATN but with a limited maximum degree (of either: 100, 75, 50 or 20 connections).

The networks generated, with different values of maximum degree, are again subjected to the central attack spatial hazard where 10 nodes are removed at a time.

Unlike the previous strategy, no rewiring takes place as airports are enveloped by the spatial hazard. The results for this analysis are compared to those for the EATN and random networks (with random node locations and those that are the same as the EATN) and are plotted in terms of the proportion of air routes, airspace and airports closed (Figure 4.38).

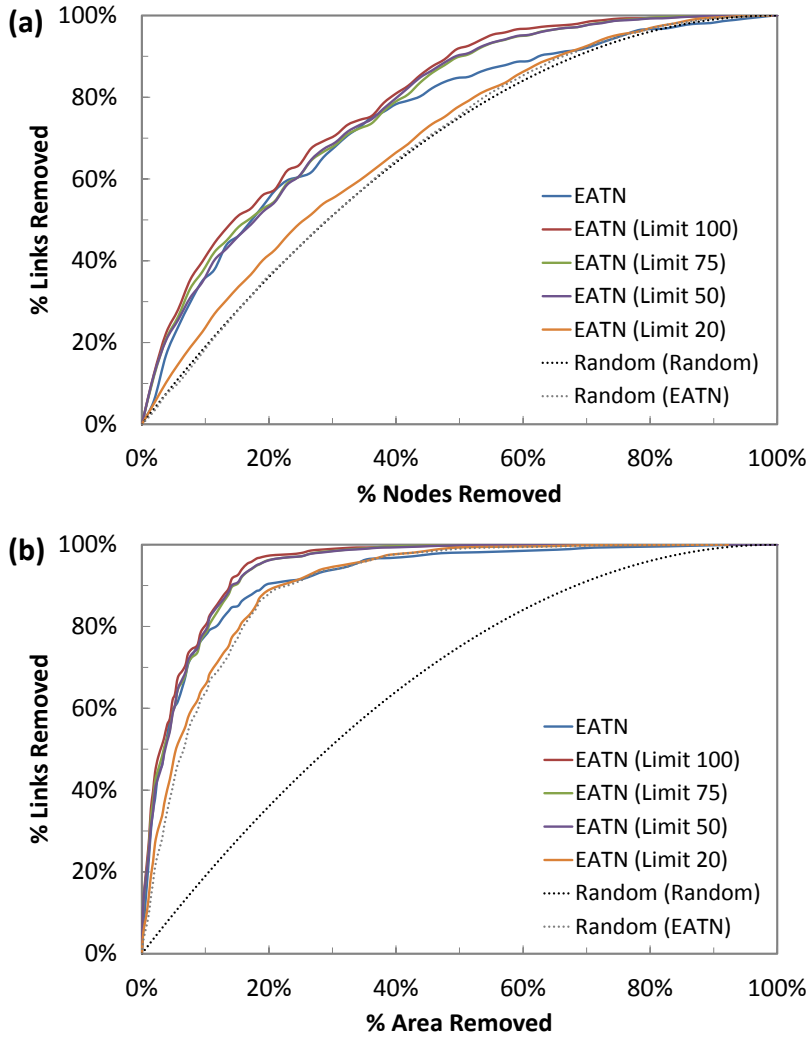


Figure 4.38: Showing (a) the relationship between the proportion of nodes and links removed for the EATN and four networks, subjected to the central attack spatial hazard, where the maximum permitted degree does not exceed 100, 75, 50 or 20. (b) Plotting the same results, but with respect to the proportion of area covered by the spatial hazard. Also showing the results of the benchmark random network, with random nodal locations, and the random network with the same nodal configuration as the EATN (dotted lines).

These results show that the size of the maximum degree airport must be severely limited to show a significant increase in the resilience of the EATN (with a maximum degree of 20 rather than 133), when considering resilience in terms of the proportion of closed air routes and airports. For example, when 20% of airports are removed there are 58% of links removed for the EATN, this only reduces by 6% points when the

hub size is limited to 75, but reduces by 17% points when the hub size is limited to 20. However, even limiting the maximum degree airport to 20 does not cause the EATN to be as, or more, resilient than the random network (it is still 6% points more vulnerable when 20% of nodes are removed). This is due to the more structured connectivity of the EATN compared to the random network. The method used to assign links from new nodes to existing nodes in these limited degree networks is the same as that used to generate the EATN (outlined in Chapter 3) and as such incorporates the element of preferential attachment. Therefore new airports still want to connect to existing airports with a high probability of attachment (either the high degree airports or those located within a close proximity) and will only attach to a lower probability airport if the desired airport has reached the maximum permitted degree. This still creates clusters of higher degree nodes close to the geographic centre of the network (where the majority of nodes are located). Figure 4.39(a, b) plots the degree of each node in the 50 and 100 limited degree networks respectively and Figure 4.39(c, d) highlights the location of the nodes that have the maximum allowed degree (red dots). In this figure, it can be seen visually that the maximum degree nodes tend to form a cluster around the geographic centre of the network. Therefore, for a small spatial hazard located over the geographic centre of the network, a large proportion of links are still removed, even though the maximum degree node is lower than that of the EATN (unless the maximum degree is severely limited). However, plotting the results in terms of the proportion of closed air routes and air space does not show a significant change in resilience for all limited hub networks compared to the actual EATN, even for the network where the hub size is limited to 20. This can be contributed to both the positioning of the airports and also to the network generation algorithm, as previously discussed.

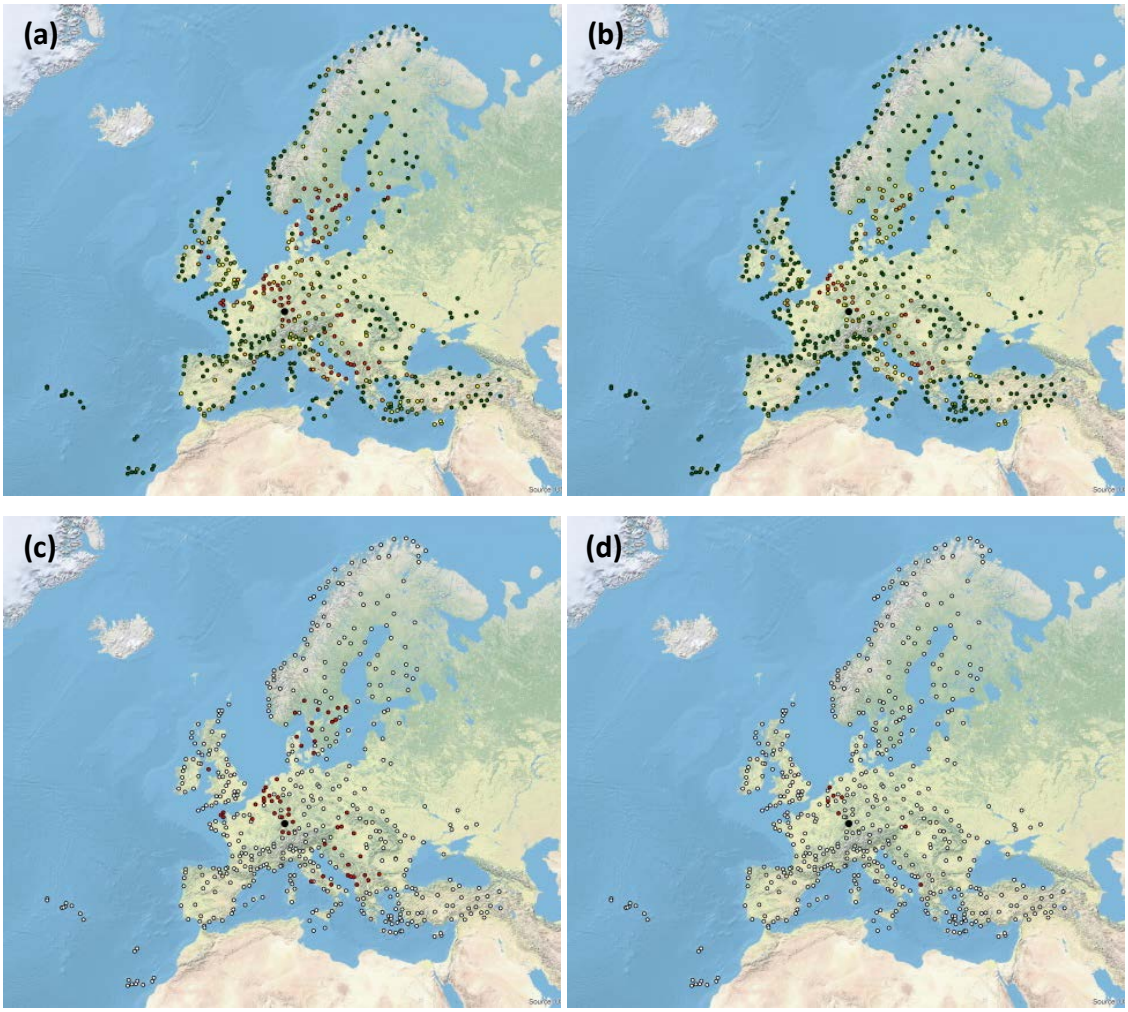
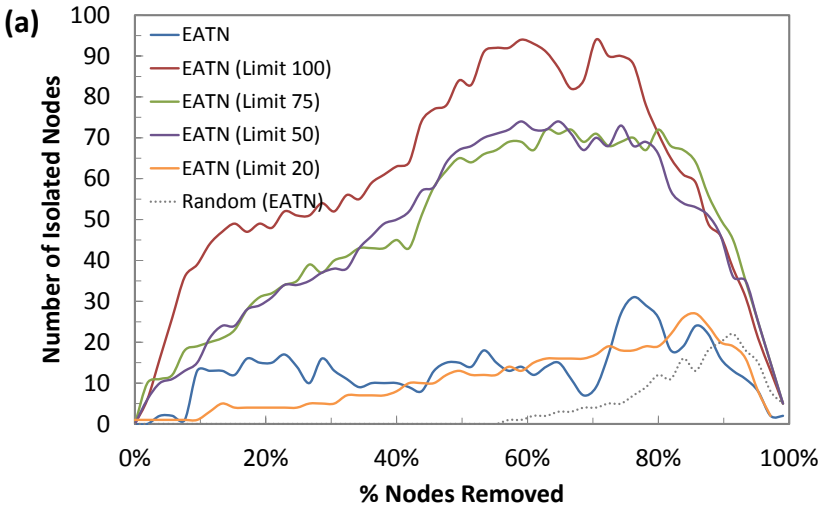
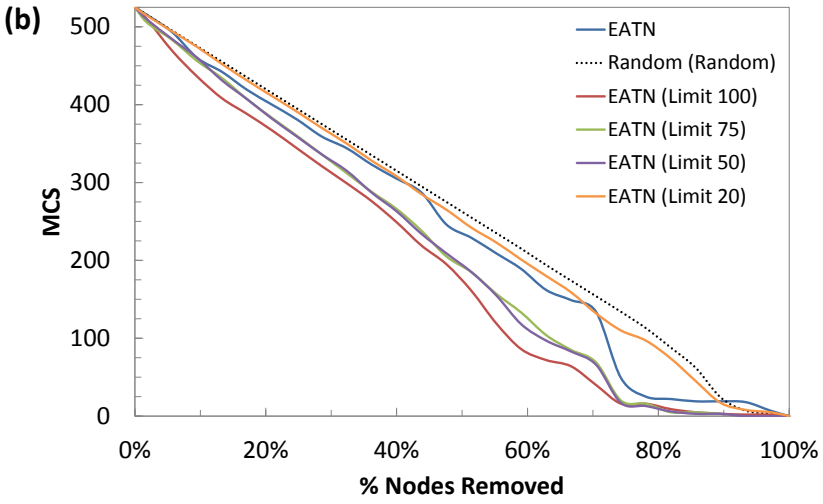
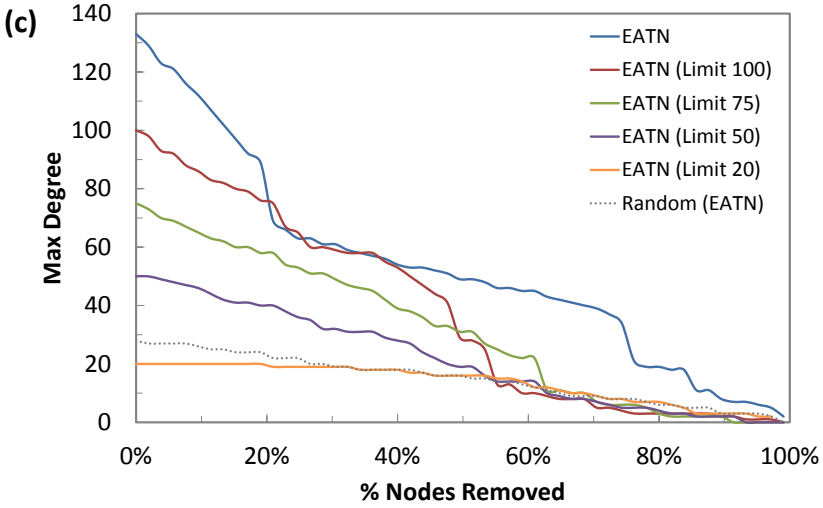


Figure 4.39: Generated GIS images showing the degree of all nodes in the generated networks with a limit of (a) 50 and (b) 100, on a red (high degree) to green (low degree) scale. The location of the nodes with the maximum value of degree (red dots) is also shown for a limit of (c) 50 and (d) 100.


(a)
Number of Isolated Nodes
100
90
80
70
60
50
40
30
20
10
0
EATN
EATN (Limit 100)
EATN (Limit 75)
EATN (Limit 50)
EATN (Limit 20)
Random (EATN)
0%
20%
40%
60%
80%
100%
% Nodes Removed


(b)
MCS
500
400
300
200
100
0
EATN
Random (Random)
EATN (Limit 100)
EATN (Limit 75)
EATN (Limit 50)
EATN (Limit 20)
0%
20%
40%
60%
80%
100%
% Nodes Removed


(c)
Max Degree
140
120
100
80
60
40
20
0
EATN
EATN (Limit 100)
EATN (Limit 75)
EATN (Limit 50)
EATN (Limit 20)
Random (EATN)
0%
20%
40%
60%
80%
100%
% Nodes Removed

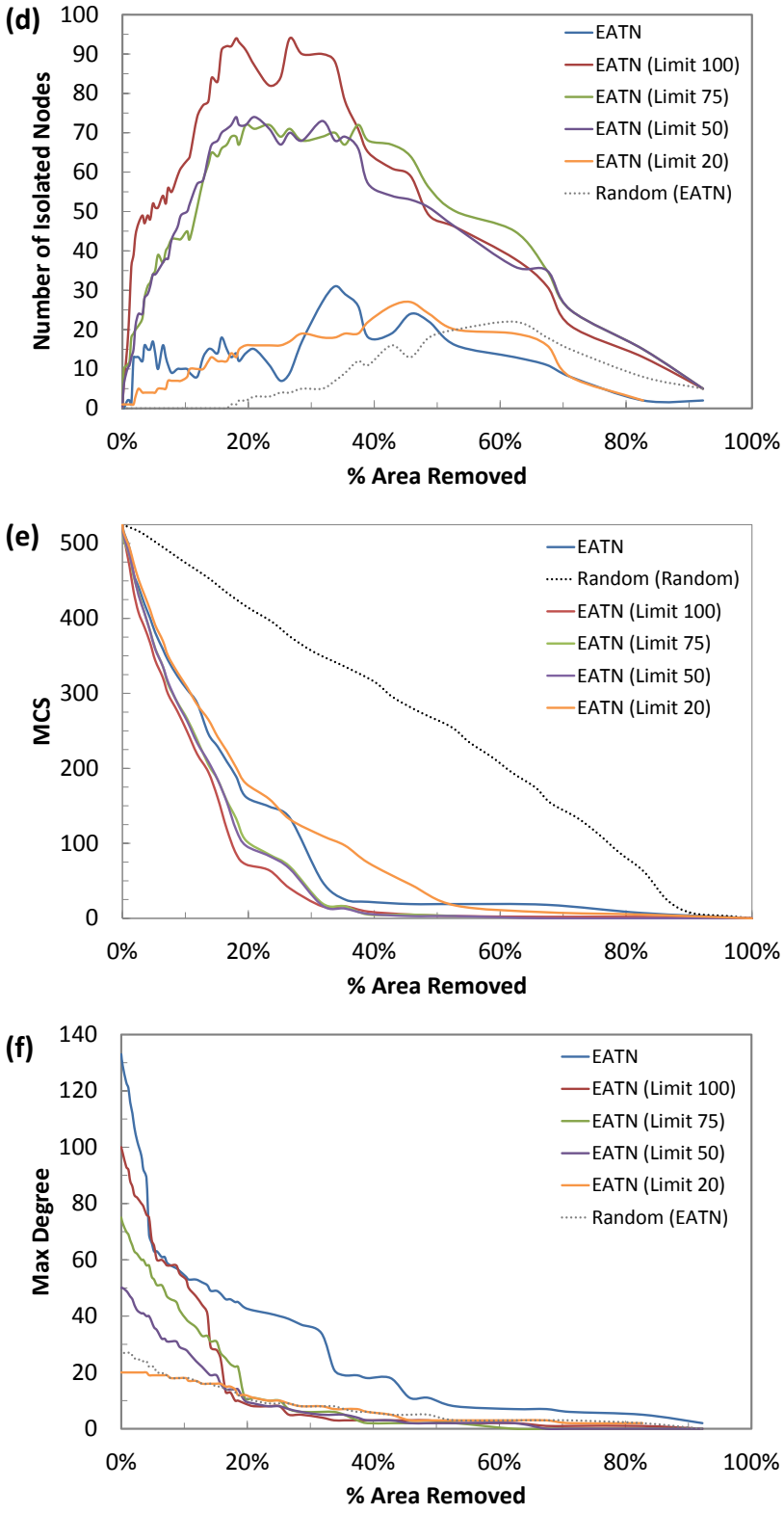


Figure 4.40: Showing the changes in (a, d) the number of isolated nodes, (b, e) the maximum cluster size (MCS) and (c, f) the maximum degree for the EATN and four networks where the maximum degree has been limited, when the networks are subject to the central attack spatial hazard. Also showing the results of the benchmark random network, with random nodal locations (dotted lines).

The number of isolated airports, MCS and the maximum degree node have been plotted, both in terms of the proportion of nodes and area removed by the spatial hazard in Figure 4.40. The number of isolated airports is used in this analysis to show the differences between the degradation of the networks, generated with different maximum degree nodes, when subjected to spatial hazard. From Figure 4.40(a, d) it can be seen that the number of isolated nodes sharply increases when the hub size is limited to 100, 75 or 50 (with the MCS reducing at a quicker rate than the EATN for the same networks, Figure 4.40(b, e)). The number of isolated nodes reaches a maximum of 31 for the EATN, 94 for a hub size of 100, 72 for a hub size of 75 and 74 for a hub size of 50. This is due to the connectivity of the networks and the location of the maximum degree nodes (as shown in Figure 4.39). Figure 4.41 plots the location of the isolated nodes (and the remaining connected nodes) for the hazard size which causes the maximum number of isolated nodes. In this figure, it can be seen that the isolated nodes tend to occur around the perimeter of the network. These nodes are those with a low degree (Figure 4.39(a, b)) and tend to be connected to the nodes in the centre of the network; therefore, removing the nodes in the centre of the network causes these nodes to become disconnected from the network and causes the high number of isolated nodes and consequently a reduced MCS. This high number of isolated nodes, and reduction in MCS, is not apparent in the EATN, or the network with a limited degree of 20, due to the increased connectivity of these outer nodes to other nearby nodes (as a result of the network generation algorithm and the severely limited maximum permitted degree).

The maximum degree of these networks has been shown in terms of the actual values, rather than the percentage changes, to enable any sharp decreases in degree to be easily identified (Figure 4.38(c, d)). These results show that the networks where the maximum degree has been limited all decrease at a relatively uniform rate; until around 50% of the airports or 15% of the network area is removed by the spatial hazard and then the maximum degree sharply decrease with any additional airports removed. This is due to the large number of airports with the maximum value of degree. In the actual EATN there is only one airport with the highest value of degree (133), however limiting the size of the highest degree airport causes more than one airport to have this value. For example, limiting the degree to 50 causes 57 airports to

have this value of degree and limiting the maximum degree to 20 causes this number to rise to 282.

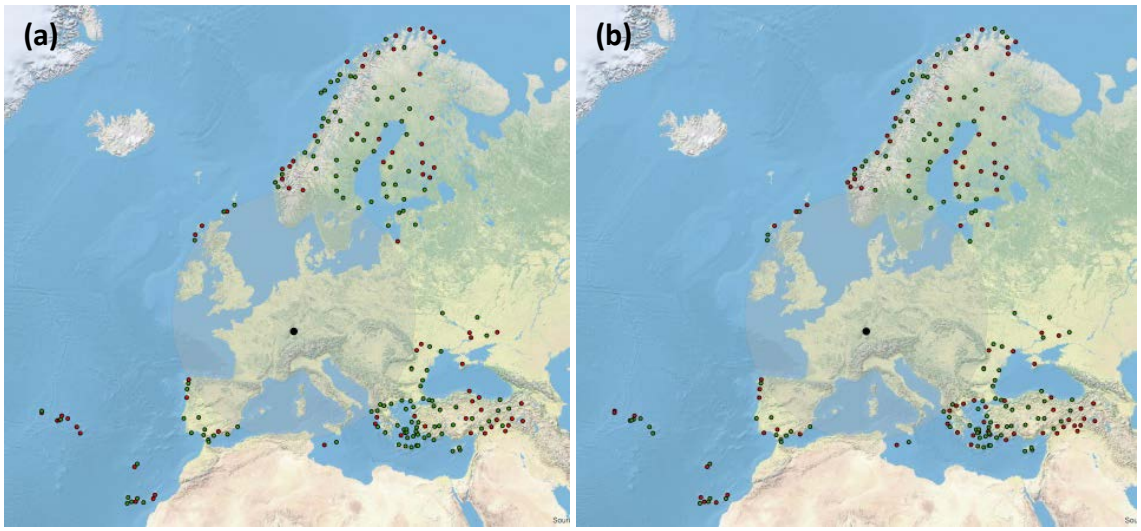


Figure 4.41: Generated GIS images showing the location of the isolated nodes (red) and the connected airports (green) for the size of spatial hazard which results in the maximum value of isolated nodes, for the network with a maximum degree of (a) 50 and (b) 100.

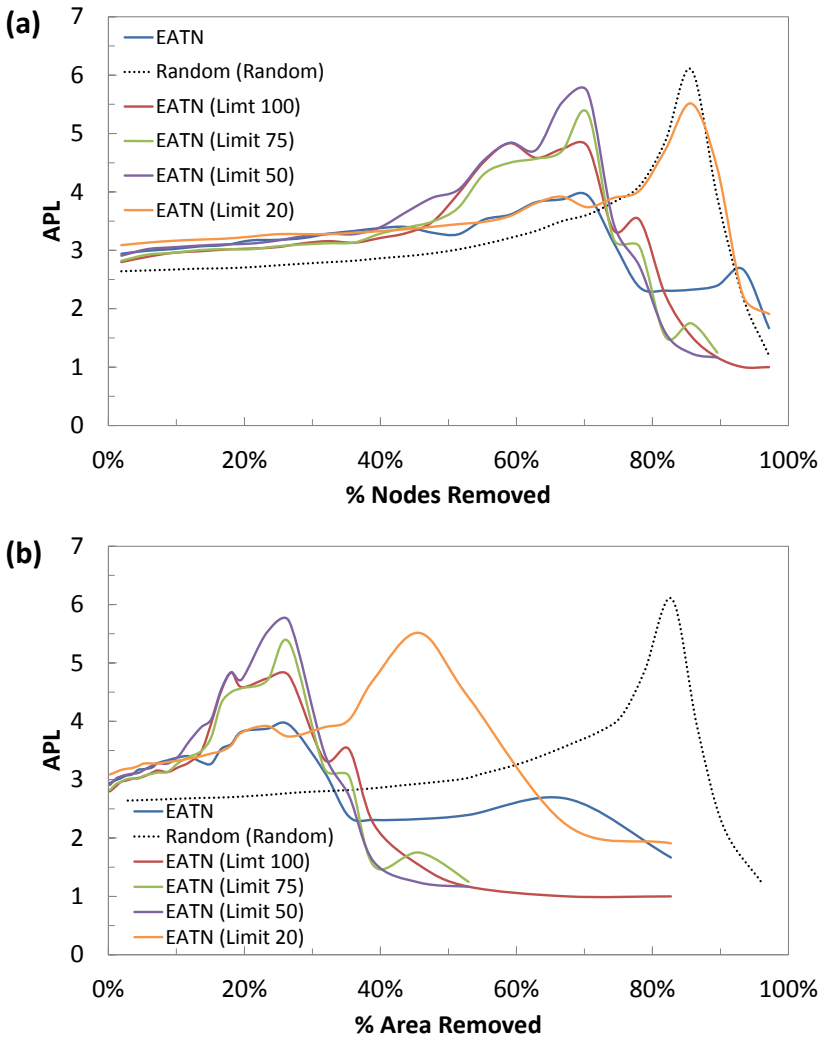


Figure 4.42: Showing the change average path length (APL) for the EATN and four networks where the maximum degree has been limited (as indicated), subjected to the central attack spatial hazard. The results in (a) have been plotted with respect to the proportion of nodes removed from the network and with respect to the size of the spatial hazard in (b). Also showing the results of the benchmark random network, with random nodal locations (dotted lines).

The APL for these networks have also been calculated at increments of 10 airports removed and are presented in Figure 4.42, in terms of both the proportion of airports and air routes closed. From this figure it can be seen that, limiting the size of the hub creates a more inefficient network, when subjected to the central attack spatial hazard. To give an example, the maximum value of APL is 5.71 when the maximum degree is limited to 50, compared to 3.94 for the actual EATN. This is due to the reduction in the size of the hub airport, meaning that it is now likely that information from one weakly connected node will need to be passed between two, or more, hub nodes to travel to another weakly connected node (rather than a single higher degree hub node), thereby increasing the path length between nodal pairs. Severely limiting the size of maximum degree airport to 20 causes the network to behave in a similar manner as

the random benchmark network, due to their similar network topologies, with this network having a maximum APL value of 5.51 compared to 6.10 for the random network. This similarity is not replicated when the results are plotted in terms of the proportion of area removed, due to the differences in nodal layout between the EATN (which contains a high proportion of nodes around the geographic centre of the network) and the uniform with area nodal configuration of the random benchmark network. Therefore, it can be concluded that limiting the size of the hub airports within the EATN causes the resilience to increase slightly compared to that of the actual network in terms of the proportion of air routes and airports closed, but causes a decrease in the efficiency of the network.

4.8.3: MODIFICATION OF 'ADAPTIVE' STRATEGY FOR IMPROVING RESILIENCE

The results in the previous two sub-chapters, for the 'adaptive' and 'permanent' rewiring strategy have shown that by adaptively rewiring the EATN the resilience of the network is significantly increased without compromising the efficiency of the network. Whilst, permanently rewiring the network does not result in a significant increase in the resilience of the EATN, but does result in the reduction of the efficiency of the network. It is therefore, recommended that the EATN is not permanently rewired, but that strategies to increase the resilience of the network through adaptively rewiring in the event of a spatial hazard are developed. Therefore, the initial adaptive strategy is modified to account for the capacity of the airports (removing the assumption that airports have an infinite capacity). This modified strategy will investigate the relationship between the additional airport capacity and the resilience of the network to the central attack spatial hazard and also the perimeter attack spatial hazard. This additional airport capacity is calculated as a percentage of the degree of the airport in the EATN; for example, an additional capacity of 10% would allow an airport with a degree of 10 in the EATN to increase to 11 and a degree of 20 to increase to 22. In this strategy, parallel edges are included in order to give an indication of the additional air traffic at each airport.

The EATN is initially subjected to the central attack spatial hazard, and airports are removed individually from the network as spatial hazard increases in size (rather than

removing 10 airports in the previous two strategies). The EATN is also subjected to the perimeter attack spatial hazard, to determine if the adaptive rewiring strategy can increase the resilience of the EATN to this spatial hazard (this will also form an assessment of the 'best' and 'worst' case spatial hazards).

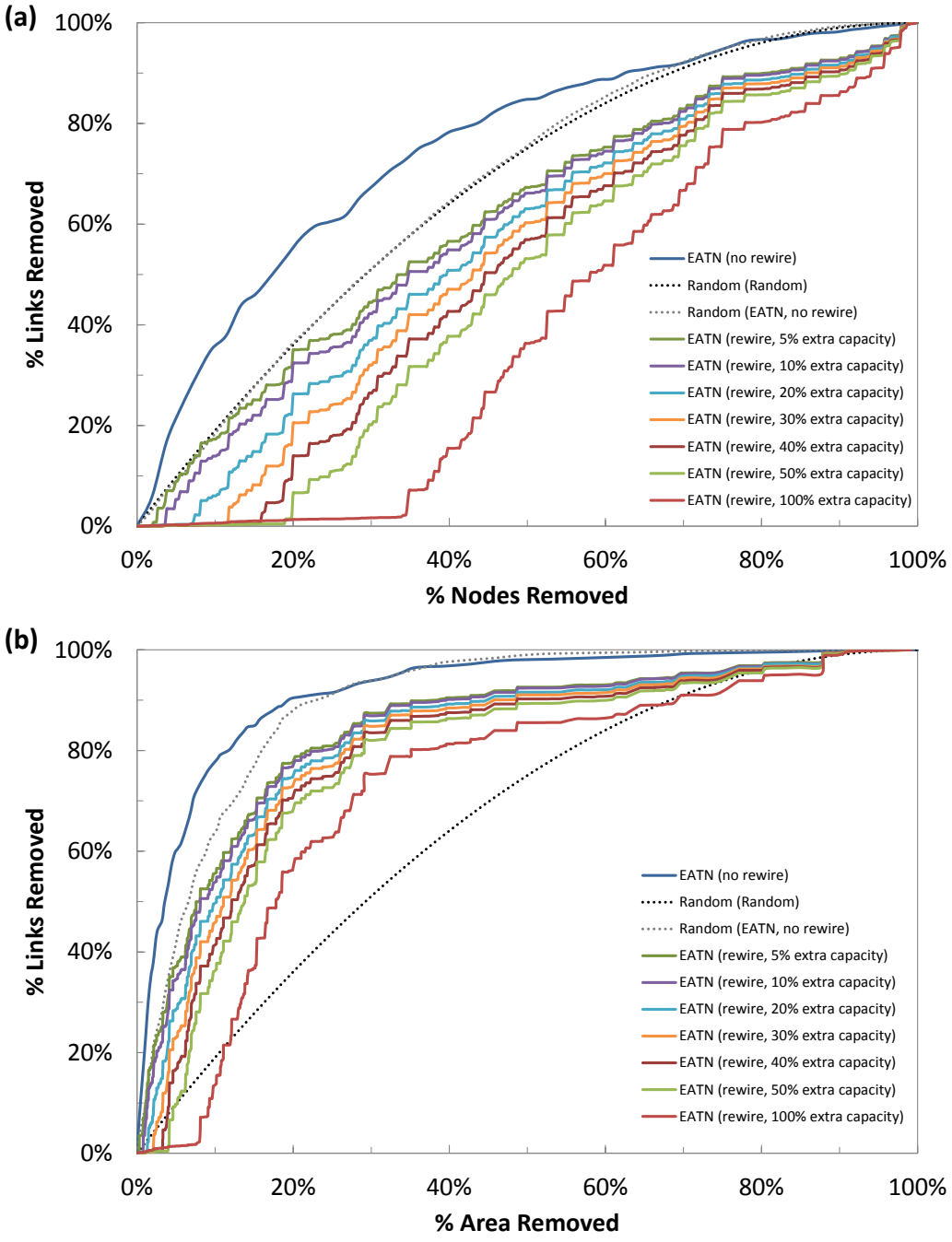


Figure 4.43: The results of the modified 'adaptive' rewiring strategy for the EATN subjected to the central attack spatial hazard. In this modified strategy the capacity of the nodes (when receiving additional links) has been limited, by an percentage of their original degree. Showing (a) the results in terms of the proportion of nodes and links removed and in (b) in terms of the proportion of area and links removed. Also showing the benchmark random network (with a random nodal layout) subjected to the same hazard, with no additional capacity (black dotted line).

Figure 4.43 plots the results for the central attack spatial hazard in terms of the proportion of closed air routes, airports and area. In this figure, air routes are only classed as 'closed' when the air route cannot be redirected, or rewired, to another airport. In Figure 4.43(a) it can be seen that the resilience of the EATN increases even for a small increase in the capacity of airports (there is an increase in resilience of 21% points for an additional airport capacity of 5%, compared to the EATN, when 20% of nodes have been removed). However, these networks are still more vulnerable than the random network, with random nodal locations, when the hazard size is over 15% of the network area (assuming that airports can have double their normal operational capacity) (Figure 4.43(b)). It is interesting to note that air routes are only failed (and not redirected) when all of the airports in the network reach their maximum capacity, therefore for small spatial hazards there is little effect to the network. Even when air routes begin to fail the disruption to air passengers will be minimised, as they can still fly to airports close to their original destination.

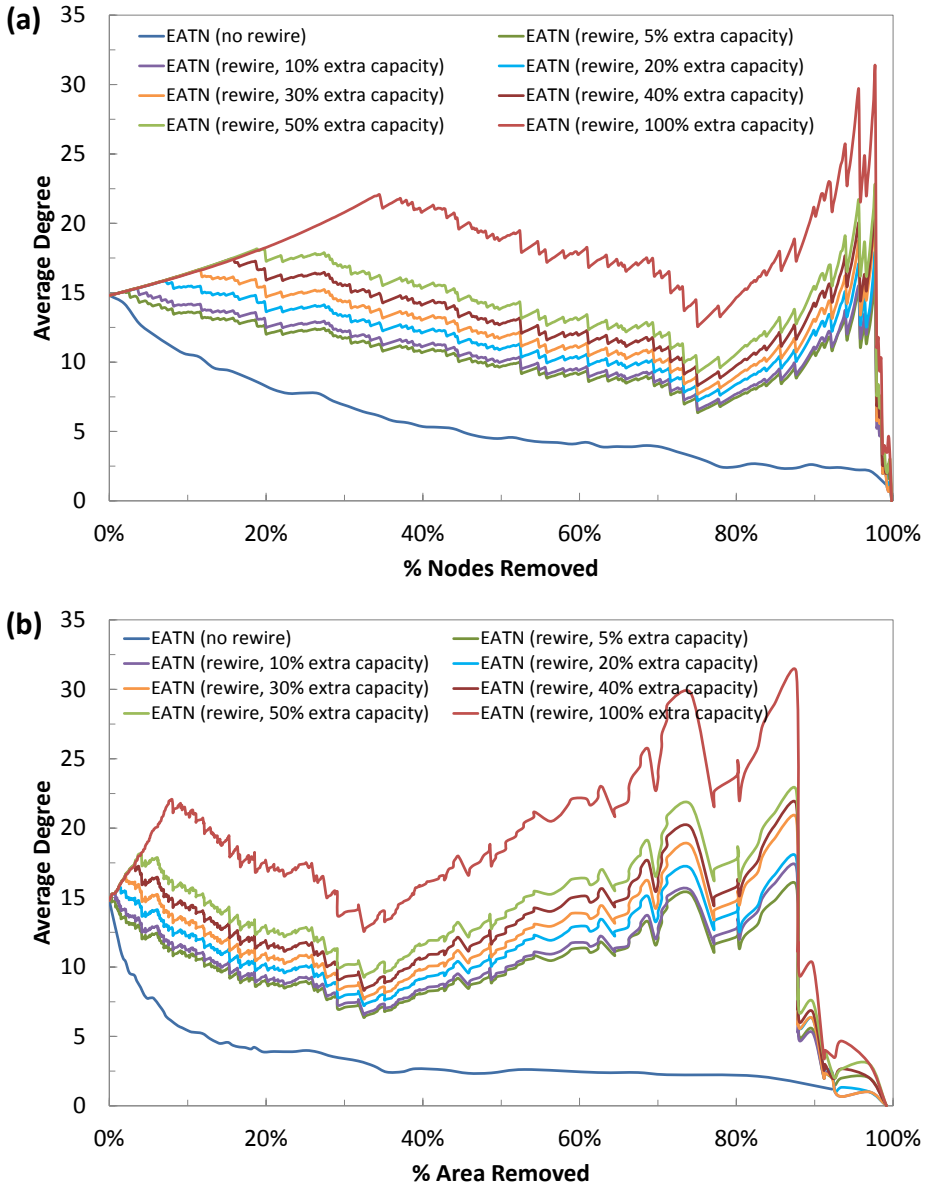


Figure 4.44: Observing the changes in the average degree of the remaining nodes for the EATN and seven adaptively rewired networks (with different nodal capacities). The results in (a) have been plotted with respect to the proportion of nodes removed and in (b) with respect to the proportion of area removed.

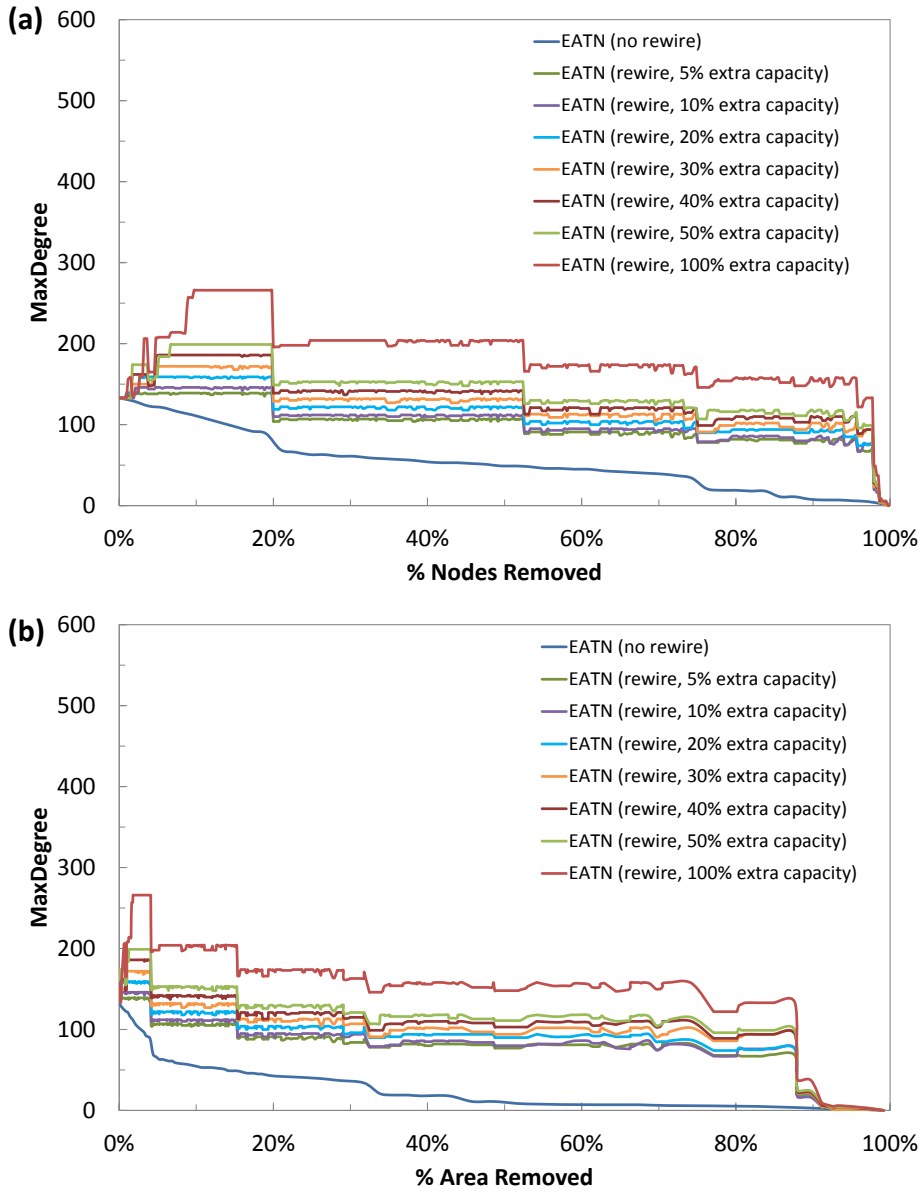


Figure 4.45: Observing the changes in the maximum degree of the remaining nodes for the EATN and seven adaptively rewired networks (with different nodal capacities). The results in (a) have been plotted with respect to the proportion of nodes removed and in (b) with respect to the proportion of area removed.

The maximum and average degree of airports in these rewired networks (and the EATN) has been plotted in Figure 4.44 and Figure 4.45. In this figure, it can be seen that the average degree of all operational airports increases until the capacity of all airports is reached and air routes begin to fail (as there is no additional capacity for them to be redirected). However, after a small number of maximum capacity airports are enclosed by the spatial hazard, the average degree of airports begins to increase again as there is now spare capacity at some airports. It can be seen that all of the adaptively rewired networks show the same pattern of average degree, even though their capacities are different.

The maximum degree of airports in the same networks, plotted in Figure 4.45(c, d), increases until the airport with the highest capacity is removed from the network and then shows a sharp decrease (for example at 20% of the airports closed or 5% of the network area removed). In a similar manner to the average degree, it can be seen that the maximum degree for all adaptively rewired air routes shows the same pattern, despite the differences in capacity.

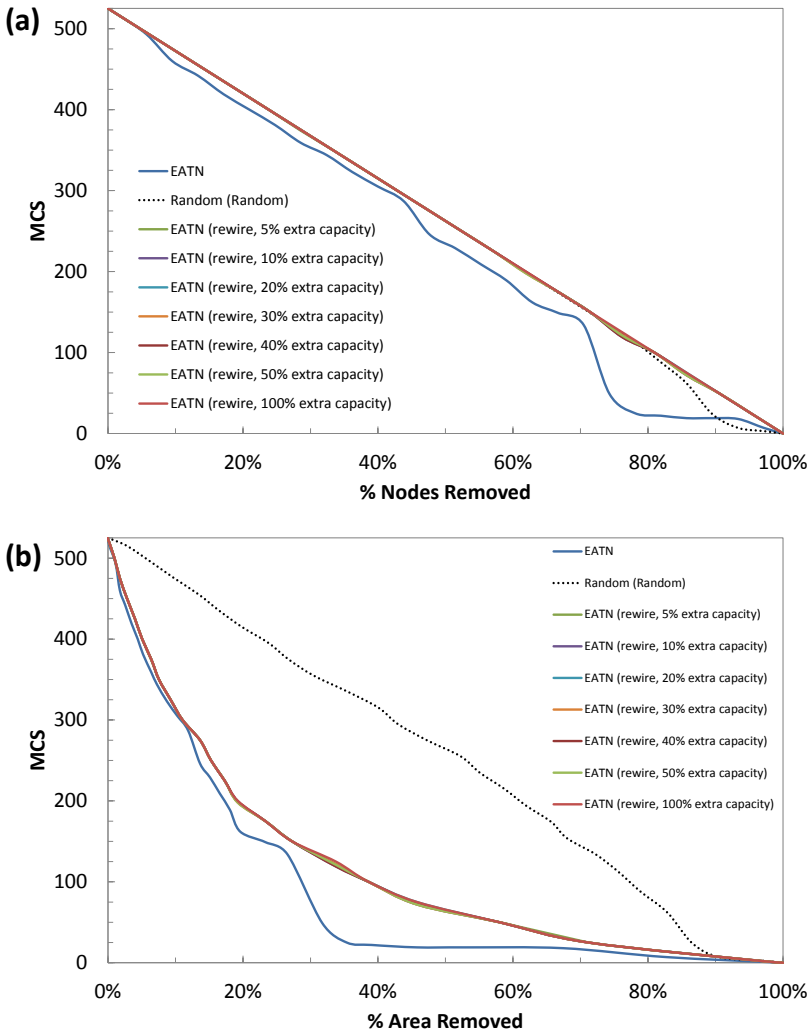


Figure 4.46: Showing the changes in the maximum cluster size (MCS) for the EATN and seven adaptively rewired networks (with different nodal capacities), subjected to the central attack spatial hazard. The results in (a) have been plotted with respect to the proportion of nodes removed from the network and with respect to the size of the spatial hazard in (b).

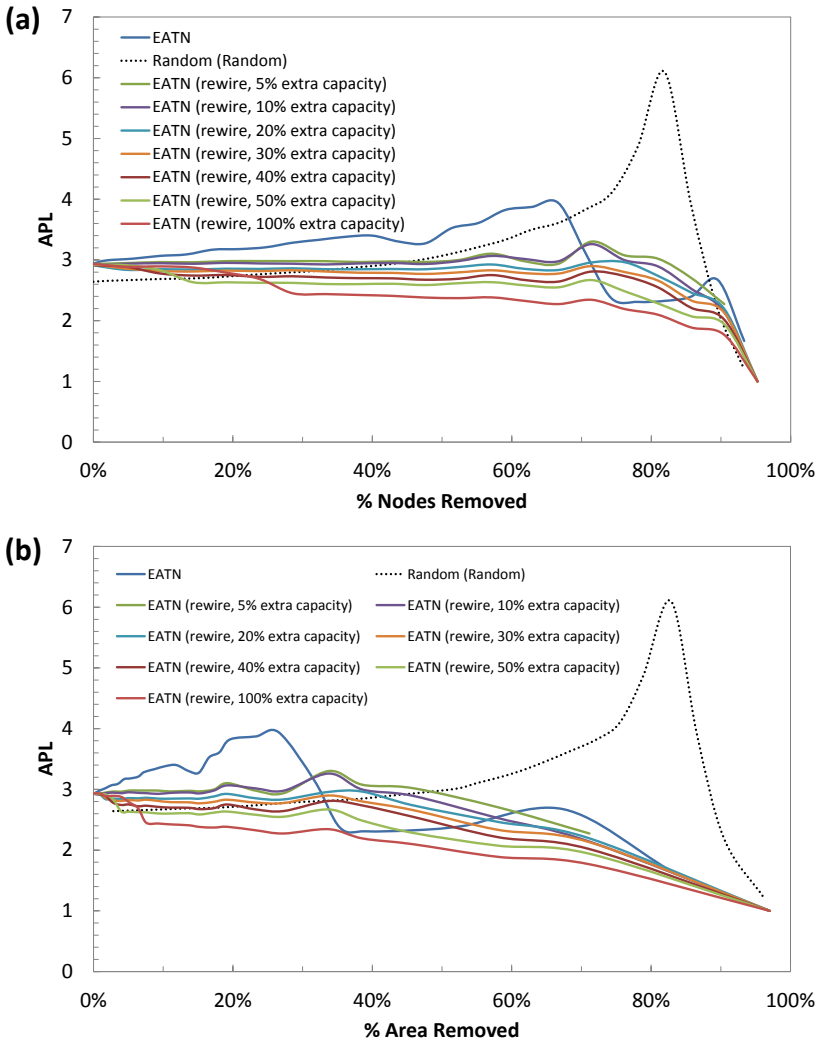


Figure 4.47: Showing the changes in the shortest average path length (APL) for the EATN and seven adaptively rewired networks (with different nodal capacities), subjected to the central attack spatial hazard. The results in (a) have been plotted with respect to the proportion of nodes removed from the network and with respect to the size of the spatial hazard in (b).

The MCS and APL for these adaptively rewired networks have been calculated and are plotted in Figure 4.46 and Figure 4.47, in terms of both the proportion of closed airports and area. It can be seen that the MCS of the rewired networks shows the same results as the random network (with random nodal locations) when plotted in terms of the proportion of airports closed, but shows an increased vulnerability when plotted in terms of the proportion of closed area (Figure 4.46). It is interesting to notice, that all of the adaptively rewired networks show the same values of MCS, indicating that even though there are fewer air routes closed for the larger values of capacity the connectivity of the network remains the same. The APL of the rewired networks also shows an increased resilience compared to the actual EATN and the random network (Figure 4.47). This indicates that by adaptively rewiring air routes

(even if the additional capacity is small) the efficiency of the network is significantly increased compared to that of the non-rewired EATN.

The ability of this modified method to increase the resilience of the EATN to the perimeter attack spatial hazard is also tested. The airports are again given a certain value of additional capacity and are removed individually from the network, the air routes from these removed airports are rewired to other nearby airports as long as there is sufficient capacity to do so. Again, parallel edges are maintained in the network to give an indication of the expected additional air traffic at airports, but are not considered when the MCS and APL are calculated. The results for this analysis are compared to the actual Eyjafjallajökull event to the actual EATN and have been plotted in terms of the proportion of removed links/nodes/area in Figure 4.48.

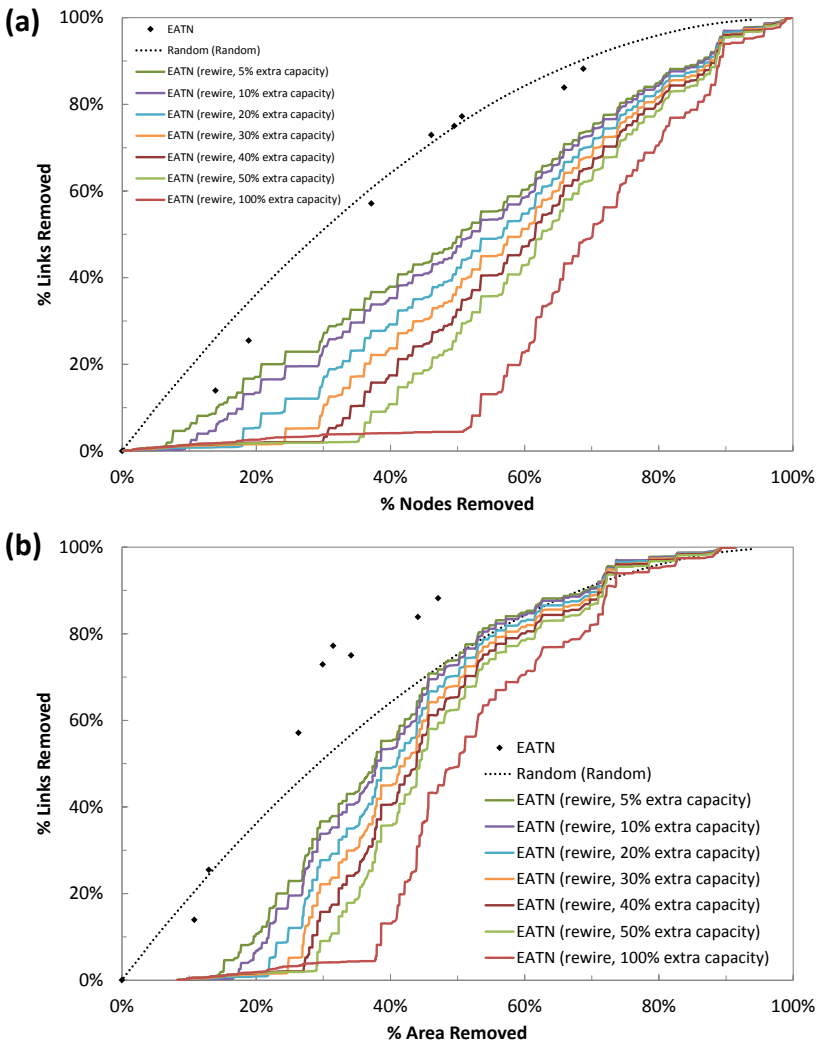


Figure 4.48: The results of the modified 'adaptive' rewiring strategy for the EATN subjected to the perimeter attack spatial hazard. In this modified strategy the capacity of the nodes (when receiving additional links) has been limited. Showing (a) the results in terms of the proportion of nodes and links removed and in (b) in terms of the proportion of area and links removed. Also showing the benchmark random network (with a random nodal layout) subjected to the same hazard, with no additional capacity (black dotted line).

Considering the results for this analysis, plotted in terms of the proportion of closed air routes and airports (Figure 4.48(a)) shows that the EATN is resilient to all sizes of the perimeter attack spatial hazard, provided that airports are given some additional capacity. For example, on the 15th April the ash cloud closed 37% of airports and resulted in the closure of 57% of air routes; however, allowing each additional airport only 5% capacity reduces the proportion of closed air routes to 37% and allowing each airport an additional 50% capacity further reduces these air route closures to only 9%. This resilience is also replicated when the results are presented in terms of the proportion of closed area and air routes (Figure 4.48(b)). The worst day of disruption, compared to the benchmark random network, occurred on the 19thApril and closed 77%

air routes and 31% of air space (24% points more vulnerable than the random network). However, if the modified adaptation strategy is applied to the EATN this vulnerability dramatically reduces and the network now shows resilience to the same size hazard compared to the random network. Giving airports an additional 5% capacity, results in the closure of 38% of air routes (15% points more resilient than the random network) and increasing this capacity to 50% results in the closure of only 11% of air routes (42% points more resilient than the random network).

It is also interesting to note, that in Figure 4.43 and Figure 4.48 there appears to be a correlation between the increase in capacity of airports and the proportion of closed air routes. For example, the proportion of air routes cancelled due to the removal of 60% of airports (when the perimeter attack spatial hazard is applied) is shown in Table 4.2. It can be seen in this table that an increase in airport capacity of 10% results in a decrease in the proportion of cancelled air routes of roughly 3-4%. This information could be used to estimate the required increase in airport capacity so that the proportion of cancelled air routes can be 'capped' for a given position of the spatial hazard.

Table 4.2: The proportion of cancelled air routes for the closure of 60% of airports for seven adaptively rewired networks with different additional airport capacities.

Additional Airport Capacity	Proportion of Cancelled Air Routes
5%	60.27%
10%	58.47%
20%	54.76%
30%	51.24%
40%	47.17%
50%	42.85%
100%	22.72%

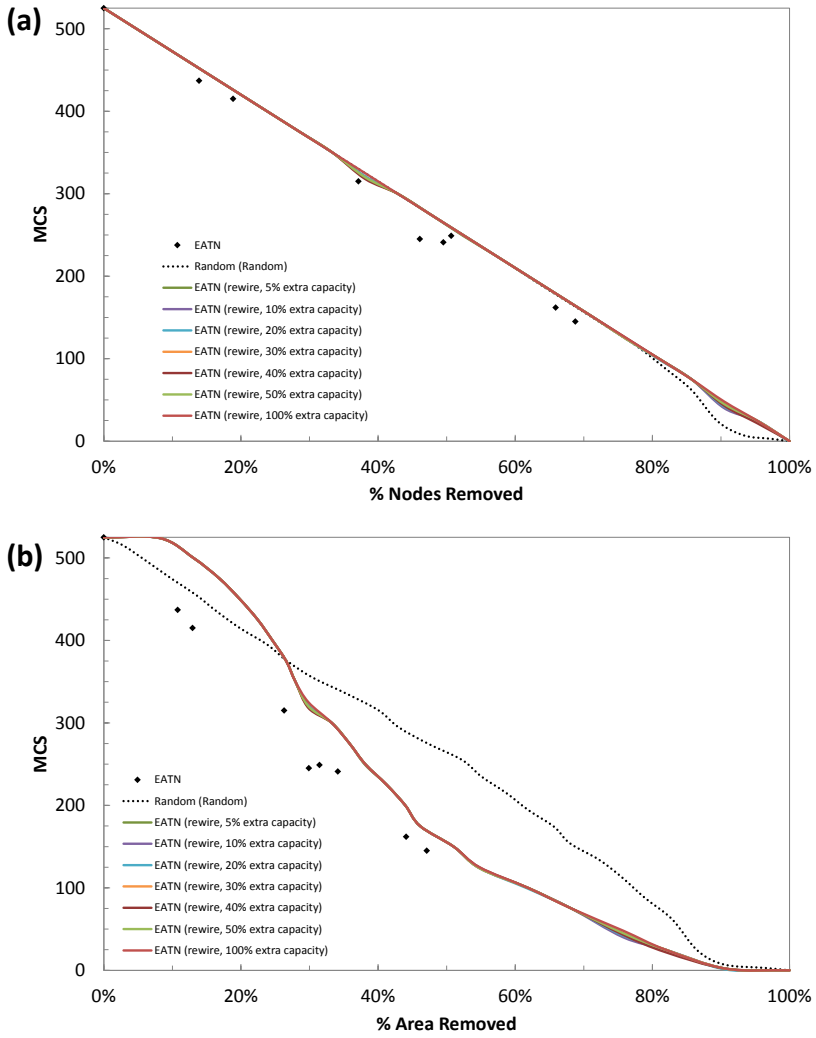


Figure 4.49: Showing the changes in the maximum cluster size (MCS) for the EATN and seven adaptively rewired networks (with different nodal capacities), subjected to the perimeter attack spatial hazard. The results in (a) have been plotted with respect to the proportion of nodes removed from the network and with respect to the size of the spatial hazard in (b).

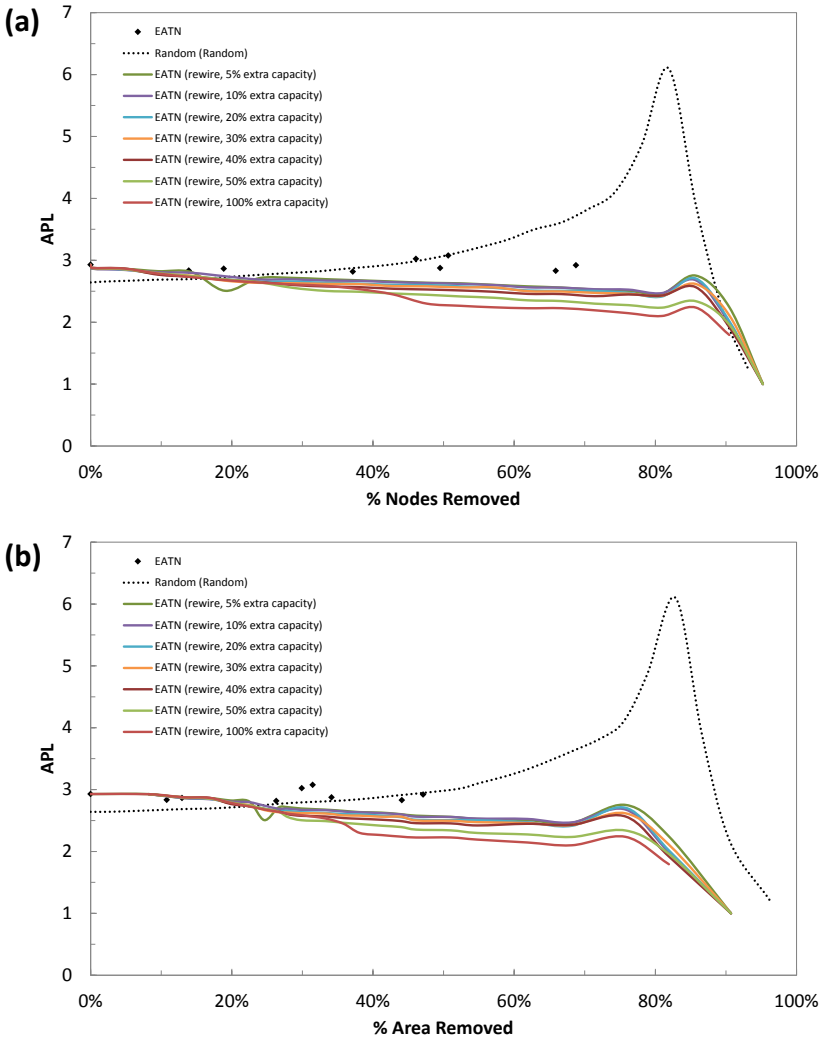


Figure 4.50: Showing the changes in the average path length (APL) of the EATN and seven adaptively rewired networks (with different nodal capacities), subjected to the perimeter attack spatial hazard. The results in (a) have been plotted with respect to the proportion of nodes removed from the network and with respect to the size of the spatial hazard in (b).

The MCS and APL for these networks were also calculated, after the removal of 10 airports, and have been shown in Figure 4.49 and Figure 4.50. In this figure, it can be seen that all networks show the same MCS value as the random network when plotted in terms of the proportion of airports closed (Figure 4.49(a)). However, plotting the results in terms of the proportion of area closed shows that these networks are resilient until around 30% of the area is covered by the spatial hazard (Figure 4.49(b)). Therefore, for small sizes of the spatial hazard it can be concluded that the network remains largely as one cluster, as air routes are allowed to rewire to other airports not affected by the hazard. The APL both plotted in terms of the proportion of airports and area removed shows that the modified adaptive rewiring strategy is the best in terms of maintaining high network efficiency (Figure 4.50). The maximum value of APL

for the modified strategy, with only an additional airport capacity of 5%, is 2.93 compared to a value of 3.94 for the EATN, which reduces to 2.93 if the additional airport capacity is increased to 50%.

This chapter has investigated the hazard tolerance of a range of synthetic spatial networks to different locations of spatial hazard. All possible combinations of hazard location, network class (exponential, scale-free and random), nodal layout (uniform with area, uniform with distance and clustered) and node introduction order (random, proportional with distance and with distance) have been considered. This analysis has revealed that the location, and size, of a spatial hazard can dramatically alter the hazard tolerance of a spatial network. For example, locating the majority of nodes, and highly connected nodes, around the geographic centre produces the most vulnerable network when subjected to the 'central attack' hazard (having up to 22% more links removed than a benchmark network); however, this network shows an increased resilience to hazards located away from this area (being up to 7% more resilient). It was also shown that scale-free and exponential networks showed a decreased connectivity, compared to a benchmark network, for all sizes of the 'central attack' spatial hazard. However, the scale-free networks became increasingly inefficient, as the hazard expanded, whereas the exponential network was able to maintain efficiency. This was attributed to the topological differences between these two network classes caused by the inclusion of a proximity component in the exponential network generation algorithm, which 'shifts' connections that were bound for a high degree node to a lower degree node, causing the network to maintain efficiency when these high degree nodes are removed.

These results were then used to inform strategies to increase the resilience of the EATN, when subjected to the 'central attack' hazard. The first strategy was aimed at 'adaptively' rewiring the network and the second 'permanently' rewiring the network. It was concluded that the adaptive strategy was superior at increasing the resilience of the EATN and, unlike the permanent strategy, did not compromise the efficiency of the network under normal operational conditions.

The results of this chapter have focused on quantifying the resilience of a network as a whole, but have shown that the removal of some individual nodes can have more of an impact to the remaining network than the removal of other nodes. For example, the removal of some nodes causes a sharp increase in the proportion of links removed and a sharp decrease in the connectivity and efficiency of the remaining network. Therefore, the next chapter will investigate the effects that the removal of these 'critical' nodes can have to the network and will develop strategies to identify these nodes.

CHAPTER 5: IDENTIFYING CRITICAL COMPONENTS IN INFRASTRUCTURE SYSTEMS

The previous chapter generated a range of spatial networks, with different spatial and topological characteristics, and subjected them to spatial hazard to quantify their resilience. Through this analysis it was also discovered that the removal of some nodes can have an increased effect to the resilience of the network than other nodes, particularly in the more structured scale-free and exponential networks which are not homogeneous (unlike random networks). This chapter focuses on the impact that the removal of a single node can have to the network and develops methods to identify individual nodes that have a disproportionate effect to the remaining network, when removed. These nodes are more likely to have a large effect to infrastructure systems that are governed by physically based rules (e.g. water distribution systems and power grids) rather than systems governed by logistical rules, as it is harder to redirect flow in these networks (e.g. aircraft can be rerouted to airports with short notice, however, due to the system constrains it is harder to redirect flow governed by physically based laws).

5.1: DEVELOPMENT OF A REDUCED COMPLEXITY FLOW MODEL

In engineering, there are numerous flow models that can be used to simulate the physical processes and the transfer of services from areas of supply to areas of demand within infrastructure systems (as previously discussed in Chapter 2.4). In this chapter, it is initially desirable to determine the applicability of using graph theory metrics to analyse infrastructure systems governed by physically based rules, in general (and not for a specific infrastructure system), and therefore, what is arguably the simplest possible flow model is developed; however, the model still has all the attributes necessary to simulate flows in a network.

To achieve this, a simple hydraulic model, which can be found in any standard hydraulic text (Novak et al. (2010) for example), is modified. Although, this is a hydraulic model it has analogies with other categories of infrastructure network, such as electrical distribution networks and traffic flow problems – for example, from Table

2.5 it can be seen that the pressure head in a hydraulic system is analogous to a potential difference in an electrical network or demand in traffic network. Equally, pipe friction in a hydraulic network could be compared to electrical impedance in an electricity network, or vehicle density in a traffic network. The similarities in the physical behaviour of different sorts of infrastructure networks means that the results obtained for one type of network although not exactly equivalent are indicative of the behaviour of other types of infrastructure networks. In the case of a hydraulic network, the governing equations for a steady-state flow problem are the conservation of mass (Equation 5.1) and conservation of energy (Equation 5.2):

- Conservation of mass. The mass at any point along a pipe must be constant (i.e. flow into a pipe = flow out of a pipe):

$$Q_{in} = Q_{out} \tag{5.1}$$

- Conservation of energy. Energy must be conserved for hydraulic networks this energy usually consists of potential energy and kinetic energy and is defined by the Bernoulli equation (for pipe flows):

$$z_1 + \frac{p_1}{v_1} + \frac{v_1^2}{2g} = z_2 + \frac{p_2}{v_2} + \frac{v_2^2}{2g} + fl \tag{5.2}$$

  Where, *z* = potential energy; *p* = pressure; *v* = velocity at points 1 and 2 respectively; *fl* = frictional losses; and *g* = gravitational constant. Equation 5.2 basically illustrates that between points 1 and 2 conservation of energy is maintained.

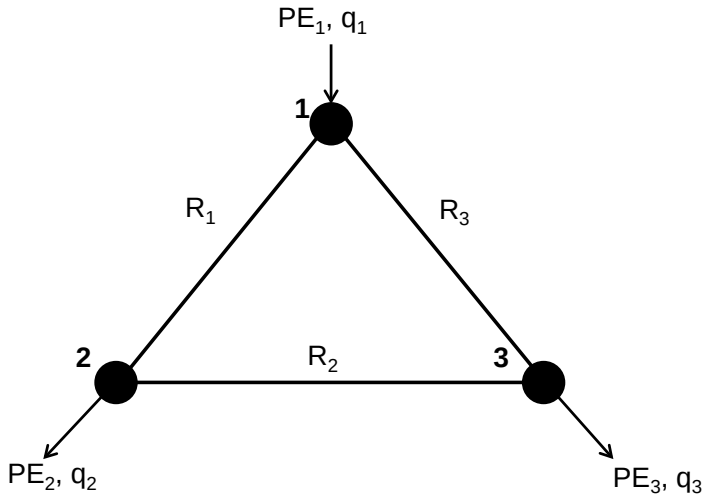


Figure 5.1: An example network consisting of three nodes and three links, where Node 1 is the supply node and Nodes 2 and 3 are the demand nodes (node numbers are indicated by the bold numbers to the left of each node); *Q* = flow of service that the node either demands or supplies; *PE* = potential energy of node; *R* = resistance of link (subscript values indicate node/link to which they refer).

The flows in a network are calculated (through both the nodes and the links) using the process described below. A small example network, consisting of three nodes and three links, is used to illustrate the process (Figure 5.1). In this example, Node 1 is a supply node and the other two nodes are demand nodes.

1. Calculate the potential energy for each node in the network

The standard hydraulic formula for calculating flow in a pipe is:

$$F_l = k(Q)^n \tag{5.3}$$

Where, F_l are the frictional losses, *k* is a constant that describes the resistance of the system (for example, pipe friction for a hydraulic network or electrical impedance for an electrical system) and *Q* is the flow through the pipe. For steady state hydraulic flow in pipes, the value of *n* normally equals 2; however, as this is a generic model that represents a range of infrastructure networks the problem is reduced to its most base level by assuming the losses have a linear relationship with flow (i.e. $n = 1$). Linearizing the losses has the added advantage of enabling the problem to be solved directly.

$$F_l = R(Q_{1-2}) \tag{5.4}$$

Where, R is the resistance of the link and $Q_{1\text{-}2}$ is the flow in the pipe connecting Nodes 1 and 2.

Assuming incompressible flow, the velocity at Nodes 1 and 2 are equal, and therefore the friction loss in the pipe is equal to the difference in potential energies of the two connected nodes. Using this and rearranging Equation 5.4 gives:

$$Q_{1-2} = \frac{1}{R}(PE_2 - PE_1) \tag{5.5}$$

Using conservation of mass, the external flow at each node (i.e. either the quantity demanded by the node, or the quantity supplied by the node), denoted by q, can be calculated by summing the flows in the connected links. For Node 1 in Figure 5.1 this becomes:

$$q_1 = \frac{1}{R_1}(PE_2 - PE_1) + \frac{1}{R_3}(PE_3 - PE_1) \tag{5.6}$$

Equation 5.6 can be rearranged as:

$$q_1 = PE_1\left(-\frac{1}{R_1} - \frac{1}{R_3}\right) + PE_2\left(\frac{1}{R_1}\right) + PE_3\left(\frac{1}{R_3}\right) \tag{5.7}$$

Using this method to obtain expressions for the external flow at the other nodes (in the same format as Equation 5.7) and combing them in a matrix form results in:

$$\begin{bmatrix} q_1 \\ q_2 \\ q_3 \end{bmatrix} = \begin{bmatrix} -\frac{1}{R_1} - \frac{1}{R_3} & \frac{1}{R_1} & \frac{1}{R_3} \\ \frac{1}{R_1} & -\frac{1}{R_1} - \frac{1}{R_2} & \frac{1}{R_2} \\ \frac{1}{R_3} & \frac{1}{R_2} & -\frac{1}{R_2} - \frac{1}{R_3} \end{bmatrix} \begin{bmatrix} PE_1 \\ PE_2 \\ PE_3 \end{bmatrix} \tag{5.8}$$

The external values of flow (q) for the demand nodes and the resistances (R) of the links are known, but the values of flow from the supply nodes are unknown. In the example network (Figure 5.1) this is easy to calculate (as it is the only supply node), however, for a network with two or more supply nodes the supply will not be evenly distributed. Setting the supply nodes as potential energy reference points (i.e. PE = 0) enables the condensation of Equation 5.8, resulting in Equation 5.9. The potential energy of each demand node can be obtained by solving Equation 5.9.

$$\begin{bmatrix} q_2 \\ q_3 \end{bmatrix} = \begin{bmatrix} -\frac{1}{R_1} - \frac{1}{R_2} & \frac{1}{R_2} \\ \frac{1}{R_2} & -\frac{1}{R_2} - \frac{1}{R_3} \end{bmatrix} \begin{bmatrix} PE_2 \\ PE_3 \end{bmatrix} \quad 5.9$$

2. *Calculate the flow through each link*

To satisfy the 'Conservation of Energy' (Equation 5.2) the flow through each link in the network is calculated using Equation 5.5.

3. *Calculate the flow provided by each supply node*

The external flow at each supply node can be found using Equation 5.8.

It is worth noting that the equations describing the reduced complexity flow model have consistent units. For example, in the case of a hydraulic network, if the input values were in terms of meters and seconds, then the output value of flow would have a unit of meters per second.

5.2: ASSESSMENT OF USING NETWORK GRAPH THEORY IN FLOW BASED PROBLEMS

To assess the applicability of using network graph theory in flow based problems, the reduced complexity flow model has been used to analyse the flows around 60 network models (20 for each of three classes of network: scale-free, exponential and random). Each network includes 1000 nodes and the number of links is varied to enable a comparison between networks with different levels of connectivity (for example, for the same number of nodes, a network with more links is better connected than a network with fewer links and will transfer the flow differently between the areas of supply and demand). The random and scale-free networks are purely topological models, generated using the traditional network generation algorithms of Erdos and Renyi (1960) and Barabasi and Albert (1999). However, in order to use the network generation algorithm for exponential networks, developed in this thesis, a spatial component must be used in the generation, due to the probability of attachment being based on both degree and proximity for these networks. This has been achieved using the random uniform with area nodal layout (Figure 4.1(b)), but will not be considered in the analysis of the flow around the system (i.e. only the topology will be considered and not the length of connections between components).

This is an initial assessment of the applicability of using graph theory in flow based problems and therefore the resistances of all links are equal. For a hydraulic system the resistance is a combination of pipe length, diameter and roughness and it is assumed that the combination of these parameters satisfies this assumption. It has been shown by Newman (2004) that the more general case of links with different properties can be addressed using the weighted network approach (modifying the graph theory metrics to take into account the differences in the link properties) such as that of Opsahl et al. (2010) but this is outside the scope of this research.

Before the flows in the 60 test networks can be calculated, values of supply and demand need to be assigned to each node. However, the nodes which are to be supply nodes (infrastructure supplying a service) and those that are to be demand nodes (regions requiring the service) need to be initially decided. This is done by ranking the nodes in descending order of degree and choosing the top 1% as supply nodes, with the others being assigned as demand nodes (for example, for a network with 1000 nodes there will be 10 supply nodes). The small proportion of supply nodes relative to demand nodes is consistent with real world infrastructure systems which will have a small proportion of nodes supplying services (e.g. power stations or reservoirs) compared to the proportion of demand nodes (e.g. households); however, the absolute value of 1% is somewhat arbitrary. In these models, it is assumed that the supply nodes in the network have sufficient capacity to supply any service required by the demand nodes and as this analysis considers a single point in time, it is assumed that the network has reached equilibrium. In real infrastructure networks (e.g. for the case of a pipe network) if a reservoir does not have sufficient capacity to meet the required demand, the reservoir will run dry and the flow will cease; if there are other reservoirs in the system the flow will be redistributed. This can be accommodated in the model by using an iterative procedure but is beyond the scope of this thesis. A numeric value of demand is assigned to the demand nodes based upon their degree (i.e. the number of links attached to them). It is argued that this is a reasonable approximation as areas with large populations and therefore large demands for services will require a correspondingly greater number of nodes and links to provide these (for example, a large city will have a greater need for service than a rural community and will also have a correspondingly larger amount of infrastructure).

In this initial assessment, the results of the reduced complexity flow model are compared to the shortest APL of the network (Equation 2.3). This metric describes the fundamental properties of a network and is a measure of the efficiency of the network (as it considers the shortest path between pairs of nodes and flow will distribute itself around the network such that it finds the minimum energy solution). The higher the value of shortest APL the further the services in the network must flow in order to travel from the supply nodes to the demand nodes and therefore the more inefficient the network.

Figure 5.2 shows the results of correlating the APL with the flow through the demand nodes (the flow is referred to as being 'through a node', for simplicity, rather than stating 'the in-flow and the out-flow at the node' (as these two values are equal)). Fitting a power law trend line through the results, shows an R^2 value of greater than 0.9, for all three classes of network model. This high R^2 value suggests that at least parts of graph theory could be used in the analysis of infrastructure networks, where flow is an important factor.

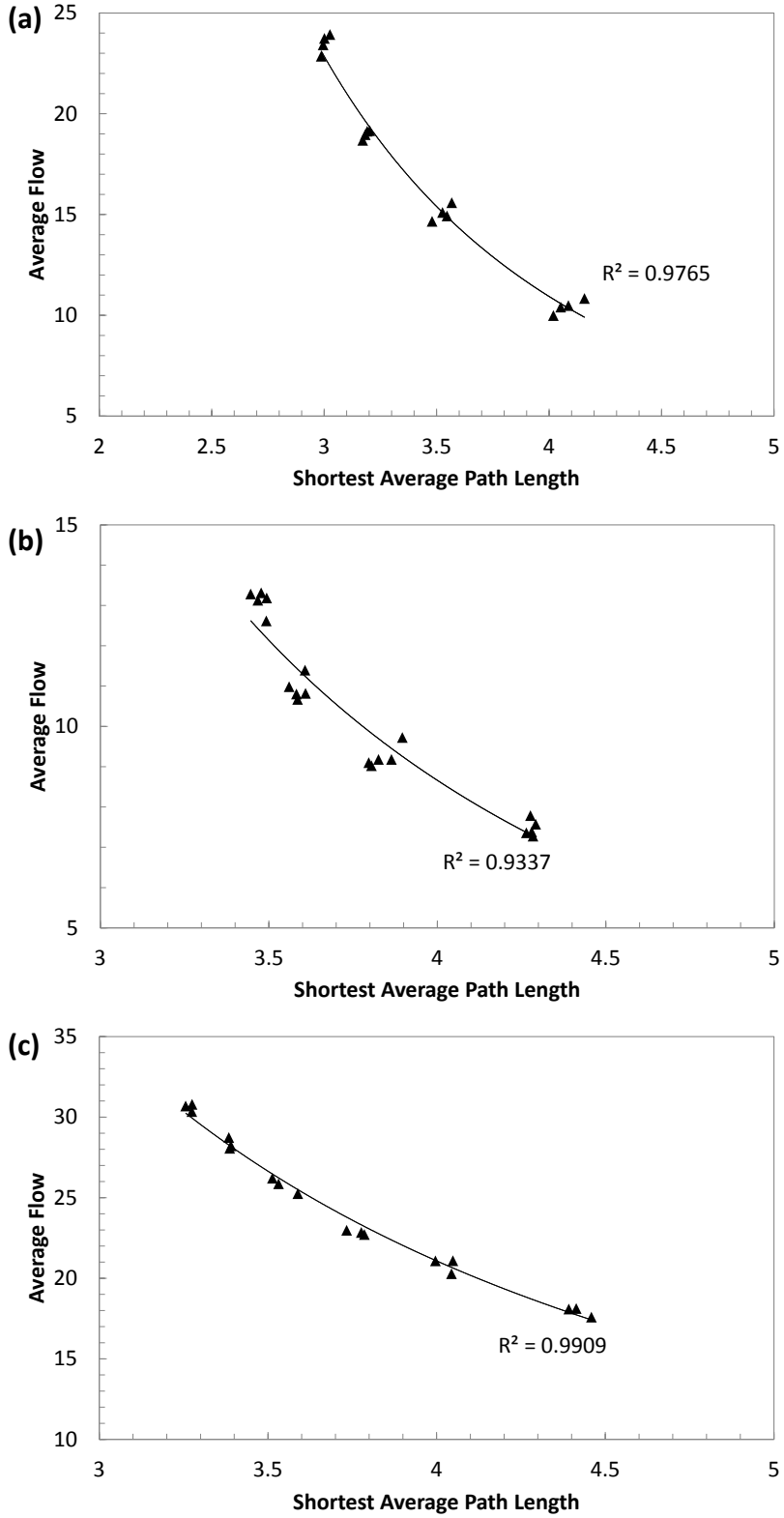


Figure 5.2: Showing the correlation between average flow and shortest average path length for 20 (a) scale-free, (b) exponential and (c) random networks, each with 1000 nodes and different number of links.

When generating the networks, used in the analysis for Figure 5.2, it was not possible to generate networks with a consistently increasing value of APL due to the way the algorithms operate, particularly for the scale-free networks (Figure 5.2(a)). In this case,

the number of links in the network is altered by changing the starting number of nodes, m_0 (see Chapter 2.5.2.3 for more detailed explanation of the network generation algorithm). The random element, when generating the number of links to connect the new node to the existing network, alters the total number of links in each network by a small amount. To generate networks with noticeably different levels of connectivity m_0 needs to be altered. Each network generated with the same number of initial nodes has approximately the same number of links, and therefore approximately the same value of APL, causing the clustering of results in Figure 5.2 (i.e. each cluster is a group of networks with the same number of initial nodes). The clusters are less apparent in the exponential networks (Figure 5.2(b)), which is surprising as the network has a similar network generation algorithm to the scale-free networks. However, this generation algorithm also allows connections to form between pairs of existing nodes, introducing another random element and causing different levels of connectivity in the different networks with a roughly equal number of links. In the case of the random networks, the weak clusters in Figure 5.2(c) represent networks with a different linking probability. Due to this probability element, networks that have the same value of linking probability can have a different total number of links, resulting in different values for APL. After showing that, at least part of, graph theory is applicable to the analysis of physically based flow networks (using APL), the application of centrality measures to these networks is now considered.

The three most commonly used centrality measures, betweenness centrality, closeness centrality and degree centrality were developed by Freeman (1979) and have previously been described in Chapter 2.5.4.3. The same networks are used (i.e. the 60 x 100 node networks in Figure 5.2) and calculate the flow through each demand node using the reduced complexity flow model, correlating this with the centrality of that node (calculated using Pajek software for all three centrality measures (Batagelj and Mrvar 2003)). Only the demand nodes are considered in this analysis, as the flow in these is of primary concern, only 1% of the nodes in the network are supply nodes (i.e. 10 nodes). Each network has 990 demand nodes and therefore contributes 990 points to the graph. Because of this and to keep the figure clear, only the results for three of the networks have been presented (chosen at random) for each centrality

measure (Figure 5.3, Figure 5.5 and Figure 5.6); however, these are typical of the correlations achieved for the other networks.

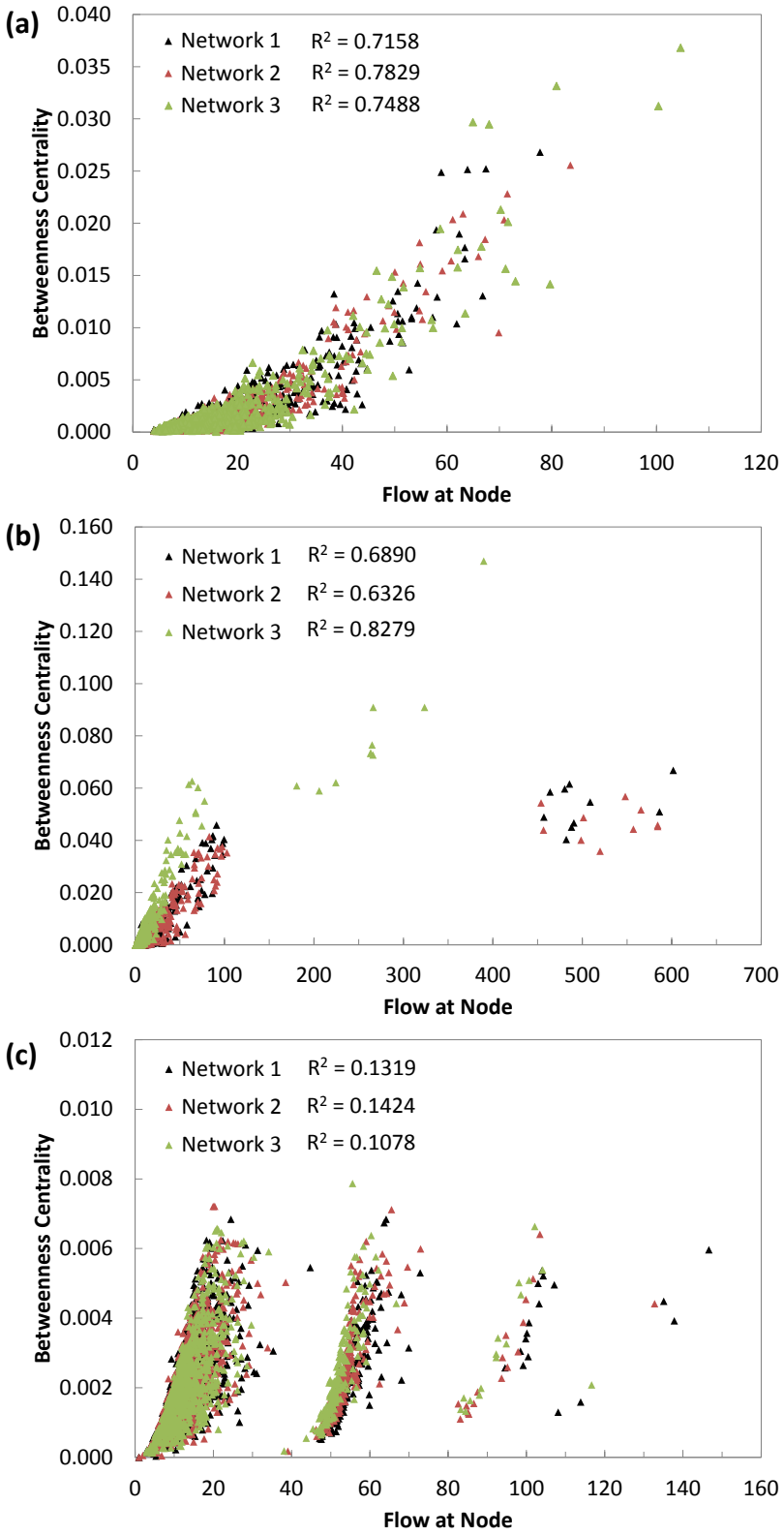


Figure 5.3: Correlation between betweenness centrality and flow at the corresponding node for (a) scale-free, (b) exponential and (c) random networks with 1000 nodes and around 5000 links. The R^2 value is generated using a best fit linear line for all networks (as this is the line of best fit).

Figure 5.3 shows the correlation between the betweenness centrality of a node and the flow through the same node for the three classes of network model. The results of these simulations show an R^2 value of around 0.7 for scale-free networks (Figure 5.3(a)), indicating that the nodes with a high value of flow through them tend to be the nodes with a high value of betweenness. This is also the case for the exponential networks; however, this class of network shows more scatter in the results (Figure 5.3(b)). It is apparent that there is little or no correlation for the random networks (Figure 5.3(c)) (the R^2 values are between 0.1-0.2).

The four clusters of results for the random networks (Figure 5.3(c)) can be explained by considering the proximity of demand nodes to the supply nodes. The nodes which are directly connected to one, or more, supply nodes will have proportionately higher flows through them than those that are not connected; as they must transfer flow through themselves to other nodes in the network that are not directly connected to a supply node. Each cluster (in Figure 5.3(c)) contains nodes that are a specific number of links away from a supply node. For example, the nodes in the far right cluster are directly connected to a supply node, while the far left cluster shows those nodes where the flow from the supply node has passed through three or more links. Figure 5.4 shows this diagrammatically, where the supply node is indicated in red and three demand nodes in black. It can be seen that the demand node which is directly connected to the supply node is transferring flow through to the other two connected demand nodes, and has a value of flow which is twice the value of its demand (this node would form part of the far right cluster in Figure 5.3(c)). The central demand node requires its own value of demand and is also transferring flow to the remaining demand node (on the far right) but has a significantly lower flow than that of the demand node directly connected to the supply node (and would form part of the central cluster in Figure 5.3(c)). The final demand node (far right) only requires its own value of demand and does not transfer this to other demand nodes, so its value of flow is equal to its degree (and would form part of the far left cluster in Figure 5.3(c)).

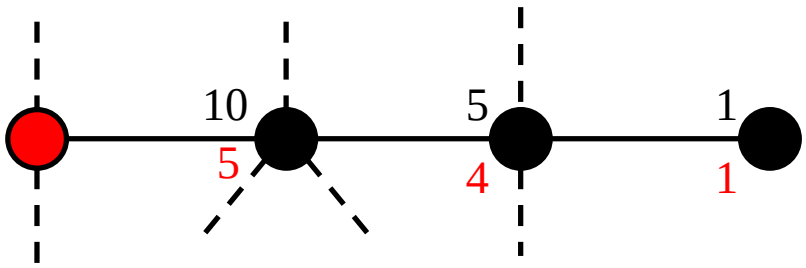


Figure 5.4: Showing a sample section of a network, indicating a supply node (in red) and three demand nodes (in black). The top number (black) indicates the flow through the node and the bottom number (red) is the amount of service provision required by that node (also equal to its degree). The dotted lines indicate connections to other nodes in the network, which have not been included for simplicity. The flows shown assume that the other nodes in the network do not require a proportion of the flow; this is assumed in this example for simplicity only and is not an assumption of the flow model itself.

Comparing the flow at a node and the closeness of that node (for the same generated networks used in Figure 5.3) shows similar results to those in Figure 5.3. The R^2 values for the scale-free networks (Figure 5.5(a)) are around 0.8, indicating that the nodes that are central to the network also have a high flow through them. The R^2 values for two of the exponential networks are similar to that of the scale-free networks (with a value of around 0.7), whereas one network shows an R^2 value of 0.4 (Figure 5.5(b)). This variability is again due to the added random element of the connections between pairs of existing nodes in the network generation algorithm. The random networks (Figure 5.5(c)) show little or no correlation between the two measures (with R^2 values between 0.1 and 0.2), but similarly to show the same clustering of results, explained by the proximity of supply nodes to demand nodes (see Figure 5.4).

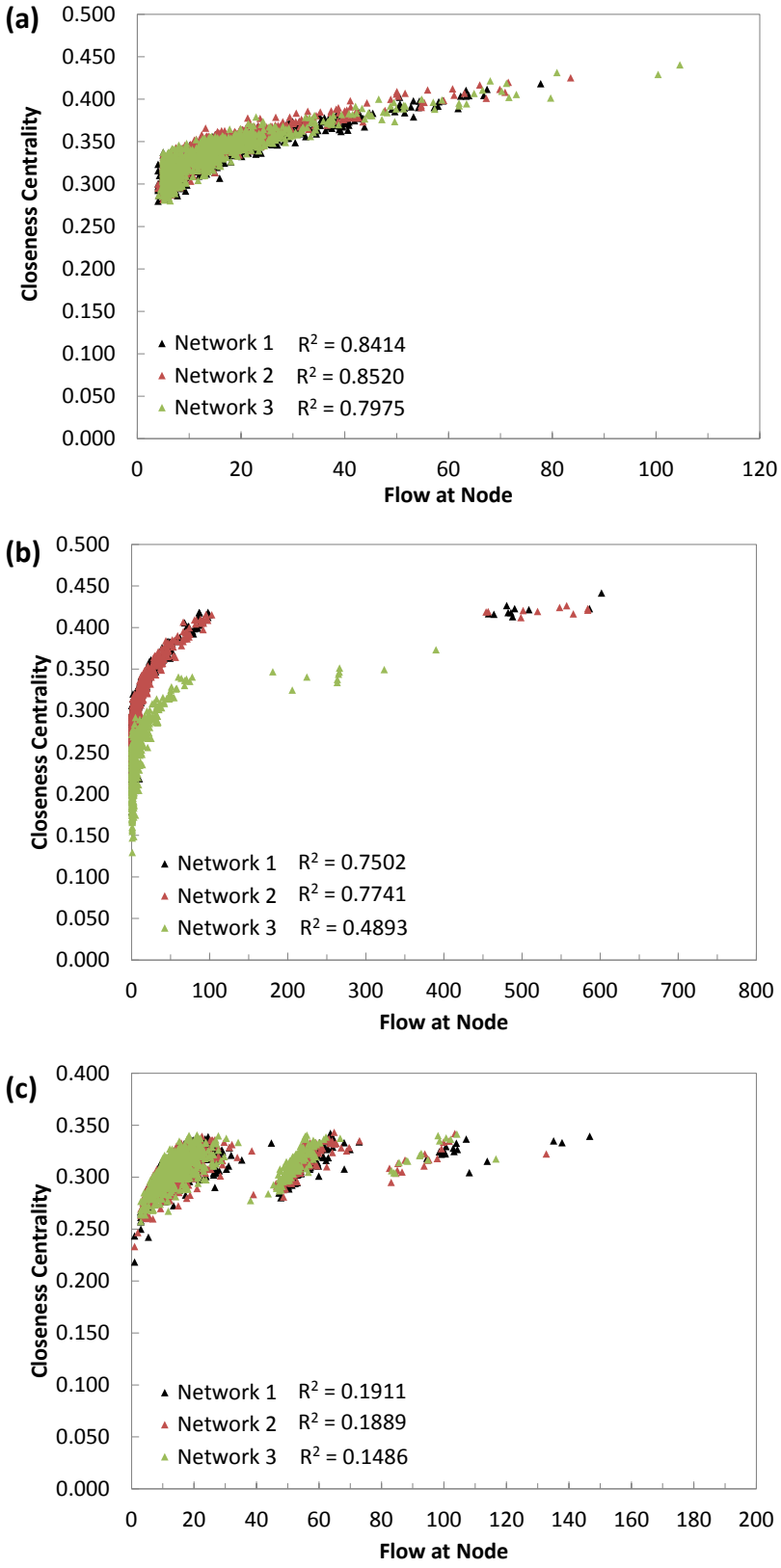


Figure 5.5: Correlation between closeness centrality and flow at the corresponding node for (a) scale-free, (b) exponential and (c) random networks with 1000 nodes and around 5000 links. The R^2 value is generated using a best fit linear line for the scale-free and random networks, and a logarithmic line for the exponential networks.

Considering the final centrality measure, degree centrality, the R^2 value for scale-free networks is around 0.7-0.8 indicating that nodes with a high degree also have a high value of flow through them (Figure 5.6(a)). This is also the case for the exponential networks (Figure 5.6(b)) and can be explained by considering one of the assumptions that was made in the creation of the networks, namely that the demand (of service) required by a node is proportional to the degree of that node. Considering this assumption it could be argued that there is expected to be higher flow at the nodes with a high degree than the nodes with a low degree, from Figure 5.6(a, b) this is shown to be the case. However, it is interesting to note in the case of the random networks (Figure 5.6(c)) the demand nodes with a high degree are not necessarily the nodes with the high flow through them. This can be explained by considering the proximity of the demand nodes to the supply nodes and also in the algorithms used to generate the networks. The main difference between the generation algorithms for scale-free networks and random networks is the method used to assign links to connect pairs of nodes. The algorithm for generating scale-free networks includes a 'rich get richer' component, meaning that nodes with a high degree 'attract' the links from new nodes (Barabasi and Albert 1999); this component is not included in the algorithm for generating random networks (where the new links are attached to nodes based on a user defined probability and not a measure of degree) (Erdos and Renyi 1960). It is also worth noting that the high degree nodes in scale-free networks tend to be attached to other high degree nodes (as a result of the algorithm). As the supply nodes are assigned to the network based upon degree (the supply nodes being the top 1% of highest degree nodes) these nodes tend to be linked to other high degree nodes resulting in the nodes which transfer the service to other nodes in the network being the ones with a high degree, suggesting the reason behind the correlation in Figure 5.6(a) and the lack of correlation in Figure 5.6(c).

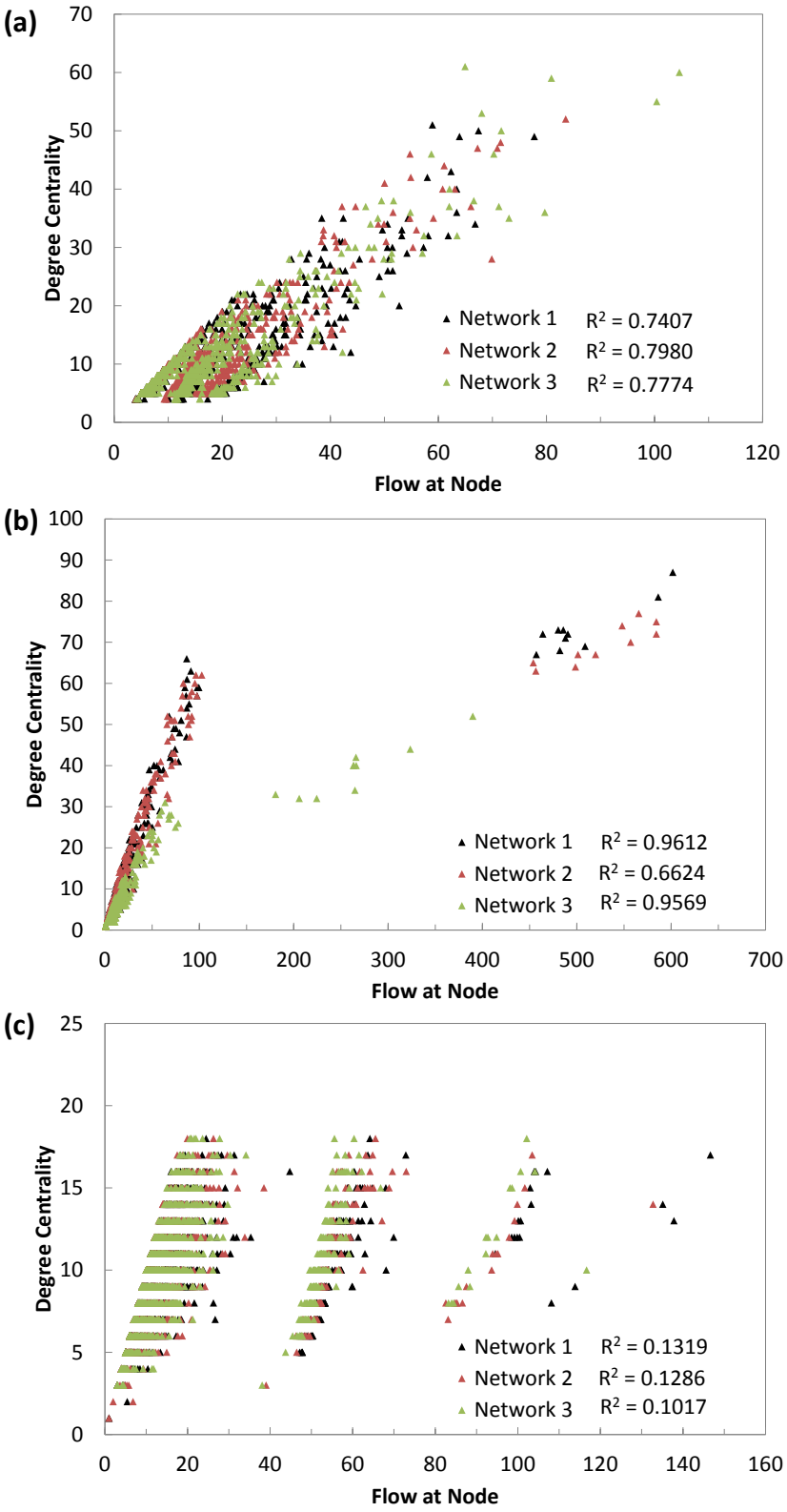


Figure 5.6: Correlation between degree centrality and flow at the corresponding node for (a)scale-free, (b) exponential and (c) random networks with 1000 nodes and around 5000 links. The R^2 value is generated using a best fit linear line for the scale-free and random networks and a power-law for the exponential networks.

5.3: APPLICATION OF GRAPH THEORY TO IDENTIFY SPECIFIC VULNERABLE AREAS

After determining that network metrics can be applied to the analysis of infrastructure systems that are governed by physically based laws, the ability of these metrics to better establish the 'critical' nodes in a network is now assessed (i.e. the nodes that, when removed from the network, have a disproportionate effect on the remaining network). As the reduced complexity flow model was used to model flow based problems in general rather than specific infrastructure networks, it may be argued that the simplification renders the analysis invalid; therefore, the focus is now shifted to a specific type of infrastructure system, namely a water distribution system and the flows are analysed using a hydraulic model (EPANET (U.S. Environmental Protection Agency 2008)) in a sample network, consisting of 15 nodes and 23 links (Figure 5.7(a)). A water distribution system has been chosen for this analysis, but another type of infrastructure system could equally have been chosen (an electrical distribution network, for example).

Weighted networks are not considered in this research (as they are deemed to be outside the scope) and therefore all links (pipes) are set to have the same value for each parameter (e.g. length, diameter, roughness coefficient). Again, it is assumed that the supply nodes have sufficient capacity to supply any service required and the demand nodes are assigned a value of demand based upon their initial degree (this demand does not change throughout the analysis, for example, if a connected node is removed, its degree will decrease but we keep the demand constant).

The proximity of a demand node to the supply node will have a large effect on the flows in the node (as previously explained, see Figure 5.4) and depending on the network architecture (class) this could lead to a disproportionately large influence on the overall behaviour of the network. To negate this effect, the concept of a "roving" supply node is introduced. This is implemented by conducting 15 series of tests on the sample network. In each test series there is only one supply node and the location of this is fixed (e.g. at node 1). The flows in the network are calculated and then one demand node is removed and the change in flows in the network is calculated (this is one simulation). This node is then replaced and another demand node is removed, again the changes in flow are calculated. This process is repeated until all demand

nodes have been removed (resulting in 14 simulations for this test series). At the end of a test series, the position of this supply node is 'moved' and the process is repeated. Again this process is repeated until all possible combinations have been tested and therefore all influences that the supply node can have on this particular network have been considered. It is worth noting that in this analysis the damage model is again binary, meaning that nodes cannot operate at a reduced level of capacity.

To quantify the change in flows in the network, when removing demand nodes, the square root of the sum of the squares (SRSS) is calculated for the change in flow through each node. For each of the test series the value is correlated with different measures to assess the predictive skill of these in identifying the important nodes in the network. Three measures (original flow, betweenness centrality and degree) and two combinations of these measures are used in this analysis, to determine if a combination of physically based and graph theory metrics has a superior predictive skill in identifying the important nodes in a network or whether these measures should be used in isolation. The first measure used is the original flow through the node (i.e. the calculated flow through the node before removing any nodes), this is a physically based metric that can be considered an indicator of the importance of a node in the network (i.e. the nodes with a high flow through them are more likely to have a large impact on the network when removed). This measure is therefore used as a benchmark for testing the predictive skills of graph theory metrics in choosing important nodes. Secondly, the degree of the node is used, as it could be argued that the most connected node is the most important in the network. The third measure is betweenness centrality (Equation 2.4), as flow will choose the shortest path between areas of supply / demand it could be argued that the measure which takes into account the number of shortest APL between pairs of other nodes to indicate the important nodes in the network. These measures are also combined to show that the predictive skill in identifying important nodes can be improved. The first of these combined measures uses original flow and betweenness centrality (Equation 5.10); the original flow takes into account the position of the supply node (i.e. the connected nodes will have a higher value of flow through them, Figure 5.4) and betweenness centrality considers the path of the flow through the network. To negate the effect of

node degree upon this relationship, the second combined measure divides this value by degree (Equation 5.11).

$$CM_1(j) = Q_j c(v_j) \quad 5.10$$

$$CM_2(j) = \frac{Q_j c(v_j)}{k_j} \quad 5.11$$

Where, in both Equations 5.10 and 5.11, *CM* refers to the combined measure, *Q* the flow through the node, *c(v)* the betweenness centrality, *k* the degree of the node and subscript *j* refers to the node in question.

For each simulation series the R^2 value for the correlation between the change in flow when a node is removed and each metric is calculated (i.e. it is the goodness of fit for the 14 simulations in each simulation series), shown in Figure 5.7(b).

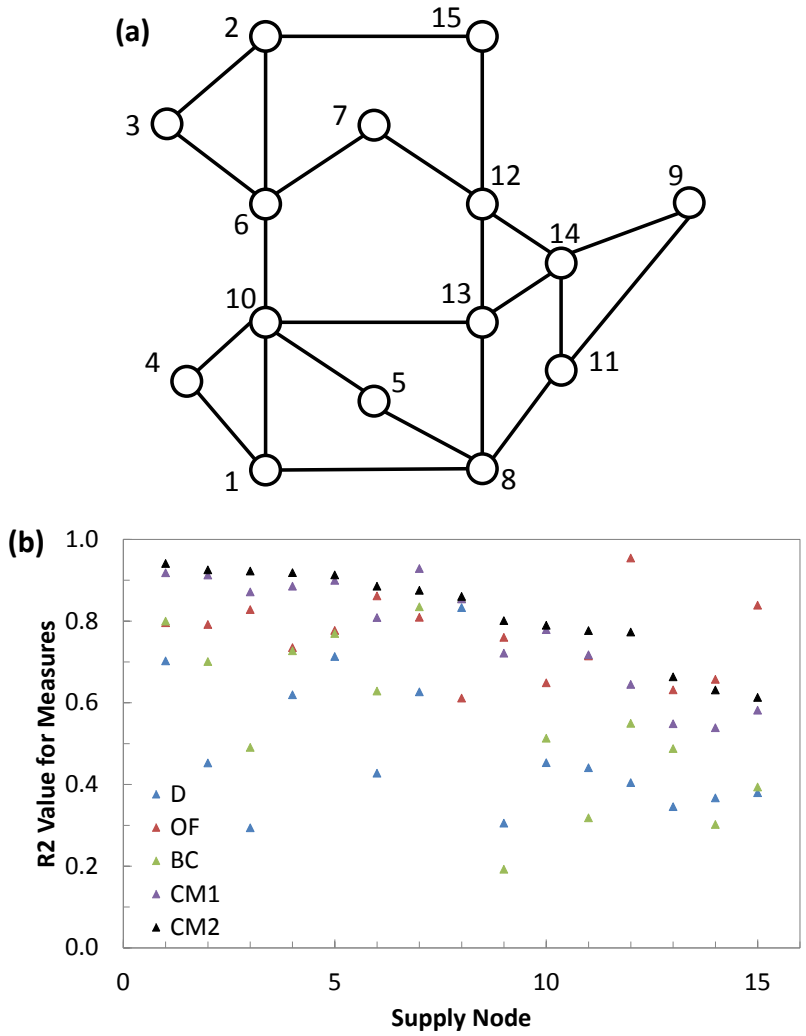


Figure 5.7: Showing (a) 15 node sample network (indicating node numbers), (b) a comparison of R^2 value for measures for each position of the supply node (where D = degree, OF = original flow, BC = betweenness centrality and CM the combined measure).

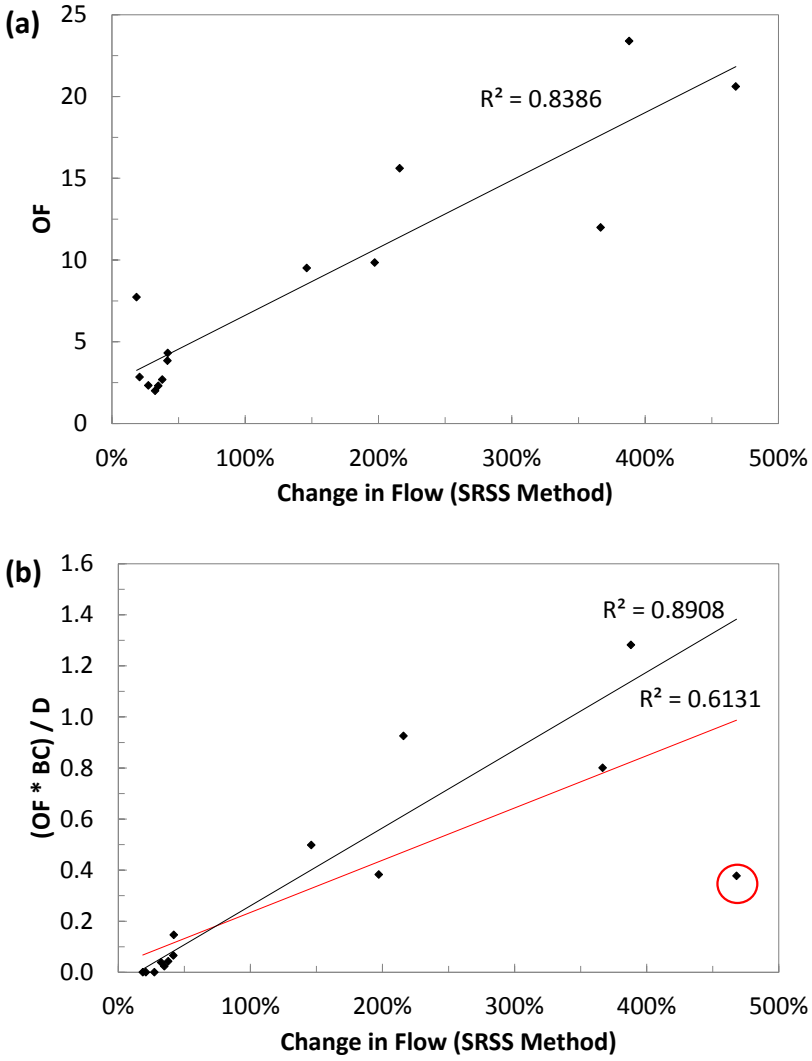


Figure 5.8: Showing (a) original flow and change in flow (calculated using SRSS method) with node 15 as the supply node, for the sample network shown in Figure 5.7, and (b) one combined measure and the change in flow (calculated using the SRSS method) with node 15 as the supply node, the red line is the linear line of best fit for all data points, and the black line is the line of best fit for all data points with the outlier removed (circled in red).

From the three individually applied measures it can be seen that the original flow (the baseline metric) is best at identifying 'critical' or vulnerable nodes (i.e. it is the most strongly correlated with change in flow) followed by betweenness centrality and finally degree. There is a reasonable amount of scatter in the R^2 values and so original flow is not universally the best indicator of vulnerable nodes; however, it has the least scatter associated with it and so the predictive skill of this metric can be said to be less affected by the position of the supply node.

Considering the two combined measures, it can be seen that the measure which includes all three individual measures is superior in predicting the important nodes in the network, for the majority of simulations (Figure 5.7(b)). The reason for this is that

flow based metrics indicate the important components in a network for a given supply / demand scenario, while graph theory metrics indicate the importance of components for a given network architecture. When a node is removed, the flows are redistributed and so the information provided by the flow metrics becomes less reliable. Graph theory metrics, on the other hand, provide information about the network in general and so are a better measure of the potential for node removal to have an effect.

Considering Figure 5.7(b), there are two locations of supply node which result in the original flow (baseline metric) being superior (node 12 and node 15). In the case of the supply node located at node 15, the removal of node 2 has a disproportionate effect to the remaining network (creating an SRSS value of around 450%). This effect is not reflected in the modified measures used, but is captured by the original flow measure because in this scenario the particular choice of supply and demand nodes overwhelms any effect that the network architecture has. Figure 5.8(a) shows the correlation between the change in flow and the original flow when the supply node is node 15. This figure shows a strong correlation between the two measures; however, plotting the change in flow against the second modified measure gives a significantly reduced correlation, due to the influence that the removal of node 2 has on the network (Figure 5.8(b)). Because node 2 was one of the two nodes connected to node 15, it had a large through flow (to enable supply of the other nodes in the network) resulting in a high value of original flow, but not the combined measure (as node 2 has a small degree and a low value of betweenness centrality). This results in the combined metrics making a significant underestimation of the importance of this node to the network. This illustrates that although the proposed metrics do result in a superior ability to identify important nodes in a network, they are not infallible.

This chapter has focused on the impact that the removal of a single node can have to the functioning of the remaining network and has developed methods to identify individual nodes that have a disproportionate effect to the remaining network when removed (i.e. 'critical' nodes). A reduced complexity flow model was developed, as it was initially desirable to analyse infrastructure systems governed by physically based rules in general. This model was used to model the flow around a series of networks

and it was found that there was a strong correlation between physically based measures and graph theory metrics for scale-free and exponential networks, with R^2 measures around 0.7-0.9, meaning that network theory is suitable for the analysis of these systems.

Once the applicability of using network metrics was established, the predictive skill of using these metrics to identify 'critical' nodes in an infrastructure system was assessed. The predictive skill of three measures (original flow, betweenness centrality and degree) and two combinations of these measures were assessed, to determine if a combination of physically based measures and network theory metrics improved the predictive skill of identifying 'critical' nodes, rather than using these measures in isolation. These measures were applied to a sample water distribution system, where the flow was modelled using a hydraulic model. The flow around the network was calculated and then recalculated as each node was removed from the network, in turn. The change in flow between these two simulations was assessed using the SRSS method and correlated with the measures to show which had the best predictive skill at identifying 'critical' nodes. From this analysis, it was concluded that a combination of these measures showed the highest predictive skill. This is due to the physically based measures accounting for the transfer of service around the system and the graph theory metrics considering the connectivity of the system. However, it was shown that this method is not infallible, as for some instances the removal of a node can cause a dramatic change in the flow to the remaining nodes in the system (captured by the original flow metric) but a negligible impact to the network architecture (causing the betweenness centrality measure to underestimate the impact of this node removal).

CHAPTER 6: CONCLUSIONS

This chapter presents the key findings of this research, discusses their utility and potential implications, and also suggests recommendations for future research. For a detailed summary of the methodology and discussion of results the reader is directed to the conclusions that were provided at the end of each chapter.

6.1: MAIN FINDINGS

The aim of this research was 'to improve the resilience of our communities by developing techniques that can identify fragile system architectures, recognize vulnerable areas within these systems and establish methods that can help to protect them from hazard'. To achieve this, a network graph theory approach was used to analyse infrastructure systems and quantify the impact that damage to these systems has on the communities, and members of society, that rely on them. The main findings of this research are now presented along with a discussion of their potential utility and implications for both informing infrastructure owners and operators of potential deficiencies within their systems and also informing future research.

The main finding of this research has shown that topological graph theory models can give a false indication of the resilience of an infrastructure system. A topological network theory approach has previously been used, in other studies, to analyse infrastructure networks and these studies have tended to focus on classifying the system into a network class, from which an assessment of the systems hazard tolerance can be made. However, this research has found that this analysis approach can be deficient when used to form an assessment of the hazard tolerance of an infrastructure system, due to the spatial component associated with these networks. This deficiency was initially shown by quantifying the disruption caused to the EATN by the Eyjafjallajökull volcanic event (as discussed in Chapter 3.1). To determine whether this vulnerability was unique to the EATN, or was characteristic of its network class, synthetic networks with the same topological and spatial characteristics as the EATN were formed. This was achieved by developing a new network generation algorithm

which was capable of replicating both the topological and spatial characteristics of a network (Chapter 3.2). To the best of the authors' knowledge this is the first time that a fully synthetic proxy network has been generated and validated. These synthetic networks were subjected to the same Eyjafjallajökull volcanic event, to which they also showed an increased vulnerability compared to a benchmark network. The hazard tolerance of two further air traffic networks was also assessed (Chapter 3.3) and from this analysis it was concluded that the vulnerability shown by a spatial network is due to a combination of network class, nodal configuration and also the location of the highly connected 'hub' airports in relation to the spatial hazard. The spatial component of both the network and hazard is not accounted for in topological network models, which in this case were shown to give a false indication of the hazard tolerance of air traffic networks. This finding has important implications for the owners and operators of these systems, as their network architecture suggests that they should be resilient to a random hazard; however this research has shown that they can be particularly vulnerable to some locations of spatial hazard. This finding also has implications for previous studies which have used purely topological network models to analyse spatial systems; as any findings relating to the hazard tolerance of these networks may be false and networks that were assumed to be resilient to a random hazard (as a result of their network architecture) may in fact by highly vulnerable to some locations, and sizes, of spatial hazard. Therefore, it is not advised to use only topological models when forming an assessment of the hazard tolerance of a network which is distributed over a geographical area.

To assess the potential implications of this finding to owners and operators of other infrastructure systems, a range of synthetic networks (with similar characteristics to infrastructure systems) were formed and subjected to a range of spatially coherent random hazards (Chapter 4). Although this analysis used synthetic networks, they could be utilised by the owners and operators of infrastructure systems to form an initial assessment of the resilience of their network. The analysis of these synthetic networks identified three main factors which affect the hazard tolerance of a spatial network: (1) the location of the highly connected components (Chapter 4.3), (2) the location of the spatial hazard (Chapter 4.4), and (3) the location of network components (Chapter 4.5). These findings have many important implications for the

owners and operators of infrastructure systems, who should take note of the spatial location of both their components and highly connected components (particularly in relation to potential spatial hazards), as these can have a dramatic effect to the hazard tolerance of the system. Infrastructure systems which have formed around a relatively uniform population density are likely to be spatially dispersed and will therefore have a similar resilience to all locations of spatial hazard. However, infrastructure systems which have formed around a single area of high population density are likely to form a non-uniform configuration centred around this area of high density. This research has shown that these networks are particularly vulnerable to hazards located over this high density area, causing not only a disproportionally large number of connections to be removed but also a disproportionate drop in the connectivity of the network and potentially a decrease in the efficiency of the network. However, this nodal configuration can also cause these networks to show an increased resilience to hazards located away from this high density area. Therefore, infrastructure owners with systems that have formed around one area of high population density should be aware of both the potential location and size of any spatial hazards in relation to this area.

This research has also found that there are some components, within infrastructure systems, that can cause a disproportionate impact to the functioning of the remaining network when removed (Chapter 5). To identify these components, this research coupled a network model with a hydraulic model and analysed the predictive skill of various measures at identifying these critical components (Chapter 5.3). It was found that a combination of network theory and physically based measures showed the best predictive skill at identifying these components. This finding could be utilised by the owners and operators of infrastructure systems to identify their critical components (i.e. those that when removed will have a large impact to the functioning of the remaining system) and could potentially be used to inform strategies to decrease the impact that the removal of these components has to the functioning of the network (aiming to increase the resilience of the network overall).

To conclude, this research has developed a new network generation algorithm capable of forming both the topological and spatial characteristics of a real world network and has used this to prove that a spatial element is crucial for determining the hazard tolerance of real world infrastructure networks. This research has also shown that

there are some components within infrastructure systems that when removed have a disproportionate impact to the functioning of the remaining network and that a combination of network theory and physically based measures shows the most predictive skill at identifying these nodes. However, to keep this research to a manageable size the scope of the research was restricted; whilst this is deemed to have had little effect to the main findings of this research, further studies should seek to incorporate these limitations into their research.

6.2: POSSIBLE FUTURE WORK

From this research, several areas for future work have been identified:

- Generic networks, with different topological and spatial characteristics, were developed and analysed in this research due to the lack of complete and obtainable datasets for real world infrastructure systems. However, further work should consider how these datasets may be obtained for specific infrastructure systems.
- Weighted network models were deemed to be outside the scope of this research; however, their inclusion would allow the proportion of cancelled flights and passengers to be quantified (rather than only considering the disruption to air routes). Therefore, future research in this area should consider developing weighted spatial network models of the air traffic networks and should also consider methods for including this weight into the generation algorithms used to form synthetic networks.
- These weighted networks could also be combined with the reduced complexity flow model to allow components with different properties to be modelled (e.g. pipes with different diameters). This would also allow the predictive skill of the combined measures to be assessed for networks with different properties (as the betweenness centrality value would need to be altered to account for this weighted component).
- This research has identified 'critical' nodes in a 15-node sample system; further work should consider using the same method to analyse larger networks (with a higher number of nodes and links) and also a larger number of networks.

- The damage models in this research were all binary models where a node either passed or failed (i.e. components could not operate at a reduced capacity). Future research in this area should consider using non-binary models particularly when considering the hazard tolerance of a flow based network. In this case, more sophisticated damage models could be used to describe the relationship between the damage to a component and its ability to provide a level of service. For example, a water treatment plant could become damaged in a hazard; however it could be capable of providing some level of service, which has not been considered in this research.
- This research has focused on the impact that the removal of nodes, and their connecting links, has to the functioning of a network (as the removal of a node is likely to cause a more significant impact to the network, than the removal of a single link). However, in real world infrastructure networks both nodes (components) and links (connections) are vulnerable to the effects of a hazard. Therefore, future research could consider the impact that the removal of nodes and links (other than those connected to the removed nodes) has to the remaining network. This future research could also seek to identify which links, when removed, have a disproportionate impact to the functioning of the remaining network (i.e. 'critical' links).
- This research has considered the application of spatial hazards to network models in general. However further work, should consider the categorisation of other real world infrastructure networks (into network classes) and either confirm or establish their evolutionary rules, as well as analysing specific threats to these networks (e.g. a likely flooding scenario).
- This research has developed adaptation strategies that are capable of increasing the resilience of infrastructure systems where the links can be 'rewired'. However, this is not the case in some infrastructure systems; for example, the pipes in a water distribution system cannot be easily moved. Further research should consider adaptation strategies that can increase the resilience of these systems to spatial hazards, without compromising their efficiency under normal operational conditions. This could consider additional capacity that should be given to components to allow the provision of service to be redistributed around the system in the event of hazard, or additional

storage tanks to provide some service to communities that have been ‘cut off’ until they can be reconnected.

REFERENCES

Albert, R., Albert, I. and Nakarado, G. L. (2004). "Structural vulnerability of the North American power grid." Physical Review E **69**.

Albert, R. and Barabasi, A. L. (2002). "Statistical mechanics of complex networks." Reviews of Modern Physics **74**(1): 47-97.

Albert, R., Jeong, H. and Barabasi, A. L. (1999). "Internet - Diameter of the World-Wide Web." Nature **401**(6749): 130-131.

Albert, R., Jeong, H. and Barabasi, A. L. (2000). "Error and Attack Tolerance of Complex Networks." Nature **406**(6794): 378-382.

Alexander, C. K. and Sadiku, M. N. O. (2009). Fundamentals of Electric Circuits. 4th Edition. New York, NY, McGraw-Hill.

Amandeo, K. (2011). "Impact of Japan's Earthquake on the Economy." Retrieved 7 October 2011, from http://useconomy.about.com/od/criticalssues/a/Japan-Earthquake.htm.

Amaral, L. A. N., Scala, A., Barthelemy, M. and Stanley, H. E. (2000). "Classes of small-world networks." Proceedings of the National Academy of Sciences of the United States of America **97**(21): 11149-11152.

ArcGIS. (2013). "ArcGIS Resource Centre: Europe." Retrieved 6 February 2013, from http://resources.arcgis.com/.

Arenas, A., Danon, L., Diaz-Guilera, A., Gleiser, P. M. and Guimera, R. (2003). "Community Analysis in Social Networks." European Physical Journal B **38**(2): 373-380.

Australian Government (2010). Critical Infrastructure Resilience Strategy.

Aven, T. (2011). "On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience." Risk Analysis **31**(4): 515-522.

Bagler, G. (2008). "Analysis of the airport network of India as a complex weighted network." Physica a-Statistical Mechanics and Its Applications **387**(12): 2972-2980.

Baldick, R., Chowdhury, B., Dobson, I., Zhaoyang, D., Bei, G., Hawkins, D., Zhenyu, H., Manho, J., Janghoon, K., Kirschen, D., Lee, S., Fangxing, L., Juan, L., Zuyi, L., Chen-Ching, L., Xiaochuan, L., Mili, L., Miller, S., Nakayama, M., Papic, M., Podmore, R., Rossmaier, J., Schneider, K., Hongbin, S., Kai, S., Wang, D., Zhigang, W., Liangzhong, Y., Pei, Z., Wenjie, Z. and Xiaoping, Z. (2009). Vulnerability assessment for cascading failures in electric power systems. Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES.

Barabasi, A.-L. and Oltvai, Z. N. (2004). "Network biology: understanding the cell's functional organization." Nat Rev Genet **5**(2): 101-113.

Barabasi, A. L. (2013). "Network Science." Philosophical Transitions of The Royal Society(371).

Barabasi, A. L. and Albert, R. (1999). "Emergence of scaling in random networks." Science **286**(5439): 509-512.

Barabasi, A. L., Albert, R. and Jeong, H. (2000). "Scale-free characteristics of random networks: the topology of the World-Wide Web." Physica A **281**(1-4): 69-77.

Barabasi, A. L. and Bonabeau, E. (2003). "Scale-Free Networks." Scientific American: 50-59.

Barthelemy, M. (2011). "Spatial networks." Physics Reports-Review Section of Physics Letters **499**(1-3): 1-101.

Batagelj, V. and Mrvar, A. (2003). Pajek - Program for Large Network Analysis. http://vlado.fmf.uni-lj.si/pub/networks/pajek.

Batagelj, V. and Brandes, U. (2005). "Efficient generation of large random networks." Physical Review E **71**(3).

BBC. (2008). "Flooding 'action plan' promised." Retrieved 26 June 2013, from http://news.bbc.co.uk/1/hi/uk/7473463.stm.

Bianconi, G. and Barabasi, A. L. (2001a). "Bose-Einstein Condensation in Complex Networks." Physical Review Letters **86**(24): 5632-5635.

Bianconi, G. and Barabasi, A. L. (2001b). "Competition and Multiscaling in Evolving Networks." Europhysics Letters **54**(4): 436-442.

Boas, P. R. V., Rodrigues, F. A. and Costa, L. D. (2009). "Modeling worldwide highway networks." Physics Letters A **374**(1): 22-27.

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M. and Hwang, D. U. (2006). "Complex networks: Structure and dynamics." Physics Reports-Review Section of Physics Letters **424**(4-5): 175-308.

Bompard, E., Wu, D. and Xue, F. (2011). "Structural vulnerability of power systems: A topological approach." Electric Power Systems Research **81**(7): 1334-1340.

British Geological Survey (2012a). Coastal Erosion.

British Geological Survey (2012b). Volcanic Hazards.

British Geological Survey (2013a). "Significant British Earthquakes." Retrieved 20 August 2013, from http://www.earthquakes.bgs.ac.uk/earthquakes/UKsignificant/index.html.

British Geological Survey (2013b). "A Revised Seismic Hazard Map for the UK." Retrieved 20 August 2013, from http://news.bbc.co.uk/1/hi/7266136.stm.

Brooker, P. (2010). "Fear in a Handful of Dust: Aviation and the Icelandic Volcano." Significance **3**: 112-115.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A. and von Winterfeldt, D. (2003). "A framework to quantitatively assess and enhance the seismic resilience of communities." Earthquake Spectra **19**(4): 733-752.

Bruneau, M. and Reinhorn, A. M. (2007). "Exploring the Concept of Seismic Resilience for Acute Care Facilities." Earthquake Spectra **23**(1): 41-62.

Bullmore, E. and Sporns, O. (2009). "Complex brain networks: graph theoretical analysis of structural and functional systems." Nature Reviews Neuroscience **10**(3): 186-198.

Cabinet Office (2008a). National Risk Register. Cabinet Office. London.

Cabinet Office (2008b). The National Security Strategy of the United Kingdom: Security in an Interdependent World. Cabinet Office. London.

Cabinet Office (2008c). The Pitt Review: Learning Lessons from the 2007 Floods. Cabinet Office. London.

Cabinet Office (2010a). Strategic Framework and Policy Statement: on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. Cabinet Office. London.

Cabinet Office (2010b). Summary of Consultation Responses: Summary of Responses to the Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. Cabinet Office. London

Cabinet Office (2010c). Sector Resilience Plans for Critical National Infrastructure. Cabinet Office. London.

Cabinet Office (2011a). Keeping the Country Running: Natural Hazards and Infrastructure (For Consultation). Cabinet Office. London.

Cabinet Office (2011b). Keeping the Country Running: Natural Hazards and Infrastructure. Cabinet Office. London.

Cabinet Office (2011c). A Summary of the: Sector Resilience Plans for Critical Infrastructure 2010/2011. Cabinet Office. London.

Cabinet Office (2012a). National Risk Register of Civil Emergencies 2012. Cabinet Office. London.

Cabinet Office (2012b). A Summary of the 2012 Sector Resilience Plans. Cabinet Office. London.

Cabinet Office (2013). National Risk Register of Civil Emergencies 2013. Cabinet Office. London.

Cadini, F., Zio, E. and Petrescu, C.-A. (2009). Using Centrality Measures to Rank the Importance of the Components of a Complex Network Infrastructure. Critical Information Infrastructure Security. R. Setola and S. Geretshuber, Springer Berlin / Heidelberg. **5508:** 155-167.

Canadian Energy Issues (unknown). Ice-ravaged electricity transmission towers.

Carrington, P. J., Scott, J., Wasserman, S. and Granovetter, M. (2005). Models and Methods in Social Network Analysis. New York, USA, Cambridge University Press.

Carvalho, R., Buzna, L., Bono, F., Gutierrez, E., Just, W. and Arrowsmith, D. (2009). "Robustness of trans-European gas networks." Physical Review E **80**(1).

Censky, A. (2011). "Japan Earthquake Could Cost $309 Billion." Retrieved 13 October 2011, from http://money.cnn.com/2011/03/23/news/international/japan_earthquake_cost/index.htm.

Chang, H. S. and Shinozuka, M. (2004). "Measuring Improvements in the Disaster Resilience of Communities." Earthquake Spectra **20**(3): 739-755.

Chang, L. and Wu, Z. G. (2011). "Performance and reliability of electrical power grids under cascading failures." International Journal of Electrical Power & Energy Systems **33**(8): 1410-1419.

China Travel Go. (2013). "Maps of China." Retrieved 25 October, 2013, from http://chinatravelgo.com/maps-of-china/.

Clarke, K. C. and Gaydos, L. (1998). "Loose-coupling a cellular automaton model and GIS: long-term urban growth prediction for San Francisco and Washington/Baltimore." International Journal of Geographical Information Science **12**(7): 699-714.

Clarke, K. C., Hoppen, S. and Gaydos, L. (1995). "A self-modifying cellular automation model of historical urbanisation in the San Francisco Bay area." Environment and Planning B-Planning & Design **24**: 27-261.

Cohen, R., Erez, K., ben-Avraham, D. and Havlin, S. (2000). "Resilience of the Internet to random breakdowns." Physical Review Letters **85**(21): 4626-4628.

Cohen, R., Erez, K., ben-Avraham, D. and Havlin, S. (2001). "Breakdown of the internet under intentional attack." Physical Review Letters **86**(16): 3682-3685.

Cohen, R. and Havlin, S. (2010). Complex Networks: Structure, Robustness and Function. 1st Edition. New York, USA, Cambridge University Press.

Comfort, L. (1999). Shared Risk: Complex Systems in Seismic Response. 1st Edition. New York, Pergamon.

Costa, L. F., Oliveira, O. N., Travieso, G., Rodrigues, F. A., Boas, P. V., Antiqueira, L., Viana, M. and Rocha, L. E. C. d. (2011). "Analyzing and Modeling Real-World

Phenomena with Complex Networks: A Survey of Applications." Advances in Physics **60**(3): 329-412.

Council for Science and Technology (2009). A National Infrastrucvture for the 21st Century.

Crucitti, P., Latora, V. and Marchiori, M. (2004a). "Model for cascading failures in complex networks." Physical Review E **69**(4).

Crucitti, P., Latora, V. and Marchiori, M. (2004b). "A topological analysis of the Italian electric power grid." Physica a-Statistical Mechanics and Its Applications **338**(1-2): 92-97.

Crucitti, P., Latora, V. and Porta, S. (2006). "Centrality measures in spatial networks of urban streets." Physical Review E **73**.

da Rocha, L. E. C. (2009). "Structural evolution of the Brazilian airport network." Journal of Statistical Mechanics-Theory and Experiment. **2009**(4).

DCSINT (2006). Critical Infrastructure Threats and Terrorism.

de Nooy, W., Mrvar, A. and Batagelj, V. (2005). Exploratory Social Network Analysis with Pajek. 1st Edition. Cambridge, Cambridge University Press.

DEFRA Flood Management (2005). The Threat Posed by Tsunami to the UK.

Deng, W., Li, W., Cai, X. and Wang, Q. A. (2011). "The exponential degree distribution in complex networks: Non-equilibrium network theory, numerical simulation and empirical data." Physica A: Statistical Mechanics and its Applications **390**(8): 1481-1485.

Dickson, M., M. Walkden, and J. Hall (2006). Modelling the impacts of climate change on an eroding coast over the 21st Century. Tyndall Centre.

Dunne, J. A., Williams, R. J. and Martinez, N. D. (2002). "Food-web structure and network theory: The role of connectance and size." PNAS **99**(20): 12917-12922.

Ebdon, D. (1977). Statistics in Geography. 2nd Edition. Oxford, Blackwell Publishers.

edigitalz.COM. (2012). "World Digital Data." Retrieved 30 August 2012, from http://www.edigitalz.com/.

Elvidge, C. (2003). Blackout leaves American cities in the dark. [Photograph]. Retrieved 13 May 2011, from http://earthobservatory.nasa.gov/IOTD/view.

Environment Agency (2007). Review of 2007 Summer Floods.

Environment Agency (2009). Flooding in England: A National Assessment of Flood Risk.

Environment Agency (2010a). The Costs of the Summer 2007 Floods in England.

Environment Agency (2010b). Assessment of Coastal Erosion and Landsliding for the Funding of Coastal Risk Management Projects.

Environment Agency (2011). Understanding the risks, empowering communities, building resilience: The national flood and coastal erosion risk management strategy for England.

Erdos, P. and Renyi, A. (1960). "On The Evolution of Random Graphs." Publication of the Mathematical Institutre of the Hungarian Academy of Sciences **5**: 17-61.

Eurocontrol (2010). Monthly Network Operations Report: April 2010

Everett, M. G. and Borgatti, S. P. (1999). "The centrality of groups and classes." Journal of Mathematical Sociology **23**(3): 181-201.

FlowingData. (2009). "Growth of Target." Retrieved 30 August 2012, from http://flowingdata.com.

FlowingData. (2010). "Growth of Wal-Mart." Retrieved 30 August 2012, from http://flowingdata.com.

Freeman, L. C. (1979). "Centrality in Social Networks Conceptual Clarifiation." Social Networks **1**(3): 215-239.

Gastner, M. T. and Newman, M. E. J. (2006a). "Optimal design of spatial distribution networks." Physical Review E **74**(1).

Gastner, M. T. and Newman, M. E. J. (2006b). "The spatial structure of networks." European Physical Journal B **49**(2): 247-252.

GfK GeoMarketing (2013). Population Density: Europe 2011/2012.

Glendinning, P. (2012). Maths in Minutes: 200 Key Concepts Explained in an Instant. 1st Edition. London, UK, Quercus Editions Ltd.

Graff, T. O. (1998). "The Locations of Wal-Mart and Kmart Supercenters: Contrasting Corporate Strategies." Professional Geographer **50**(1): 46-57.

Graff, T. O. and Ashton, D. (1993). "Spatial Diffusion of Wal-Mart: Contagious and Reverse Hierarchical Elements." Professional Geographer **46**(1): 19-29.

Gray, B. H. and Herbert, K. (2006). After Katrina: Hospitals in Hurricane Katrina - Challenges Facing Custodial Institutions in a Disaster.

Grayman, W. M. (2006). "Use of Distribution System Water Quality Models in Support of Water Security." Security of Water Supply Systems **8**: 39-50.

Great Britian (2004). Civil Contingencies Act 2004. The Stationery Office. London.

Guida, M. and Maria, F. (2007). "Topology of the Italian Airport Network: A scale-free small-world network with a fractal structure?" Chaos Solitons & Fractals **31**(3): 527-536.

Guimera, R. and Amaral, L. A. N. (2004). "Modeling the world-wide airport network." European Physical Journal B **38**(2): 381-385.

Guimera, R., Mossa, S., Turtschi, A. and Amaral, L. A. N. (2005). "The worldwide air transportation network: Anomalous centrality, community structure, and cities'

global roles." Proceedings of the National Academy of Sciences of the United States of America **102**(22): 7794-7799.

Haimes, Y. Y. (2009). "On the Definition of Resilience in Systems." Risk Analysis **29**(4). 498-501.

Han, D. D., Qian, J. H. and Liu, J. G. (2009). "Network topology and correlation features affiliated with European airline companies." Physica A-Statistical Mechanics and Its Applications **388**(1): 71-81.

Heathrow Winter Resilience Enquiry (2011). Report of the Heathrow Winter Resilience Enquiry.

Hines, P., Cotilla-Sanchez, E. and Blumsack, S. (2010). "Do topological models provide good information about electricity infrastructure vulnerability?" Chaos **20**(3).

HM Treasury and Infrastructure UK (2010). National Infrastructure Plan. The Stationery Office Limited. London.

Holling, C. S. (1973). "Resilience and Stability of Ecological Systems." Annual Review of Ecology and Systematics **4**: 1-23.

Hollingshead, M. (2007). Northwest Missouri Ice Storm.

Holmes, T. J. (2011). "The Diffusion of Wal-Mart and Economies of Density." Econometrica **79**(1): 253-302.

Holmgren, A. J. (2006). "Using Graph Models to Analyze the Vulnerability of Electric Power Networks." Risk Analysis **26**(4): 955-969.

Homeland Security Advisory Council (2011). Community Resilience Task Force Recommendations.

Institution of Civil Engineers (2009). The State of the Nation: Defending Critical Infrastructure.

Jenelius, E., Petersen, T. and Mattsson, L. G. (2006). "Importance and exposure in road network vulnerability analysis." Transportation Research Part a-Policy and Practice **40**(7): 537-560.

Jolly, D. and Werdigier, J. (2010). Snow Hampers Travel in Europe. The New York Times. Retrieved 28 October 2010, from http://www.nytimes.com/2010/12/21/world/europe/21snow.html?pagewanted=all&_r=0.

Kinney, R., Crucitti, P., Albert, R. and Latora, V. (2005). "Modeling cascading failures in the North American power grid." The European Physical Journal B - Condensed Matter and Complex Systems **46**(1): 101-107.

Latora, V. and Marchiori, M. (2002). "Is the Boston subway a small-world network?" Physica a-Statistical Mechanics and Its Applications **314**(1-4): 109-113.

Lee, D. S., Park, J., Kay, K. A., Christakis, N. A., Oltvai, Z. N. and Barabasi, A. L. (2008). "The implications of human metabolic network topology for disease

comorbidity." Proceedings of the National Academy of Sciences of the United States of America **105**(29): 9880-9885.

Lewis, T. G. (2009). Network science: theory and practice. 1st Edition. New Jersey, USA, John Wiley & Sons.

Li, W. and Cai, X. (2004). "Statistical analysis of airport network of China." Phys Rev E Stat Nonlin Soft Matter Phys **69**(4 Pt 2): 046106.

Li, W., Wang, Q. A., Nivanen, L. and Le Mehaute, A. (2006). "How to fit the degree distribution of the air network?" Physica a-Statistical Mechanics and Its Applications **368**(1): 262-272.

Liu, J. Z. and Tang, Y. F. (2005). "An exponential distribution network." Chinese Physics **14**: 643-645.

Liu, Y. (2009). Modelling Urban Development with Geographical Information Systems and Cellular Automata. 1st Edition. Florida,US, CRC Press.

Lloyd's (2010). Space Weather: Its impact on Earth and implications for businesses.

Magnien, C., Latapy, M. and Guillaume, J. L. (2011). "Impact of Random Failures and Attacks on Poisson and Power-Law Random Networks." Acm Computing Surveys **43**(3).

MapofUSA.net. (2013). "Map of the USA." Retrieved 25 October, 2013, from http://www.mapofusa.net/us-population-density-map.htm.

Mazzocchi, M., Hansstein, F. and Ragona, M. (2010). "The 2010 Volcanic Ash Cloud and its Financial Impact on the European Airline Industry." CESifo Forum **11**: 92-100.

McColl, L., Palin, E. J., Thornton, H. E., Sexton, D. M. H., Betts, R. and Mylne, K. (2013). "Assessing the potential impact of climate change on the UK's electricity network." Climate Change **14**(1): 821-835.

Met Office (2011). "Case Study: Winter 2009/10." Retrieved 9 August 2013, from http://www.metoffice.gov.uk/about-us/who/how/case-studies/winter09-10.

Met Office (2012). "Heavy Rainfall / Flooding in the Lake District, Cumbria – November 2009". Retrieved 9 August 2013, from : http://www.metoffice.gov.uk/climate/uk/nov2009.

Met Office (2013). "Severe Gales. " Retrieved 9 August 2013, from http://www.metoffice.gov.uk/weather/uk/advice/storm.html.

Milgram, S. (1967). "The Small-World Problem." Psychology Today **1**(1): 61-67.

Murray, A. and Grubesic, T. (2007). Critical Infrastructure: Reliability and Vulnerability. 1st Edition. Leipzig, Germany, Springer.

NASA (2009). "The Day the Sun Brought Darkness. " Retrieved 9 August 2013, from http://www.nasa.gov/topics/earth/features/sun_darkness.html.

Network Workbench (2009). Network Workbench Tool: User Manual 1.0.0.

New Civil Engineer (2013). Clarke to head up infrastructure project. New Civil Engineer (24.10.13): 29.

New Zealand Government (2010). National Infrastructure Plan.

Newman, M. E. J. (2003). "The structure and function of complex networks." Siam Review **45**: 167-256.

Newman, M. E. J., Watts, D. J. and Strogatz, S. H. (2002). "Random graph models of social networks." Proceedings of the National Academy of Sciences of the United States of America **99**: 2566-2572.

Newman, M. E. J. (2004). "Analysis of weighted networks." Physical Review E **70**(5): 056131.

Nojima, N. (2006). Evaluation of Functional Performance of Complex Networks for Critical Infrastructure Protection. First European Conference on Earthquake Engineering and Seismology. Geneva, Switzerland.

Northumberland Gazette (2013). "Landslide road will not re-open for a year. " Retrieved 15 August 2013, from http://www.northumberlandgazette.co.uk/news/local-news/landslide-road-will-not-re-open-for-a-year-1-5432455.

Novak, P., Guinot, V., Jeffrey, A. and Reeve, D. E. (2010). Hydraulic Modelling - An Introduction: Principles, Methods and Applications. 1st Edition. London and New York, Spon Press.

NWB Team. (2006). Network Workbench Tool. Indiana University, Northeastern University and University of Michigan. http://nwb.cns.iu.edu.

OFWAT (2007). Water and sewerage services during the summer 2007 floods.

Openflights. (2010). "OpenFlights.org." Retrieved 13 August, 2010, from http://openflights.org/.

Opsahl, T., Agneessens, F. and Skvoretz, J. (2010). "Node centrality in weighted networks: Generalizing degree and shortest paths." Social Networks **32**(3): 245-251.

O'Rourke, T. D. (2007). "Critical Infrastructure, Interdependencies, and Resilience." The Bridge. 22-29

Osiadacz, A. J. (1987). Simulation and Analysis of Gas Networks. 1st Edition. London, UK, E. & F. N. Spon.

Ouyang, M. and Duenas-Osorio, L. (2012). "Time-dependent resilience assessment and improvement of urban infrastructure systems." Chaos **22**(3).

Ouyang, M., Duenas-Osorio, L. and Min, X. (2012). "A three-stage resilience analysis framework for urban infrastructure systems." Structural Safety **36-37**: 23-31.

Oxford Dictionaries. (2012). "Oxford Dictionaries." Retrieved 14 January 2013, from http://oxforddictionaries.com/.

Pansini, A. J. (2005). Guide to Electrical Power Distribution Systems. 6th Edition. Lilburn, GA, The Fairmont Press, Inc.

Paoletti, T. (2013). "Leonard Euler's Solution to the Konigsberg Bridge Problem." Retrieved 8 April 2013, from http://mathdl.maa.org/mathDL/.

Pastor-Satorras, R., Vazquez, A. and Vespignani, A. (2001). "Dynamical and correlation properties of the Internet." Physical Review Letters **87**(25).

Petersen, G. N. (2010). "A short meteorological overview of the Eyjafjallajokull eruption 14 April-23 May 2010." Weather **65**(8): 203-207.

Qian, J. H. and Han, D. D. (2009). "A spatial weighted network model based on optimal expected traffic." Physica a-Statistical Mechanics and Its Applications **388**(19): 4248-4258.

Reed, D. A., Kapur, K. C. and Christie, R. D. (2009). "Methodology for Assessing the Resilience of Networked Infrastructure." IEEE Systems Journal **3**(2): 174-180.

Risk Management Solutions. (2007). The Great Storm of 1987: 20-Year Retrospective.

Robertson, N., Sanders, D. P., Seymour, P. and Thomas, R. (2007). "The Four Color Theorem." from http://people.math.gatech.edu/.

Rogers, P. (2011). "Development of Resilient Australia: enhancing the PPRR approach with anticipation, assessment and registration of risks." The Australian Joural of Emergency Management **26**(1): 54-58.

Rosas-Casals, M., Valverde, S. and Sole, R. V. (2006). "Topological Vulnerability of the European Power Grid under Errors and Attacks." International Journal of Bifurcation and Chaos **17**(7): 2465-2475.

Rothenberg, R. B., Potterat, J. J., Woodhouse, D. E., Darrow, W. W., Muth, S. Q. and Klovdahl, A. S. (1995). "Choosing a centrality measure: Epidemiologic correlates in the Colorado Springs study of social networks." Social Networks **17**(3–4): 273-297.

Royal Academy of Engineering (2013). Extreme space weather: impacts on engineered systems and infrastructure.

Rual, J.-F., Venkatesan, K., Hao, T., Hirozane-Kishikawa, T., Dricot, A., Li, N., Berriz, G. F., Gibbons, F. D., Dreze, M., Ayivi-Guedehoussou, N., Klitgord, N., Simon, C., Boxem, M., Milstein, S., Rosenberg, J., Goldberg, D. S., Zhang, L. V., Wong, S. L., Franklin, G., Li, S., Albala, J. S., Lim, J., Fraughton, C., Llamosas, E., Cevik, S., Bex, C., Lamesch, P., Sikorski, R. S., Vandenhaute, J., Zoghbi, H. Y., Smolyar, A., Bosak, S., Sequerra, R., Doucette-Stamm, L., Cusick, M. E., Hill, D. E., Roth, F. P. and Vidal, M. (2005). "Towards a proteome-scale map of the human protein-protein interaction network." Nature **437**(7062): 1173-1178.

Sallam, A. A. and Malik, O. P. (2011). Electrical Distribution Systems: Planning and Utilisation. 1st Edition. Hoboken, New Jersey, John Wiley & Sons Inc.

Sen, P., Dasgupta, S., Chatterjee, A., Sreeram, P. A., Mukherjee, G. and Manna, S. S. (2003). "Small-world properties of the Indian railway network." Physical Review E **67**(3).

Sole, R. V., Rosas-Casals, M., Corominas-Murtra, B. and Valverde, S. (2008). "Robustness of the European power grids under intentional attack." Physical Review E **77**(2).

Sporns, O. (2002). "Network analysis, complexity, and brain function." Complexity **8**(1): 56-60.

Stam, C. J. and Reijneveld, J. C. (2007). "Graph Theoretical Analysis of Complex Networks in the Brain." Nonlinear Biomedical Physics **1**(3): 1-19.

Synolakis, C., Okal, E., and Bernard, E., (2005). *The Megatsunami of December 26, 2004.* The Bridge, **35**(2): p. 26-35.

The Guardian. (2010). "Cockermouth, a year on from the floods. " Retrieved 9 August 2013, from http://www.theguardian.com/society/2010/nov/16/cockermouth-cumbria-floods-first-anniversary.

The Institution of Professional Engineers New Zealand (2012). A Safer New Zealand: Reducing our Exposure to Natural Hazards. Wellington, New Zealand.

The Telegraph. (2010). Aftermath of the Haitian Earthquake. [Photograph] Retrieved 26 June 2013, from http://www.telegraph.co.uk/news/worldnews/centralamericaandthecaribbean/haiti/9011990/Haitians-pay-tribute-on-second-anniversary-of-devastating-earthquake.html.

Thomas, R. (1998). "An Update on the Four Color Theorem." Notices of the AMS **45**(7): 848-859.

Transport Committee (2011). Keeping the UK moving: The impact on transport of the winter weather in December 2010. The Stationary Office: London.

Tu, Y. F., Yang, C. and Chen, X. H. (2013). "Road network topology vulnerability analysis and application." Proceedings of the Institution of Civil Engineers-Transport **166**(2): 95-104.

Tu, Y. H. (2000). "How robust is the Internet?" Nature **406**(6794): 353-354.

U.S.-Canada Power System Outage Task Force (2004). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations.

U.S. Congressional Budget Office (1983). Public Works Infrastructure: Policy Considerations for the 1980s.

U.S. Congressional Budget Office (1988). New Directions for the Nation's Public Works.

U.S. Congressional Reseach Service (2004). Critical Infrastructure and Key Assets: Definition and Identification. Unitied States.

U.S. Environmental Protection Agency. (2008). EPANET. U.S. Environmental Protection Agency. http://www.epa.gov/nrmrl/wswrd/dw/epanet.html.

U.S. Government (1984). Public Law 98-501, sec 203.

U.S. Homeland Security (2012). National Protection and Programs Directorate: Office of Infrastructure Protection Strategic Plan: 2012 - 2016.

Valverde, S. and Solé, R. V. (2003). "Hierarchical small worlds in software architecture." Arxiv preprint cond-mat/0307278.

Walski, T. (1993). "Water distribution valve topology for reliability analysis." Reliability Engineering & System Safety **42**(1): 21-27.

Watts, D. J. (2004). "The "new" science of networks." Annual Review of Sociology **30**: 243-270.

Watts, D. J. and Strogatz, S. H. (1998). "Collective dynamics of 'small-world' networks." Nature **393**(6684): 440-442.

Wik, M., Pirjola, R., Lundstedt, H., Viljanen, A., Wintoft, P. and Pulkkinen, A. (2009). "Space weather effects in July 1982 and October 2003 and the effects of geomagnetically induced currents on Swedish technical systems." Annales Geophysicae **27**: 1775-1787.

WLRN. (2010). Hurricane, I Mean Earthquake. [Photograph]. Retrieved 26 June 2013, from http://wlrnunderthesun.org/2010/05/cane-versus-quake/.

World Health Organisation (2005). "Three months after the Indian Ocean earthquake-tsunami report." Retrieved 16 August 2013, from http://www.who.int/hac/crises/international/asia_tsunami/3months/report/en/.

Wu, F. (2002). "Calibration of Stochastic Cellular Automata: The Application to Rural-Urban Land Conversions." International Journal of Geographical Information Science **16**(8): 795-818.

Yang, H., Chung, C. Y., Zhao, J. and Dong, Z. (2013). "A Probability Model of Ice Storm Damages to Transmission Facilities." IEEE Transactions on Power Delivery **28**(2): 557-565.

Yazdani, A. and Jeffrey, P. (2011). "Applying Network Theory to Quantify the Redundancy and Structural Robustness of Water Distribution Systems." Journal of Water Resources Planning and Management **138**(2): 153-161.

Yazdani, A. and Jeffrey, P. (2012). "Water distribution system vulnerability analysis using weighted and directed network models." Water Resources Research **48**.

Zanin, M. and Lillo, F. (2013). "Modelling the air transport with complex networks: A short review." European Physical Journal-Special Topics **215**(1): 5-21.

Zhang, J., Cao, X. B., Du, W. B. and Cai, K. Q. (2010). "Evolution of Chinese airport network." Physica a-Statistical Mechanics and Its Applications **389**(18): 3922-3931.

APPENDIX A

The Vulnerability of the European Air Traffic Network to Spatial Hazards

Nat Hazards
DOI 10.1007/s11069-011-9885-6

ORIGINAL PAPER

The vulnerability of the European air traffic network to spatial hazards

Sean M. Wilkinson · Sarah Dunn · Shu Ma

Received: 8 April 2011 / Accepted: 24 June 2011

Abstract The 2010 eruption of the Eyjafjallajökull volcano had a devastating effect on the European air traffic network, preventing air travel throughout most of Europe for 6 days (Oroian in ProEnvironment 3:5–8, 2010). The severity of the disruption was surprising as previous research suggests that this type of network should be tolerant to random hazard (Albert et al. in Nature 406(6794):378–382, 2000; Strogatz in Nature 410(6825):268–276, 2001). The source of this hazard tolerance lies in the degree distribution of the network which, for many real-world networks, has been shown to follow a power law (Albert et al. in Nature 401(6749):130–131, 1999; Albert et al. in Nature 406(6794):378–382, 2000). In this paper, we demonstrate that the ash cloud was unexpectedly disruptive because it was spatially coherent rather than uniformly random. We analyse the spatial dependence in air traffic networks and demonstrate how the combination of their geographical distribution and their network architectures jeopardises their inherent hazard tolerance.

Keywords Network reliability · Scale-free networks · Spatial hazard · Airline networks · Hazard tolerance · Exponential networks

1 Introduction

Complex networks can be found in all aspects of modern society. Many of these complex networks, including the Internet and World Wide Web, have been shown to be scale-free (Barabasi and Albert 1999; Albert et al. 2000). Scale-free networks are networks whose degree distribution (defined as the cumulative probability distribution of the number of connections that each node has to other nodes, see Fig. 1a, b for further explanation) follows a power law and therefore comprises a small number of high-degree nodes and a large number of smaller-degree nodes. They have been shown to be resilient to random hazard and vulnerable to targeted attack as a random hazard has a small chance of removing a high-degree node, whereas an informed and pernicious agent will target the

S. M. Wilkinson (✉) · S. Dunn · S. Ma
School of Civil Engineering and Geosciences, Newcastle University, Newcastle upon Tyne, UK
e-mail: s.m.wilkinson@ncl.ac.uk

Published online: 19 August 2011

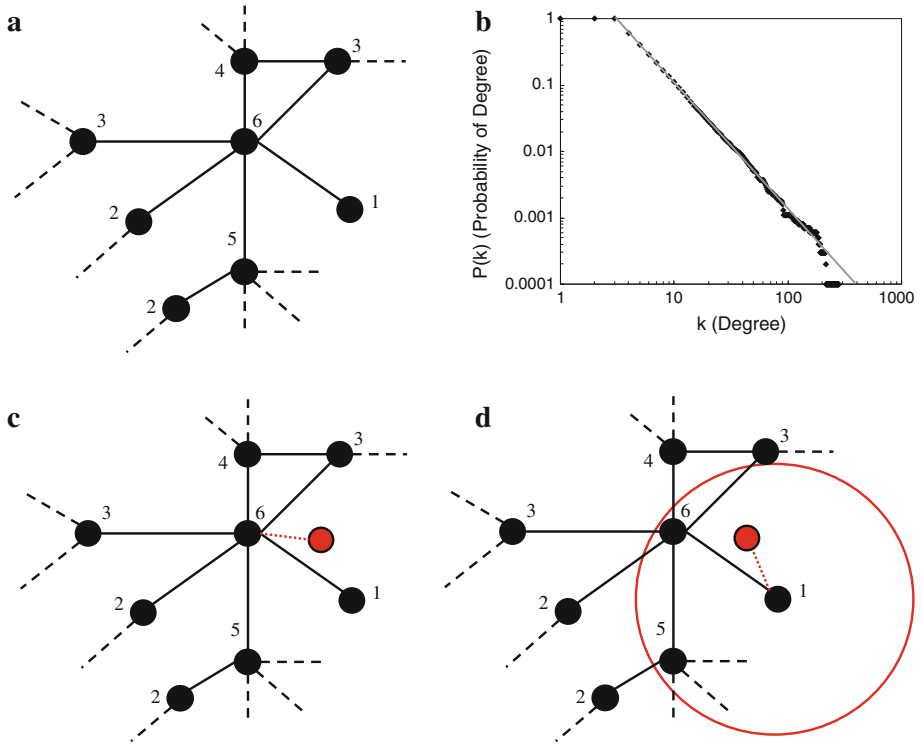


Fig. 1 The calculation of degree distribution is made by obtaining the degree of each node. The degree of a node, k, is the number of links attached to this node from other nodes, for example, if a node has 3 links attached to it, then it has a degree of 3. **a** shows a small sample from a scale-free network, created using Network Workbench, and shows the degree of each node (the *dashed lines* indicate links to other nodes in the network that have been removed from this figure for clarity). The degree distribution of the network, $P(k)$, gives the cumulative probability that a selected node has k or greater links. $P(k)$ is calculated by summing the number of nodes with $k = 1, 2, \ldots$ links divided by the total number of nodes. It is this distribution that allows for the distinction between different classes of network and also defines the inherent hazard tolerance of the network (Barabasi and Oltvai 2004). The degree distribution for the scale-free network (partly shown in **a**) is shown in **b**. Preferential attachment based on degree and based on both proximity and degree is indicated in **c** and **d,** respectively. In **c,** a new node (in *red*) is introduced into the network, and using the algorithm of Barabasi and Albert (1999) would be most likely to attach itself to the high-degree node; however, considering proximity as well as degree alters the probability because the spatial domain of the low-degree node (in the *centre* of the *red circle*) includes the high-degree node and therefore inflates its probability of attachment (desirability)

highest-degree node resulting in a disproportionately severe impact to the network (Albert et al. 2000). Those physical networks that have been shown to be scale-free (for example, the Internet and the World Wide Web) require little physical space; the routers and servers, which comprise the Internet, each require only a room, or even a small space within a room. Even the largest hubs require little physical space and little or no planning permission. The World Wide Web requires even less space. Web pages and the hyperlinks that connect them are virtual entities whose physical size amounts to only a few nanometres on a hard disc drive. Previous studies have not considered the effects of space and physical size on these networks, as space has little effect on the network physical configuration.

Other infrastructure networks, on the other hand, such as electrical transmission networks or transportation networks, require large amounts of space and are usually subject to strict planning regulations. A few studies have considered the spatial configuration of real-world networks, such as airline networks (for example, Guimera and Amaral 2004; Burghouwt et al. 2003; Qian and Han 2009; Gastner and Newman 2006); however, these studies have not considered hazard tolerance.

The 2010 eruption of the Eyjafjallajökull volcano, in Iceland, occurred on the 14th March forcing almost 800 local residents to evacuate their homes (Petersen 2010). With further eruptions, airspace in Europe became restricted, and no fly zones came into operation on 14th April (Brooker 2010) (see Fig. 2a–c). The resulting airport closures and disruption to air travel caused more than 10 million passengers to be delayed. The economic impact to the airline industry, in terms of revenue loss for airlines from scheduled services, during the period 15th–21st April, was estimated at 1.7 billion US dollars (Mazzocchi et al. 2010). We show that this disruption was disproportionate by quantifying the magnitude of the disturbance relative to the cause. We have achieved this using the data contained in Openflights (2010) to produce a comprehensive set of 525 European airports, 3,886 air routes operated by 203 airlines as well as travel statistics for Europe for the 14th–21st April 2010 (Eurocontrol 2010). We have used these data to form a European air traffic network (EATN) and have then obtained its degree distribution, which gives us information about its inherent tolerance to random hazard. We have also investigated the tolerance of the EATN to two types of spatially coherent hazard, in both cases, taking note of the number of airports closed, air routes cancelled, the proportion of closed airspace and the maximum cluster size of the network. We have used these data to determine whether the EATN is vulnerable to spatial hazards.

2 Initial assessment of the hazard tolerance of the European air traffic network

Our first investigation into the EATN is achieved by plotting the network's degree distribution. As this is defined as the probability distribution of the number of connections that each node has to other nodes, it is therefore a key indicator of its hazard tolerance. Comparing the degree distribution of EATN (Fig. 3a) to other published research, we find that the European data set is similar to the North American (Guimera and Amaral 2004; Chi et al. 2003; Li et al. 2006) and Chinese (Li and Cai 2004) air traffic networks in that they conform to a truncated power law (Guimera and Amaral 2004). This type of network should therefore have relatively high hazard tolerance to random events.

To investigate whether the volcanic eruption had a disproportionate effect on the network, we have identified airports that had no flights for 12 or more hours on a particular day using the data of Eurocontrol (2010). We have taken these data and plotted Fig. 2a–c, showing the open and closed flight information regions (FIR), for the worst affected day of the hazard (18th April) and two other affected days. The figure shows that the ash cloud mainly affected northern Europe, but also closed central Europe on the worst day of the event. In Fig. 2d, we plot the proportion of air routes closed against the proportion of closed airspace. If the effect is proportionate to the cause (i.e. the disruption is proportionate to the area of closed airspace), then the points (representing different days of disruption and therefore different airport closures) should sit on the 45° line in the graph. From Fig. 2d, we can see that the relationship shows that the disruption was proportionally greater than the closed airspace, demonstrating the EATN is vulnerable to spatial hazards.

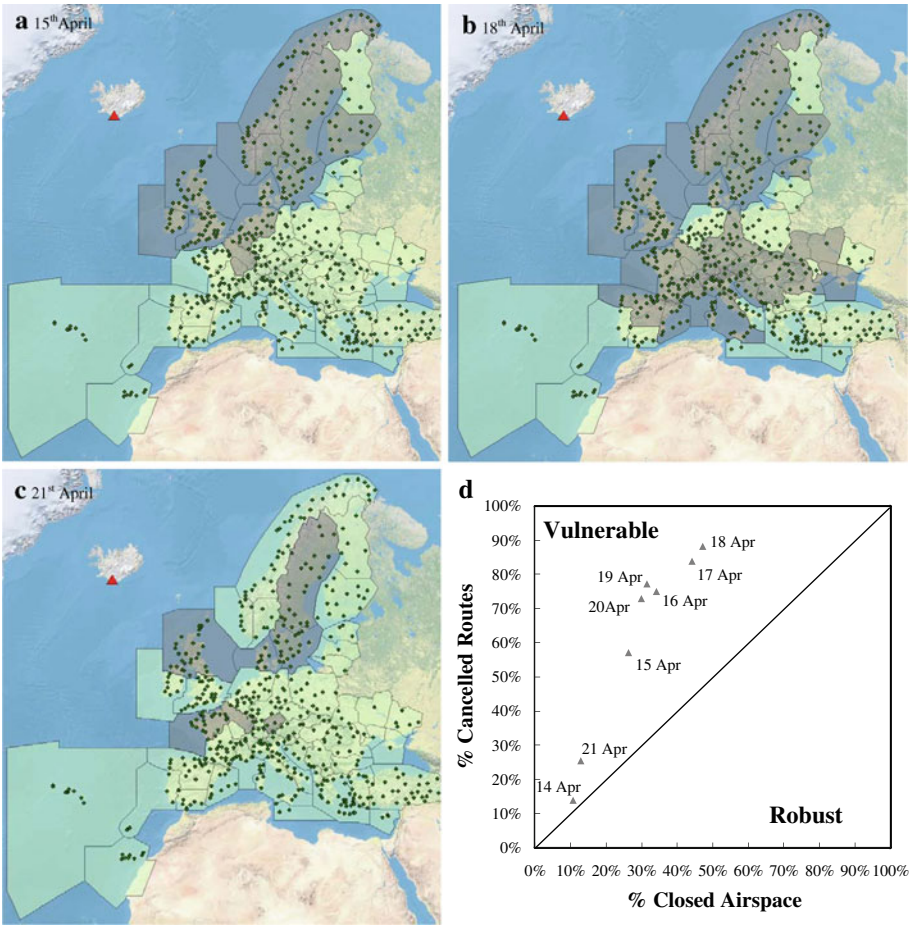


Fig. 2 *Open* (*light green*) and *closed* (*grey*) FIR in Europe (i.e. airspace) for **a** 15th April, **b** 18th April and **c** 21st April 2010 (Eurocontrol 2010). Also, **d** showing proportion of travel disruption, relative to the proportion of closed airspace, during the Eyjafjallajökull eruption of 14th–21st April 2010. The *red triangle* is the Eyjafjallajökull volcano

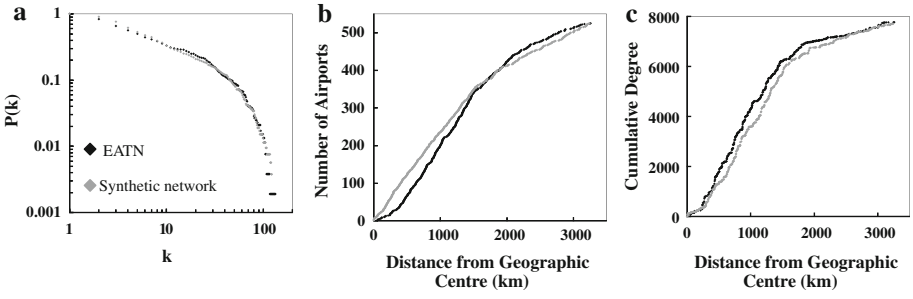


Fig. 3 **a** Cumulative degree distribution, **b** number of airports within a given radius and **c** spatial degree distribution for the EATN (data were obtained from Openflights 2010), and one generated synthetic network

To understand the influence of geography on the spatial vulnerability of the EATN, we examine the spatial distribution of European airports as well their spatial degree distribution (Fig. 3b, c). These distributions were obtained by first calculating the geographical centre of the airports (weighted by their degree) and then plotting the number of airports within a given radius (Fig. 3b) and the cumulative degree (Fig. 3c). For the EATN, the geographical centre of the network is located in Germany (approximately 190 km east of Frankfurt). Both exhibit a bilinear form, meaning that they are uniform with distance from the geographical centre of the air traffic network up to radius of $\sim$1,500 km, after which the distribution of both airports and their degrees becomes sparser but remains relatively uniform. The change in grade shown in Fig. 3b, c occurs as the considered area extends into the Atlantic Ocean in the west, and the border of the European Union in the east.

3 Synthetic network generation algorithm

To assess the vulnerability of this class of network (not just the EATN), we have developed a synthetic network generation algorithm that not only reproduces the relational architecture of these networks but also incorporates a spatial element. In this algorithm, we propose that poorly connected nodes can capitalise on their close proximity to a highly connected hub by attracting links that were bound for the high degree hub. For example, an airline may wish to establish a route to a major regional airport; however, the operating costs at this airport are high. Flying to a nearby airport will still attract passengers as it is only a short overland journey from this node to the highly connected hub, but for this subordinate node, the fares can be reduced due to the lower operating costs. We therefore argue that the decision of where to establish a new route is made based on both degree and proximity. We use this proposition to extend the algorithm of Barabasi and Albert (1999) (used to generate scale-free networks) by enclosing the network within a spatial domain and preferentially attaching new nodes based on the degree of all nodes within a subdomain (neighbourhood) (Fig. 1c, d). Following Barabasi and Albert (1999), we initially choose a given number of starting nodes, m_0, but each starting node is now given a random location. At each step, we add a new node to the network and assign it a random distance bearing from the geographical centre so that the spatial distribution has the same form as shown in Fig. 3b. We then generate, between 1 and m_0, links and preferentially attach this node to the existing network in the same manner as for a scale-free network; however, preference is now based on the degree of all nodes within the neighbourhood of the node we are attempting to attach to. The size of the neighbourhood is set by assigning a radius, r, which represents the distance people are prepared to travel overland to reach an airport. Setting the radius to zero removes the spatial dependence of the network resulting in a scale-free network, while setting the radius to twice the size of the spatial domain results in random attachment. To obtain the same spatial degree distribution as EATN, the radius of an airport's neighbourhood is made proportional to the distance the airport is from the centre of the network. This last rule is intuitive because airports are more densely packed in the centre of the network giving people a greater selection of routes for smaller overland travel distances.

Our new algorithm also includes the modification of Guimera and Amaral (2004), which allows a proportion of the new links, p, to connect to pre-existing nodes. This simulates the establishment of new routes between existing airports and is necessary to reproduce reconfigurable networks, such as the EATN. We do not include the flight distance criteria for preferential attachment of Guimera and Amaral (2004), as we are not considering

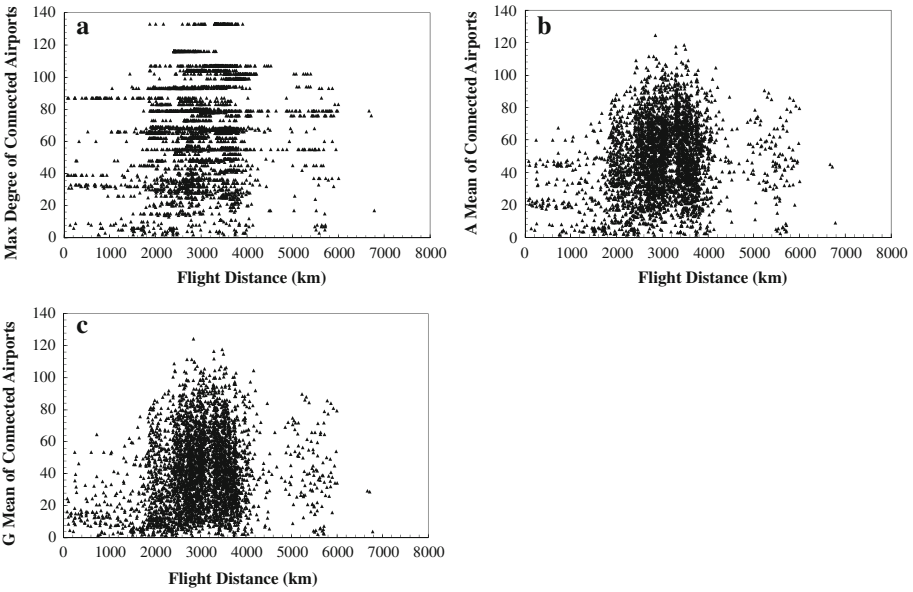


Fig. 4 The air route distance between airports (in km) compared to **a** maximum degree of connected airports, **b** arithmetic mean of the two connected airports and **c** geometric mean of the two connected airports for the EATN. All of the graphs in the figure show that there is no correlation between the air route distance (i.e. the distance between two airports connected via an air route) and various measures of degree of the two connected airports

intercontinental flights and deregulation of the EATN has led to flight path length becoming uncorrelated from degree. We demonstrate this by plotting, in Fig. 4, flight length of different air routes against various measures of degree, showing that there is no correlation between the flight length and connectivity of an airport. In Fig. 4a, we compare the maximum degree airport that an air route is connected to; in Fig. 4b, we compare the arithmetic mean of the degree of the two airports that an air route connects; and in Fig. 4c, we compare the geometric mean of the two airports that an air route connects. These figures show that there is no correlation between degree and flight path length for the EATN.

To generate the bilinear distribution in Fig. 3b, we define a distance from the geographical centre inside which a percentage of the total nodes in the network are randomly placed, with the remainder of the nodes being randomly placed in the area between this point and the outer edge of the network. This results in the number of airports within a given radius being an approximation of the EATN.

We demonstrate this algorithm by generating a 525-node synthetic network with $m_0 = 14$, $r = 0.15$ (an average distance of approximately 250 km around 2–3 h driving time on modern roads) and $p = 0.8$. The resultant degree and spatial degree distributions are shown in Fig. 3 and fit our European data set extremely well.

To demonstrate that our algorithm best fits the data over the entire distribution, we vary these parameters to gauge their influence on the degree distribution (Fig. 5). The best fit for the EATN is the exponential network with $p = 0.8$ and $r = 0.15$. Generating networks with $p = 0$ and $r = 0.15$ shows that the distribution is exponential (i.e. it is linear when

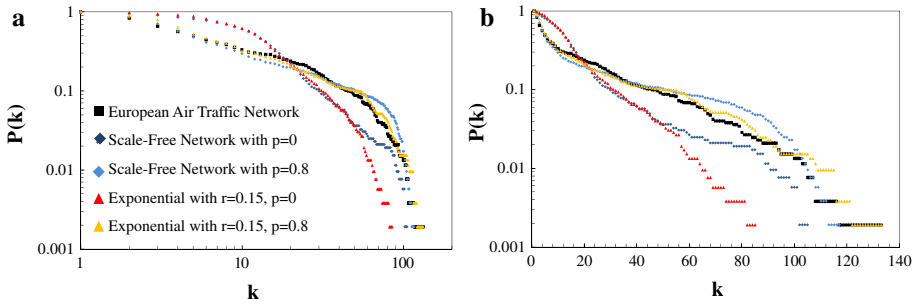


Fig. 5 EATN and four synthetic networks, generated using different algorithms, showing **a** degree distribution plotted on log–log scales and **b** degree distribution plotted on log-linear scales, where p is the proportion of new links, introduced in each time step that are allowed to connect to pre-existing nodes (e.g. if $p = 0.8$ then 80% of the new links will be between existing nodes), and r is the neighbourhood size, representing the distance that people are prepared to travel overland to an airport (e.g. if $r = 0.15$, then the equivalent distance is approximately 250 km)

plotted on log-linear axes). The difference between the exponential networks with values of $p = 0$ and $p = 0.8$, for the same value of r, demonstrates that in generating airline networks, new links will form between two existing nodes for a given time step (i.e. new flight routes will be added by an airline between existing airports) and are not only confined to attaching between the new node and existing nodes (see Guimera and Amaral 2004). If new routes are not permitted to form between existing airports (i.e. $p = 0$), the resultant is fewer 'hub' airports forming (i.e. airports with large degrees). Both scale-free networks follow the initial curve of the EATN data, but then do not follow the truncated part of the network, meaning that our synthetic exponential network generation algorithm produces the best fit for the EATN.

In reproducing the EATN, the r value used suggests that, on average, air passengers are prepared to travel approximately 250 km overland to an airport. In a disaster scenario, this value is unlikely to remain constant. Air passengers are likely to be prepared to take much greater overland journeys to ensure that they reach their destinations, especially in the case of returning journeys. In fact, during the Eyjafjallajökull event, accounts of people driving across Europe were not uncommon. While air transport regulations do allow for a spontaneous change of destination in hazardous situations, air space regulations, as well as airline-specific infrastructure problems, make it extremely difficult to quickly open alternative routes. In this sense, the network is more complex and rather inflexible in comparison with other networks, such as the Internet. For example, a flight en route from Zurich to Manchester may get permission for an emergency landing, at say Heathrow. If Manchester airport was closed for several days and Heathrow airport remained open, passengers may take the option of travelling to and from Heathrow to Manchester. The redirection of air traffic and the increased overland journeys that people may be prepared to make have not been taken into account in this analysis due to their unpredictability.

4 Assessment of hazard tolerance of this generic class of network

To better assess the vulnerability of this class of network and the associated scatter between different networks, we use our algorithm to generate three synthetic networks, with the same spatial properties and the same network architecture as the EATN (but each

with different node positions and linkages), and expose them to different spatial hazards. To simulate the Eyjafjallajökull event, we place a circular hazard at the edge of our domain and gradually increase its size, removing links and nodes as they become enveloped by this hazard. We also expose these networks to random but spatially coherent hazards, defined by a circle of varying diameters and random locations. To enable equivalent comparisons, the spatial hazards, for both the EATN and our synthetic networks, cover the same percentage airspace and are located at the same distance from their geographical centres. The results of these simulations are displayed in Fig. 6a, b, together with the Eyjafjallajökull event and the EATN exposed to our random, spatially coherent hazard. The scatter in the hazard tolerance for these synthetic networks is surprisingly small and is in good agreement with the EATN, demonstrating this class of network's vulnerability to both hazards. Although the individual hazard tolerance results of our synthetic networks compare very favourably with the EATN, there are a few outliers, for example, there are two points in Fig. 6a, relating to the EATN subjected to random hazard that occurs below the 45° line. These two random hazards occur in northern Scandinavia, where both the density of airports and the average degree of airports are lower than that for central Europe, due to this region being in close proximity to the edge of the spatial boundary of the network. This results in flights from northern Scandinavia only being permitted to travel to airports with a more southerly location (i.e. stay within the boundaries of European airspace), resulting in airports with disproportionately low degrees. This results in fewer cancelled air routes for the same number of closed airports.

For our final investigation into hazard tolerance, we plot the maximum cluster size (MCS) in Fig. 6c, d. This last measure is defined as the ratio of the largest connected

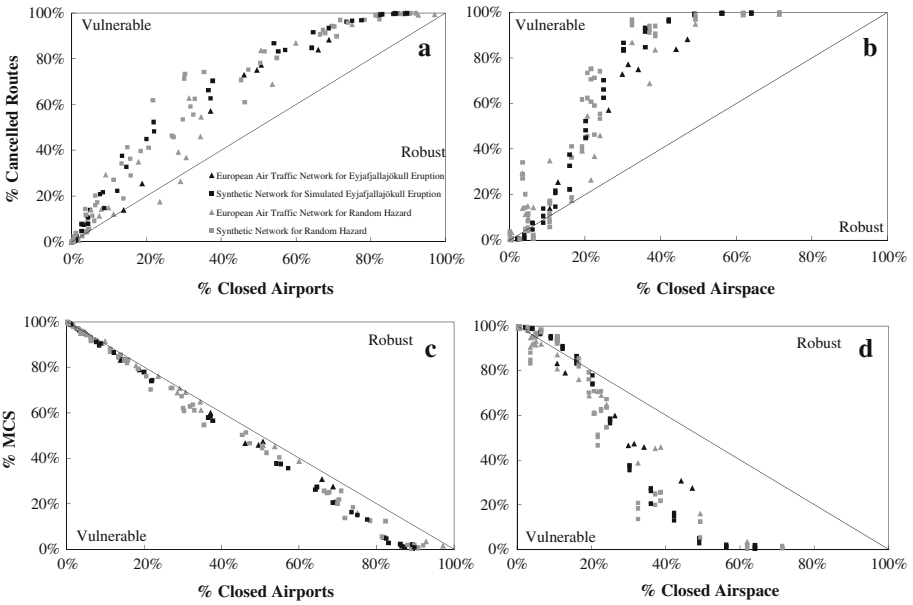


Fig. 6 Comparison of network vulnerability for the EATN and our three synthetic networks, showing **a** the impact of airport closure on air route operations; **b** the influence of airspace closure on air route operations; **c** the reduction in MCS due to airport closures; and **d** the influence of airspace closure on MCS

cluster in a fragmented network to the original size of network and therefore is a key indicator of how degraded a network has become (see Albert et al. 2000 for further details). In Fig. 6, we see that, as expected, the MCS versus proportion of closed airports for the EATN and our three synthetic networks falls on the neutral line (Albert et al. 2000); however, as our simulations and the real EATN show, it is vulnerable when measured as a proportion of closed airspace. Both our algorithm and the data show that these networks usually have neutral tolerance to spatial hazard up to about 10–15%, of the total network area, but become increasingly vulnerable after this. In the case of random hazard, both our algorithm and the EATN data set demonstrate that it is possible for a relatively small spatially coherent hazard to have a devastating effect on this class of network. This is best demonstrated in Fig. 6d, where two points on our synthetic network are centred over the geographical centre of the network resulting in a devastating effect.

5 Conclusion

In summary, the eruption of Eyjafjallajökull in 2010 caused a massive disruption to the European air traffic network. We have demonstrated that the effect on air traffic was disproportionately severe due to the network possessing a truncated, scale-free distribution and a spatial degree distribution that is uniform with distance from the centre of the network, resulting in a network that is vulnerable to spatial hazards. We believe that these distributions result from a combination of the desirability of a location, space limitations and the distance users are prepared to travel overland to an airport. As many real-world networks have been shown to be either scale free or exponential (Albert et al. 2004; Crucitti et al. 2004), it is possible that the underlying growth rules for these types of networks may result in them also being susceptible to spatial hazard. In the future, it may be desirable to reduce this susceptibility to spatial hazard. One possible method is to move some of the airports away from the geographical centre, located in Germany (specifically the high-degree airports); however, this approach may render the network less effective for normal operations. This approach also encounters the problem that each country in Europe may desire a 'hub' airport, meaning that moving airports away from the geographical centre may not be a possibility. Another method could be to enable reconfiguration of air routes for cases such as the Eyjafjallajökull eruption.

Acknowledgments The flight information regions necessary to define the closed airports was provided by EUROCONTROL. GIS advice on handling the data sets was provided by Dave Alderson and Ali Ford of Newcastle University. Maximum cluster size was calculated using Network Workbench. This research was partly funded by the Engineering and Physical Sciences Research Council, UK, and their support is gratefully acknowledged.

References

Albert R, Jeong H, Barabasi AL (1999) Internet—diameter of the world-wide web. Nature 401(6749):130–131

Albert R, Jeong H, Barabasi AL (2000) Error and attack tolerance of complex networks. Nature 406(6794):378–382

Albert R, Albert I, Nakarado GL (2004) Structural vulnerability of the North American power grid. Phys Rev E 69. doi:10.1103/PhysRevE.69.025103
Barabasi AL, Albert R (1999) Emergence of scaling in random networks. Science 286(5439):509–512
Barabasi AL, Oltvai ZN (2004) Network biology: understanding the cell's functional organization. Nat Rev Genet 5(2):101–113
Brooker P (2010) Fear in a handful of dust: aviation and the Icelandic volcano. Significance 3:112–115
Burghouwt G, Hakfoort J, van Eck JR (2003) The spatial configuration of airline networks in Europe. J Air Transp Manag 9(5):309–323. doi:10.1016/s0969-6997(03)00039-5
Chi LP, Wang R, Su H, Xu XP, Zhao JS, Li W, Cai X (2003) Structural properties of US flight network. Chin Phys Lett 20(8):1393–1396
Crucitti P, Latora V, Marchiori M (2004) A topological analysis of the Italian electric power grid. Physica A Stat Mech Appl 338(1–2):92–97. doi:10.1016/j.physa.2004.02.029
Eurocontrol (2010) Monthly network operations report: April 2010
Gastner MT, Newman MEJ (2006) The spatial structure of networks. Eur Phys J B 49(2):247–252. doi:10.1140/epjb/e2006-00046-8
Guimera R, Amaral LAN (2004) Modeling the world-wide airport network. Eur Phys J B 38(2):381–385. doi:10.1140/epjb/e2004-00131-0
Li W, Cai X (2004) Statistical analysis of airport network of China. Phys Rev E Stat Nonlin Soft Matter Phys 69(4 Pt 2):046106
Li W, Wang QA, Nivanen L, Le Mehaute A (2006) How to fit the degree distribution of the air network? Physica A Stat Mech Appl 368(1):262–272. doi:10.1016/j.physa.2005.11.050
Mazzocchi M, Hansstein F, Ragona M (2010) The 2010 volcanic ash cloud and its financial impact on the European airline industry. CESifo Forum 11:92–100
Openflights (2010) OpenFlights.org. http://openflights.org/. Accessed 13 Aug 2010
Oroian I (2010) Eyjafjallajokull volcano eruption—a brief approach. ProEnvironment 3:5–8
Petersen GN (2010) A short meteorological overview of the Eyjafjallajokull eruption 14 April–23 May 2010. Weather 65(8):203–207. doi:10.1002/wea.634
Qian JH, Han DD (2009) A spatial weighted network model based on optimal expected traffic. Physica A Stat Mech Appl 388(19):4248–4258. doi:10.1016/j.physa.2009.05.047
Strogatz SH (2001) Exploring complex networks. Nature 410(6825):268–276

APPENDIX B

Identifying Critical Components in Infrastructure Networks using Network Topology

Identifying Critical Components in Infrastructure Networks Using Network Topology

Sarah Dunn[1] and Sean M. Wilkinson[2]

Abstract: This paper applies graph theory metrics to network flow models, with the aim of assessing the possibility of using these metrics to identify vulnerable areas within infrastructure systems. To achieve this, a reduced complexity flow model that can be used to simulate flows in infrastructure networks is developed. The reason for developing this model is not to make the analysis easier, but to reduce the physical problem to its most basic level and therefore produce the most general flow model (i.e., applicable to the widest range of infrastructure networks). An initial assessment of the applicability of graph theory metrics to infrastructure networks is made by comparing the distribution of flows, calculated using this model, to the shortest average path length in three of the most recognized classes of network—scale-free networks, small-world networks, and random graph models—and it is demonstrated that for all three classes of network there is a strong correlation. This suggests that at least parts of graph theory may be used to inform one about the behavior of physical networks. The authors further demonstrate the utility of graph theory metrics by using them to improve their predictive skill in identifying vulnerable areas in a specific type of infrastructure system. This is done using a hydraulic model to calculate the flows in a sample water distribution network and then to show that using a combination of graph theory metrics and flow gives superior predictive skill over just one of these measures in isolation. **DOI: 10.1061/(ASCE)IS.1943-555X.0000120.**

CE Database subject headings: Infrastructure; Network analysis; Lifeline systems; Disasters.

Author keywords: Infrastructure; Network analysis; Lifeline systems; Disasters.

Introduction

Critical infrastructure systems such as electrical distribution and water and transport networks form the backbone of modern communities, promote social well-being, and support economic growth and productivity. They do this by delivering a flow of services from areas where they are stored or generated (e.g., power stations) to areas of demand (e.g., communities). The importance of these networks and their potential fragility can be demonstrated by the catastrophic consequences that can result from the failure of a few elements, or potentially even a single element, within these systems. For example, in August 2003 North America suffered a blackout affecting two million people in eight U.S. states, with estimated economic losses between US$7 and $10 billion; the blackout started with the failure of a single power station (U.S.–Canada Power System Outage Task Force 2004). Traditionally these systems have been analyzed using physically based models and their performance judged by their ability to deliver the required services (e.g., flow of water, electricity) to communities. A great deal of recent research has attempted to use network graph theory to identify the vulnerable components within infrastructure systems, including Crucitti et al. (2005), Genesi et al. (2007), and Cadini et al. (2009); however, these studies have not used physically based flow models and subsequently have not ranked the importance of nodes based on their impact on the flow of services. The aim of this paper is to determine whether there is a relationship between flows calculated by physically based flow models and network topology and, if so, whether this could be used to improve the ability to identify vulnerable nodes within infrastructure systems.

Rationale for Considering Network Graph Theory for This Application

From the many network models in existence today, three stand out as being probably the most important and widely recognized. These are (1) scale-free (Barabasi and Albert 1999), (2) small-world (Watts and Strogatz 1998), and (3) random graph (Erdös and Renyi 1960) models. The Erdös and Renyi random graph model was the first developed network model (Erdös and Renyi 1960) and is arguably the simplest graph possible (Albert and Barabasi 2002). This type of network does not model real-world networks (including infrastructure networks) particularly well (Newman 2003) but is normally used as a baseline for comparison with more structured networks (Lewis 2009). To more accurately model real-world systems, Watts and Strogatz modified the random graph model using the concept of six degrees of freedom (Milgram 1967) forming small-world networks (Watts and Strogatz 1998). Both small-world and random networks are characterized by a Poisson degree distribution [defined as the cumulative probability distribution of the number of connections that each node has with other nodes (Barabasi and Oltvai 2004)]. However, Barabasi and Albert (1999) discovered that real-world networks [including the Internet (Albert et al. 2000) and the World Wide Web (Barabasi and Albert 1999; Barabasi et al. 2000)] tend to form a power-law

[1]Ph.D. Researcher, School of Civil Engineering and Geosciences, Newcastle Univ., Newcastle Upon Tyne, NE1 7RU, UK (corresponding author). E-mail: sarah.dunn@ncl.ac.uk

[2]Senior Lecturer, School of Civil Engineering and Geosciences, Newcastle Univ., Newcastle Upon Tyne, NE1 7RU, UK. E-mail: s.m.wilkinson@ncl.ac.uk

Note. This manuscript was submitted on July 21, 2011; approved on July 24, 2012; published online on August 15, 2012. Discussion period open until November 1, 2013; separate discussions must be submitted for individual papers. This paper is part of the ***Journal of Infrastructure Systems***, Vol. 19, No. 2, June 1, 2013. © ASCE, ISSN 1076-0342/2013/2-157-165/$25.00.

degree distribution. Networks that follow this power law are more commonly known as scale-free networks.

The power-law degree distribution, for these scale-free networks, means that they comprise a small number of high-degree nodes and a large number of smaller-degree nodes. As such, they are resilient to random hazards and are vulnerable to targeted attack as a random hazard has a small chance of removing the important nodes (i.e., those with a high degree), whereas targeted attacks will often remove the highest-degree node, resulting in a disproportionately severe impact on the network as a whole (Albert et al. 2000). Other researchers have tried to develop more sophisticated measures of establishing the importance of nodes rather than just using node degree. The most widely used measures are known as centrality measures and have been used to show that these high-degree nodes are not necessarily the most important in a network (e.g., Guimera et al. 2005). Centrality measures have been applied to social networks (Everett and Borgatti 1999) with the aim of identifying the central person/figure or group/class in a social network. Recently, these measures have also been applied to infrastructure networks (Choi et al. 2006; Crucitti et al. 2006). These studies found that the most connected node (i.e., the node with the highest degree) is not necessarily the node with the highest value of centrality (Guimera et al. 2005; Cadini et al. 2009). However, these studies do not consider how the services that the network provides flows around the network, nor do they stress the network (by removing nodes or links) to gauge the effect on performance. It is therefore unproven as to whether the node with the highest value of centrality would have more of an effect on a network, when removed, compared to a node with the highest degree.

Development of a Reduced Complexity Flow Model

Infrastructure networks are critically important to modern society as they provide the essential services upon which communities rely. They can be placed into one of several groups: electrical power, gas and liquid fuels, telecommunications, transportation, waste disposal, and water supply (O'Rourke 2007). All of these services are provided thanks to a flow of commodities from locations where the service is either generated or stored to areas where it is consumed. Traditionally, a flow model is used to analyze these infrastructure systems, simulating the transfer in services from areas of supply to areas of demand. In engineering, numerous flow models can be used to simulate the physical processes. It is desirable initially to determine the applicability of graph theory metrics to the analysis of infrastructure systems in general, and so what is arguably the simplest flow model is developed; however, the model still has all the attributes necessary to simulate flows in a network.

To achieve this, a simple hydraulic model that can be found in any standard hydraulic text is modified (e.g., Novak et al. 2010). Although this is a hydraulic model, it has analogies with other categories of infrastructure network, such as electrical distribution networks and traffic flow problems—for example, the pressure head in a hydraulic system is analogous to a potential difference in an electrical network or demand in traffic or data networks. Equally, pipe friction in a hydraulic network could be compared to electrical impedance in an electricity network, or road capacity in a traffic network. The similarities in the physical behavior of different sorts of infrastructure networks means that the results obtained for one type of network, although not exactly equivalent, are indicative of the behavior of other types of infrastructure networks. In the case of a hydraulic network, the governing equations for a steady-state flow problem are as follows:

- Conservation of mass. The mass at any point along a pipe must be constant (i.e., flow into a pipe = flow out of a pipe):

$$Q_{\text{in}} = Q_{\text{out}} \tag{1}$$

- Conservation of energy. Energy must be conserved; for hydraulic networks this energy usually consists of potential energy (or the potential difference in the case of an electrical network) and kinetic energy and is defined by the Bernoulli equation (for pipe flows)

$$z_1 + \frac{p_1}{v_1} + \frac{v_1^2}{2g} = z_2 + \frac{p_2}{v_2} + \frac{v_2^2}{2g} + fl \tag{2}$$

where z = potential energy; p = pressure; v = velocity at Points 1 and 2, respectively; fl = frictional losses; and g = gravitational constant. Eq. (2) basically illustrates that between Points 1 and 2 conservation of energy is maintained.

Implementation of Reduced Complexity Flow Model

The flows in a network are calculated (through both the nodes and the links) using the process described below. A small example network is used to illustrate the process (Fig. 1). In this example, Node 1 is a supply node, whereas the other nodes are demand nodes.

Calculate the Potential Energy for Each Node in the Network

The standard hydraulic formula for calculating flow in a pipe is

$$F_l = k(Q)^n \tag{3}$$

where F_l = frictional losses; k = a constant that describes the resistance of the system (e.g., pipe friction for a hydraulic network or electrical impedance for an electrical system); and Q = flow through pipe. For steady-state hydraulic flow in pipes, the value of n normally equals 2; however, because a generic model that represents a range of infrastructure networks is desired, the problem is reduced to its most base level by assuming the losses have a linear relationship with flow (i.e., $n = 1$). Linearizing the losses has the added advantage of making it possible to solve the problem directly:

$$F_l = R(Q_{1\text{–}2}) \tag{4}$$

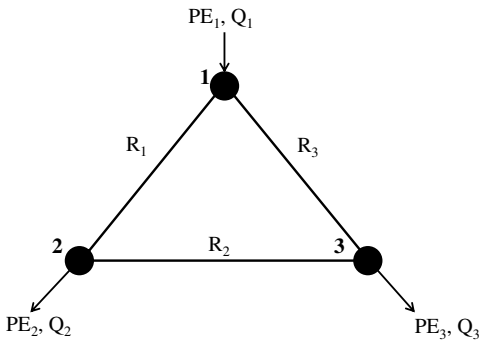


Fig. 1. Example network consisting of three nodes and three links, where Node 1 is the supply node and Nodes 2 and 3 are the demand nodes (node numbers are indicated by the bold numbers to the left of each node); Q = flow of service that the node either demands or supplies; PE = potential energy of node; R = resistance of link (subscript values indicate node/link to which they refer)

J. Infrastruct. Syst. 2013.19:157-165.

where R = resistance of the link; and Q_{1-2} = flow in pipe connecting Nodes 1 and 2.

Assuming incompressible flow, the velocities at Nodes 1 and 2 are equal, and therefore the friction loss in the pipe is equal to the difference in the potential energies of the two connected nodes. Using this and rearranging Eq. (4) gives

$$Q_{1-2} = \frac{1}{R}(PE_2 - PE_1) \tag{5}$$

Using conservation of mass, the external flow at each node (i.e., either the quantity demanded by the node or the quantity supplied by the node), denoted by q, can be calculated by summing the flows in the connected links. For Node 1 in Fig. 1 this becomes

$$q_1 = \frac{1}{R_1}(PE_2 - PE_1) + \frac{1}{R_3}(PE_3 - PE_1) \tag{6}$$

Eq. (6) can be rearranged as

$$q_1 = PE_1\left(-\frac{1}{R_1} - \frac{1}{R_3}\right) + PE_2\left(\frac{1}{R_1}\right) + PE_3\left(\frac{1}{R_3}\right) \tag{7}$$

Using this method to obtain expressions for the external flow at the other nodes [in the same format as in Eq. (7)] and combining them in matrix form results in

$$\begin{bmatrix} q_1 \\ q_2 \\ q_3 \end{bmatrix} = \begin{bmatrix} -\frac{1}{R_1} - \frac{1}{R_3} & \frac{1}{R_1} & \frac{1}{R_3} \\ \frac{1}{R_1} & -\frac{1}{R_1} - \frac{1}{R_2} & \frac{1}{R_2} \\ \frac{1}{R_3} & \frac{1}{R_2} & -\frac{1}{R_2} - \frac{1}{R_3} \end{bmatrix} \begin{bmatrix} PE_1 \\ PE_2 \\ PE_3 \end{bmatrix} \tag{8}$$

The external values of flow (q) for the demand nodes and the resistances (R) of the links are known, but the values of flow from the supply nodes are unknown. In the example network (Fig. 1) this is easy to calculate (because it is the only supply node); however, for a network with two or more supply nodes the supply will not be evenly distributed. Setting the supply nodes as potential energy reference points (i.e., $PE = 0$) enables the condensation of Eq. (8), resulting in Eq. (9). The potential energy of each demand node can be obtained by solving Eq. (9):

$$\begin{bmatrix} q_2 \\ q_3 \end{bmatrix} = \begin{bmatrix} -\frac{1}{R_1} - \frac{1}{R_2} & \frac{1}{R_2} \\ \frac{1}{R_2} & -\frac{1}{R_2} - \frac{1}{R_3} \end{bmatrix} \begin{bmatrix} PE_2 \\ PE_3 \end{bmatrix} \tag{9}$$

Calculate the Flow through Each Link

To satisfy the conservation of energy [Eq. (2)], the flow through each link in the network is calculated using Eq. (5).

Calculate the Flow Provided by Each Supply Node

The external flow at each supply node can be found using Eq. (8).

The equations describing the reduced complexity flow model have consistent units. For example, in the case of a hydraulic network, if the input values were in terms of meters and seconds, then the output value of flow would have a unit of meters per second.

Physically Based Metrics and Centrality Measures

In the authors' first experiment, the reduced complexity flow model is applied to 60 network models (20 for each of the 3 classes of network: scale-free, small-world, and random). Each network includes 1,000 nodes, and the number of links is varied to enable a comparison between networks with different levels of connectivity (e.g., for the same number of nodes, a network with more links is better connected than a network with fewer links and will transfer the flow differently between the areas of supply and demand). All of the networks were created using *Network Workbench*.

Because this is an initial assessment of the applicability using graph theory in flow-based problems, the resistance of the links are made equal. For a hydraulic system the resistance is a combination of pipe length, diameter, and roughness, and it is assumed that the combination of these parameters satisfies this assumption. It was shown by Newman (2004) that the more general case of links with different properties could be addressed using the weighted network approach (modifying the graph theory metrics to take into account the differences in the link properties) such as that of Opsahl et al. (2010), but this is beyond the scope of this initial paper.

Before the flow in the test networks can be calculated, values of supply and demand need to be assigned to each node in the network. First, the decision is made as to which nodes are to be supply nodes (infrastructure supplying a service) and which are to be demand nodes (regions requiring the service) by ranking the nodes in descending order of degree. The top 1% are chosen as supply nodes, the others are assigned as demand nodes (for example, for a network with 1,000 nodes there will be 10 supply nodes). The small proportion of supply nodes relative to demand nodes is consistent with real-world infrastructure systems, which have a small proportion of nodes supplying services (e.g., power stations or reservoirs) compared to the proportion of demand nodes (e.g., households); however, the absolute value of 1% is somewhat arbitrary. It is assumed that the supply nodes in the network have sufficient capacity to supply any service required by the demand nodes, and because a single point in time is being considered, it is also assumed that the network has reached equilibrium. In real infrastructure networks (e.g., for the case of a pipe network), if a reservoir does not have sufficient capacity to meet the required demand, then the reservoir will run dry and the flow will cease; if there are other reservoirs in the system, then the flow will be redistributed. This can be accommodated in the model using an iterative procedure, but this is beyond the scope of this paper. A numeric value of demand is assigned to the demand nodes based on their degree (i.e., the number of links attached to them). It is argued here that this is a reasonable approximation because areas with large populations, and therefore high demand for services, will require a correspondingly greater number of nodes and links to provide these (e.g., a large city will have a greater need for services than a rural community and will also have a correspondingly larger amount of infrastructure).

For this initial assessment, the results of the reduced complexity flow model are compared with the shortest average path length (APL) of the network. This metric describes the fundamental properties of a network and is defined in terms of the number of links between two nodes, rather than the physical length of the links. The shortest APL was chosen, rather than other metrics, because the shortest APL is a "*measure of the typical separation between two nodes in the graph*" (Boccaletti et al. 2006) and is therefore a measure of the efficiency of the network (as flow will distribute itself around the network such that it finds the minimum energy solution) (Albert and Barabasi 2002). The higher the value of the shortest APL, the further the services in the network must flow to travel from the supply nodes to the demand nodes, and therefore the more inefficient the network. The APL is determined by Eq. (10) (Boccaletti et al. 2006), and in this paper the APL is calculated using *Network Workbench*:

$$L = \frac{1}{N(N-1)} \sum_{i,j \in N, i \neq 1} d_{ij} \tag{10}$$

J. Infrastruct. Syst. 2013.19:157-165.

where L = shortest APL of the network; N = total number of nodes; and d_{ij} = shortest path length between nodes i and j.

Fig. 2 shows the results of correlating this measure with the flow through the demand nodes [the flow is referred to as being through a node, for simplicity; the inflow and the outflow at the node are not stated (because these two values are equal)] for scale-free [Fig. 2(a)], small-world [Fig. 2(b)], and random [Fig. 2(c)] networks. Fitting a power-law trend line through the results shows an R^2 value of greater than 0.9 for all three classes of network model. This high R^2 value suggests that at least parts of graph theory could be used in the analysis of infrastructure networks [which tend to be scale-free (Da Costa et al. 2011)].

When generating the networks used in the analysis for Fig. 2, it was not possible to generate networks with a consistently increasing value of APL due to the way the algorithms operate, particularly for the scale-free [Fig. 2(a)] and small-world networks [Fig. 2(b)]. In the case of scale-free networks, the network is formed by starting with an initial number of nodes, connected by links (Barabasi and Albert 1999). A new node is then introduced to the network, with a number of links between 1 and the initial number of links (which are used to connect this new node to the existing network). This random element, when generating links to connect the new node to the network, alters the total number of links in each network by a small amount. To generate networks with noticeably different levels of connectivity, the number of initial nodes needs to be altered. Because each network generated with the same number of initial nodes has approximately the same number of links, they have approximately the same value of APL, causing the clustering in Fig. 2(a) (i.e., each cluster is a group of networks with the same number of initial nodes). For small-world networks, the number of links in the network depends on the total number of nodes in the network and the number of initial neighbors that each node has (i.e., how many other nodes it is connected to) (Watts and Strogatz 1998). No new links are introduced into or removed from the network; the existing links are rewired using a rewiring probability, possibly altering one of the nodes that a link connects. Therefore, for networks with the same number of nodes, the number of initial neighbors will have a corresponding (and unchanging) number of links. The rewiring probability is kept constant in this paper, and the number of initial neighbors is changed to alter the connectivity of the network; therefore each cluster in Fig. 2(b) represents a network with a certain number of initial neighbors. This clustering of results is not as marked for random networks [Fig. 2(c)]. For random networks, each pair of nodes is considered in turn and a connection is made between them based upon the value of linking probability (the higher this value, the more likely it is that a link will be generated) (Erdös and Renyi 1960). Due to this probability element, networks that have the same value of linking probability can have a different total number of links, resulting in different values for APL. The weak clusters in Fig. 2(c) represent networks with different linking probabilities.

Having shown that at least part of graph theory is applicable to the analysis of physically based flow networks (using APL), the application of centrality measures to these networks is now considered.

The three most commonly used centrality measures—betweenness centrality, closeness centrality, and degree centrality—were developed by Freeman (1979). The betweenness centrality of a node is the proportion of all shortest APLs between pairs of other nodes that include this node (Freeman 1979; de Nooy et al. 2005) and is based on the concept that central nodes are included on the shortest APL of pairs of other nodes

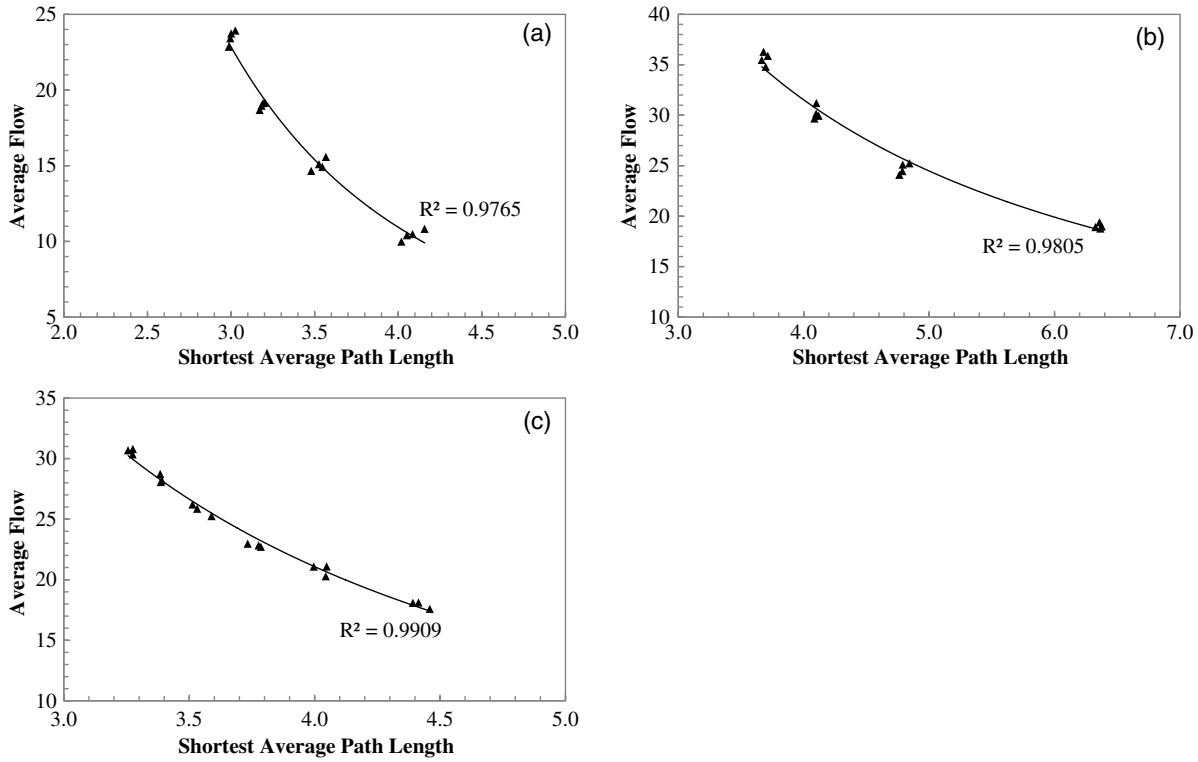


Fig. 2. Correlation between average flow and shortest average path length for 20 (a) scale-free; (b) small-world; (c) random networks, each with 1,000 nodes and different numbers of links; the average flow was calculated for each network by first summing the flow through (i.e., the inflow or the outflow as these are equal) the 990 demand nodes in the network and then dividing this number by the total number of demand nodes in the network (i.e., 990)

J. Infrastruct. Syst. 2013.19:157-165.

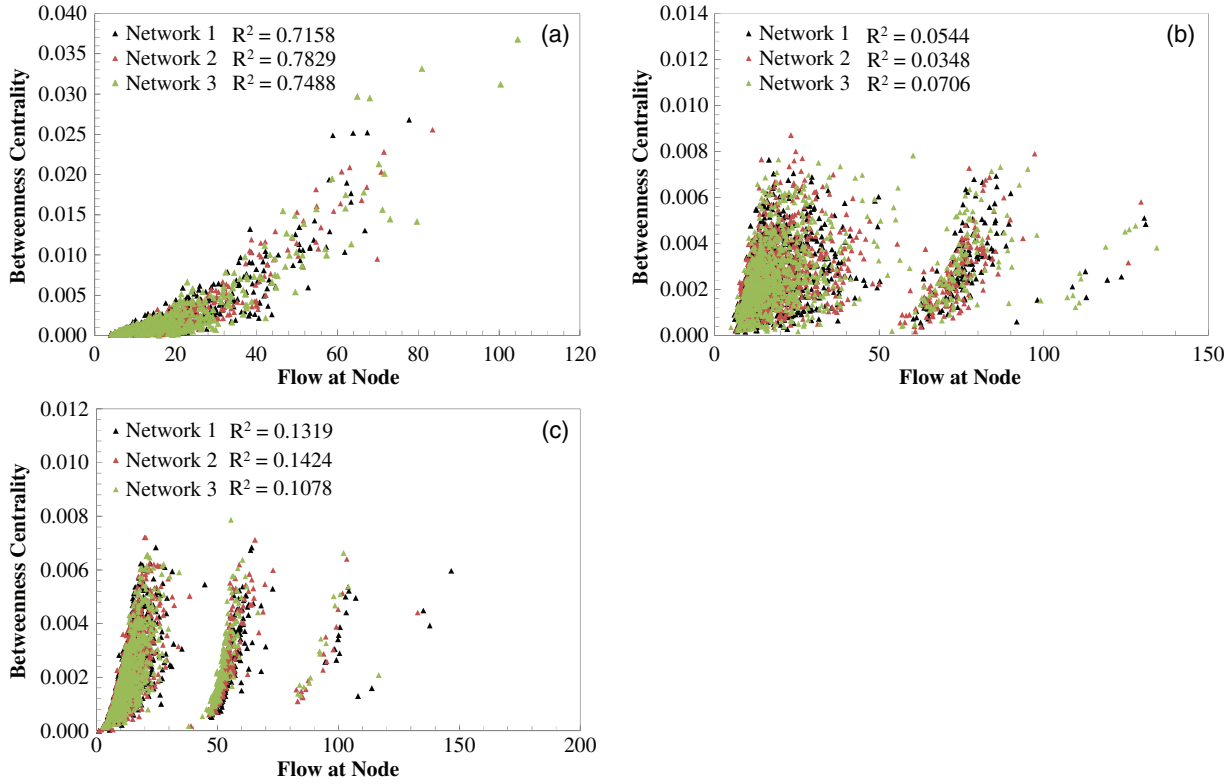


Fig. 3. (Color) Correlation between betweenness centrality and flow at corresponding node for (a) scale-free; (b) small-world; (c) random networks with 1,000 nodes and approximately 5,000 links

(de Nooy et al. 2005). The closeness centrality of a node is defined as the mean shortest path between that node and all other nodes reachable from it (nodes that tend to have a small shortest path length between other nodes in the network have a higher value of closeness) (Freeman 1979; de Nooy et al. 2005) and comprises the idea of speed of communication between pairs of nodes in a network (de Nooy et al. 2005; Cadini et al. 2009). The degree centrality of a node is equal to its degree (i.e., the number of links attached to that node) (Freeman 1979).

The same networks as were used previously are used here [i.e., the 60 × 1,000 node networks (Fig. 2)], and the flow through each demand node is calculated using the reduced complexity flow model, and this is correlated with the centrality of that node [calculated using Pajek (Batagelj and Mrvar 2003) for all three centrality measures]. Only the demand nodes are considered in this analysis because the flow in these is of primary concern; only 1% of the nodes in the network are supply nodes (i.e., 10 nodes). Each network has 990 demand nodes and therefore contributes 990 points to the graph. Because of this and to keep the figure clear, only results for three of the networks (chosen at random) for each centrality measure are presented; however, these are typical of the correlations achieved for the other networks.

Fig. 3 shows the correlation between betweenness centrality of a node and the flow through the same node for the three classes of network model. The results of these simulations show an R^2 value of around 0.7 for scale-free networks [Fig. 3(a)], indicating that the nodes with a high value of flow through them tend to be the nodes with a high value of betweenness. It is apparent that there is little or no correlation for the small-world [Fig. 3(b)] and random [Fig. 3(c)] networks (the R^2 values are between 0.0 and 0.2).

The three clusters of results for the small-world networks [Fig. 3(b)] and the four clusters of results for the random networks [Fig. 3(c)] can be explained by considering the proximity of demand nodes to the supply nodes. Those nodes that are directly connected to (one or more) supply nodes will have proportionately higher flows through them than those that are not connected because they must transfer flow through themselves to other nodes in the network that are not directly connected to a supply node. Each cluster [in Figs. 3(b and c)] contains nodes that are a specific number of links away from a supply node. For example [using Fig. 3(b)], the nodes in the far right cluster are directly connected to a supply node, whereas the far left cluster shows those nodes where the flow from the supply node has passed through three or more links. Fig. 4 shows this diagrammatically, where the supply node is indicated in red and three demand nodes in black. It can be seen that the demand node that is directly connected to the supply node is transferring flow through to the other two connected demand nodes and has a value of flow that is twice the value of

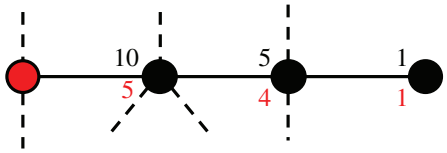


Fig. 4. (Color) Sample section of a network indicating a supply node (red) and three demand nodes (black); top number (black): flow through node; bottom number (red): amount of service provision required by that node (also equal to its degree); dotted lines: connections to other nodes in network (not included for simplicity); flows shown assume that other nodes in network do not require a proportion of the flow (this is assumed in this example for simplicity only and is not an assumption of the flow model itself)

J. Infrastruct. Syst. 2013.19:157-165.

its demand [this node would form part of the far right cluster in Fig. 3(b)]. The central demand node requires its own value of demand and is also transferring flow to the remaining demand node (on the far right) but has a significantly lower flow than the demand node directly connected to the supply node [and would form part of the central cluster in Fig. 3(b)]. The final demand node (far right) only requires its own value of demand and does not transfer this to other demand nodes, so its value of flow is equal to its degree [and would form part of the far left cluster in Fig. 3(b)].

Comparing the flow at a node and the closeness of that node (for the same generated networks used in Fig. 3) shows results similar to those in Fig. 3. The R^2 values for the scale-free networks [Fig. 5(a)] are around 0.8, indicating that the nodes that are central to the network also have a high flow through them. The small-world networks [Fig. 5(b)] and random networks [Fig. 5(c)] show little or no correlation between the two measures (with R^2 values between 0.0 and 0.2) but, similarly to Fig. 3, show the same clustering of results, explained by the proximity of supply nodes to demand nodes (Fig. 4).

Considering the final centrality measure, degree centrality, the R^2 value for scale-free networks is approximately 0.7–0.8, indicating that nodes with a high degree also have a high value of flow through them [Fig. 6(a)]. This can be explained by considering one of the assumptions that was made in the creation of the networks, namely, that the demand (of service) required by a node is proportional to the degree of that node. Considering this assumption it could be argued that higher flow is expected at nodes with a high degree than at nodes with a low degree, and Fig. 6(a) shows this to be the case. However, it is interesting to note in the case of the small-world [Fig. 6(b)] and random [Fig. 6(c)] networks that the demand nodes with a high degree are not necessarily the nodes with high flow through them. This can be explained by considering the proximity of the demand nodes to the supply nodes and also in the algorithms used to generate the networks. The main difference between the generation algorithms for scale-free networks, and small-world and random networks is the method used to assign links to connect pairs of nodes. The algorithm for generating scale-free networks includes a "rich-get-richer" component, meaning that nodes with a high degree "attract" the links from new nodes (Barabasi and Albert 1999); this component is not included in the algorithms for small-world and random networks (where the new links are attached to nodes based on a user-defined probability and not a measure of degree) (Erdös and Renyi 1960; Watts and Strogatz 1998). It is also worth noting that the high-degree nodes in scale-free networks tend to be attached to other high-degree nodes (as a result of the algorithm). Because the supply nodes are assigned to the network based on degree (the supply nodes being the top 1% of the highest degree nodes), these nodes tend to be linked to other high-degree nodes, resulting in a situation where those nodes that transfer the service to other nodes in the network are nodes with a high degree, suggesting the reason behind the correlation in Fig. 6(a) and the lack of correlation in Figs. 6(b and c).

Development of a New Technique to Identify Important Nodes in Networks

It is now demonstrated that centrality measures can be used to better establish which nodes are important to the functioning of a network (i.e., nodes that, when removed from the network, have a disproportionate effect on the remaining network). Because the simplified model was used to model flow-based problems in general rather than specific infrastructure networks, it may be argued that the simplification renders the analysis invalid; therefore,

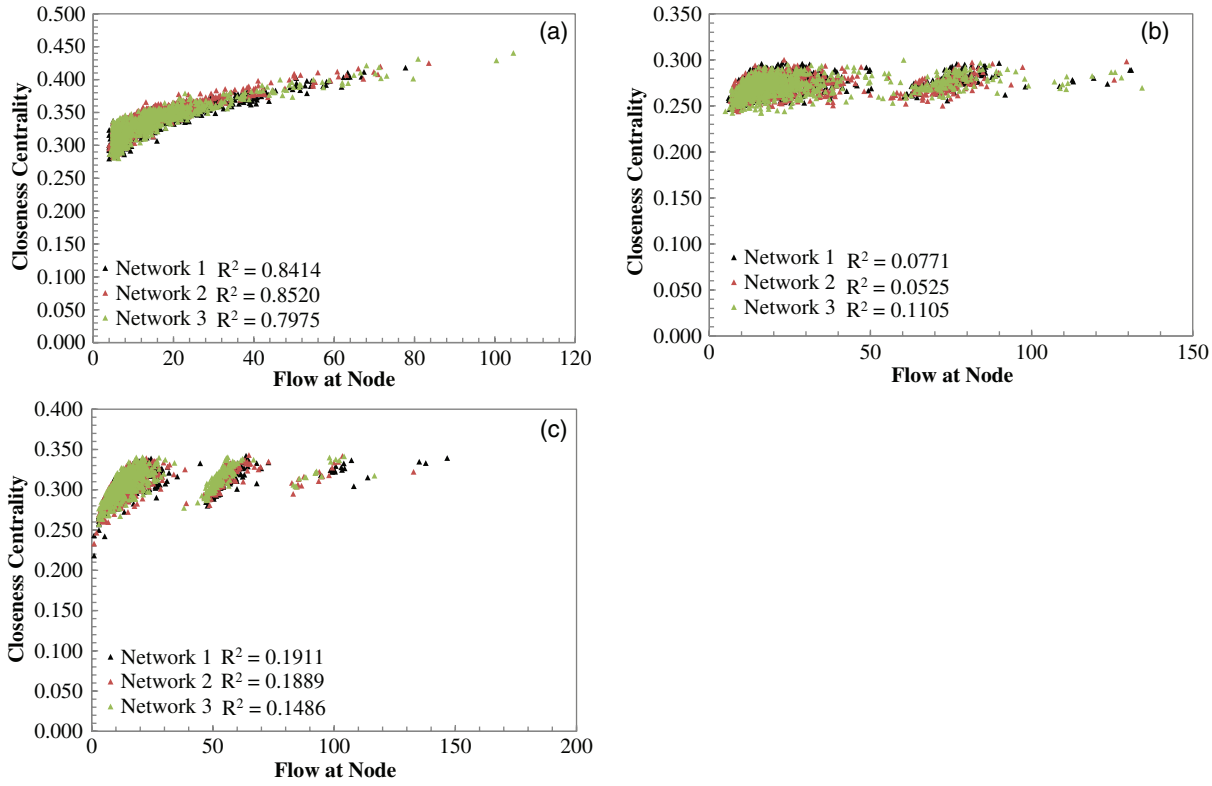


Fig. 5. (Color) Correlation between closeness centrality and flow at corresponding node for (a) scale-free; (b) small-world; (c) random networks with 1,000 nodes and approximately 5,000 links

J. Infrastruct. Syst. 2013.19:157-165.

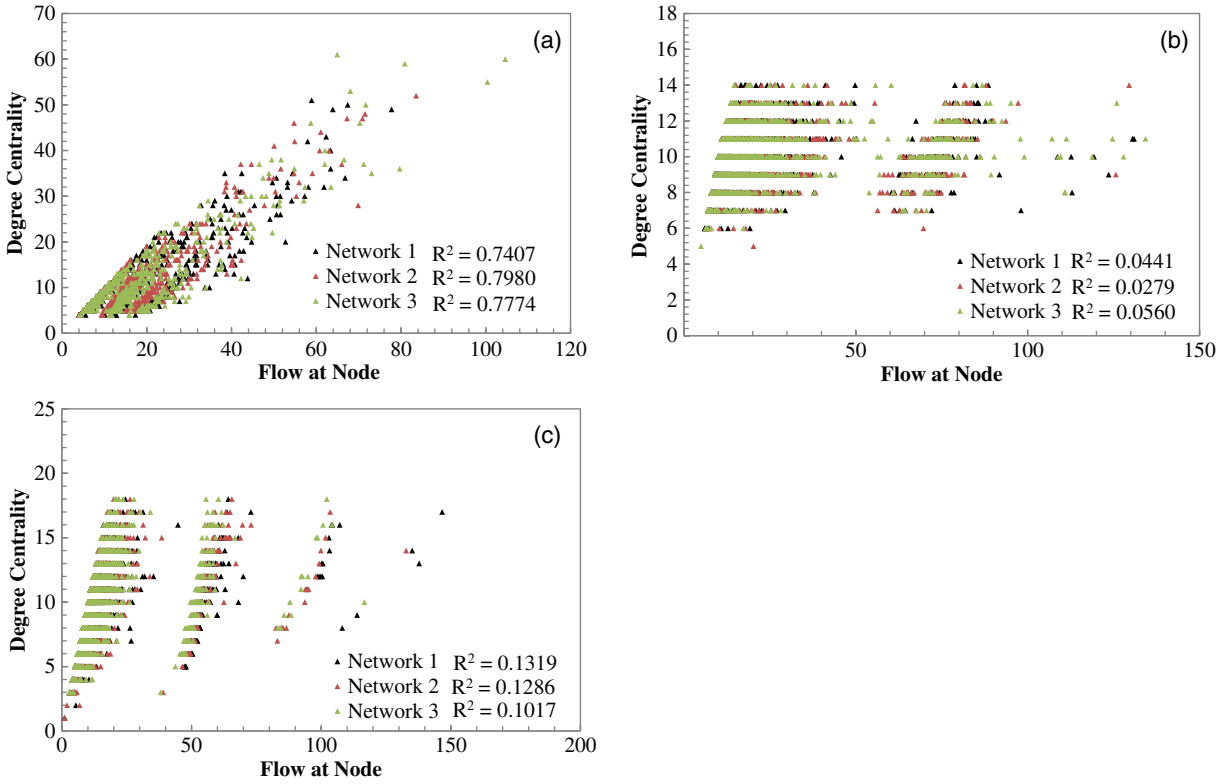


Fig. 6. (Color) Correlation between degree centrality and flow at corresponding node for (a) scale-free; (b) small-world; (c) random networks with 1,000 nodes and approximately 5,000 links

the focus will now be on a single type of infrastructure system, namely, a water distribution system, and the flows will be analyzed using a hydraulic model [EPANET (U.S. Environmental Protection Agency 2008)] in a sample network consisting of 15 nodes and 23 links [Fig. 7(a)]. It was decided to analyze a water distribution system, but another type of infrastructure system (an electrical distribution network, for example) could just as well have been chosen.

Because weighted networks are not considered in this paper, all links (pipes) are set to have the same value for each parameter (e.g., length, diameter, roughness coefficient). Again, it is assumed that the supply nodes have sufficient capacity to supply any service required and the demand nodes are assigned a value of demand based upon their initial degree (this demand does not change throughout the analysis; for example, if a connected node is removed, its degree will decrease, but the demand is kept constant).

The proximity of a demand node to the supply node will have a large effect on the flows in this node (previously explained). Depending on the network architecture, this could lead to a disproportionately large influence on the overall behavior of the network. To negate this effect, the concept of a "roving" supply node is introduced. It is implemented by conducting 15 series of tests on the sample network. In each test series, there is only one supply node and its location is fixed (e.g., at Node 1). The flows in the network are calculated, and then a demand node is removed and the change in flows in the network (this is one simulation) is calculated. This node is then replaced and another demand node is removed, and again the change in flow is calculated. This process is repeated until all demand nodes have been removed (resulting in 14 simulations for this test series). At the end of a test series, the position of this supply node is moved and the process is repeated. Again the process is repeated until all possible combinations have been tested and, therefore, all influences that the supply node can have on this particular network have been considered.

To quantify the changes in flows in the network, when removing demand nodes, the square root of the sum of the squares (SRSS) for the change in flow through each node is calculated. For each of the test series this value is correlated with different measures to assess the predictive skill of these in identifying the important nodes in the network.

Three measures and two combinations of these measures are used in this analysis to show that a combination of physically based and graph theory metrics increases one's predictive skill in identifying the important nodes in a network. First, the original flow through the node (the calculated flow through the node before removing any nodes) is used; this is a physically based metric that can be considered an indicator of the importance of a node in the network (i.e., nodes with a high flow through them are more likely to have a large impact on the network when removed). Therefore, this case is used as a benchmark for testing the predictive skill of graph theory metrics in choosing important nodes. Second, the degree of the node is used because it could be argued that the most connected node is the most important in the network. The third measure is betweenness centrality; because flow will choose the shortest path between areas of supply and demand, it could be argued that the measure, which takes into account the number of shortest APLs between pairs of other nodes, indicates the important nodes in the network. These measures are also combined to show that an improvement takes place in predictive capabilities in identifying important nodes. The first of these combined measures uses original flow and betweenness centrality; the original flow takes into account the position of the supply node (i.e., the connected nodes will have a higher value of flow through them, Fig. 4), and betweenness centrality considers the path of the flow through the network. To negate the effect of node degree on this relationship, the second combined measure divides this value by degree (i.e., it is

J. Infrastruct. Syst. 2013.19:157-165.

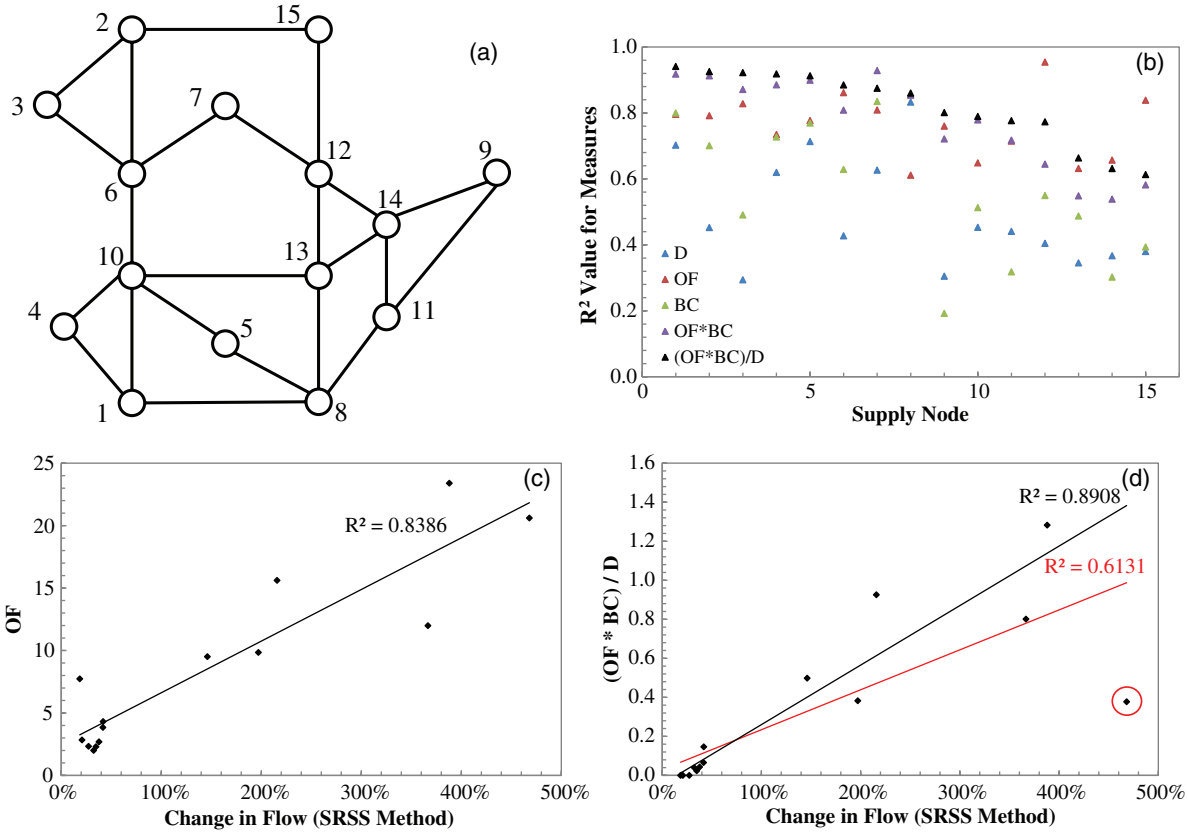


Fig. 7. (Color) (a) Sample network with 15 nodes (indicating node numbers); (b) comparison of R^2 value of measures for each position of supply node (D = degree, OF = original flow, BC = betweenness centrality); (c) original flow and change in flow (calculated using SRSS method) with Node 15 as supply node; (d) one combined measure and change in flow (calculated using SRSS method) with Node 15 as supply node; red line: linear line of best fit for all data points; black line: line of best fit for all data points with outlier removed (circled in red)

the product of the original flow and betweenness centrality, divided by the node degree).

For each simulation series the R^2 value is calculated for the correlation between the change in flow when a node is removed and each metric (i.e., it is the goodness of fit for the 14 simulations in each simulation series), shown in Fig. 7(b).

From the three individually applied measures it can be seen that the original flow (the baseline metric) is best at identifying vulnerable nodes (i.e., it is most strongly correlated with change in flow), followed by betweenness centrality and, finally, degree. There is a reasonable amount of scatter in the R^2 values, and so original flow is not universally the best indicator of vulnerable nodes; however, it has the least scatter associated with it, and so the predictive skill of this metric can be said to be less affected by the position of the supply node.

Considering the two combined measures, it can be seen that a measure that includes all three individual measures is superior in predicting the important nodes in the network, for the majority of simulations [Fig. 7(b)]. The reason for this is that flow-based metrics indicate the important components in a network for a given supply–demand scenario, while graph theory metrics indicate the importance of components for a given network architecture. When a node is removed, the flows are redistributed, and so the information provided by the flow metrics becomes less reliable. Graph theory metrics, on the other hand, provide information about the network in general and so are a better measure of the potential for node removal to have an effect.

Considering Fig. 7, there are two locations of supply node that result in the superiority of the original flow (baseline metric) (i.e., Nodes 12 and 15). In the case of the supply node located at Node 15, the removal of Node 2 has a disproportionate effect on the remaining network (creating an SRSS value of approximately 450%). This effect is not reflected in the modified measures used but is captured by the original flow measure because in this scenario the particular choice of supply and demand nodes overwhelms any effect that the network architecture has. Fig. 7(c) shows the correlation between the change in flow and the original flow when the supply node is Node 15. This figure shows a strong correlation between the two measures; however, plotting the change in flow against the second modified measure gives a significantly reduced correlation, due to the influence that the removal of Node 2 has on the network [Fig. 7(d)]. Because Node 2 was one of the two nodes connected to Node 15, it had a large through flow (to enable supply of the other nodes in the network), resulting in a high value of original flow, but not the combined measure (because Node 2 has a small degree and a low value of betweenness centrality). As a result, the new metrics significantly underestimate the importance of this node for the network. This illustrates that, although the proposed metrics do result in a superior ability to identify important nodes in a network, they are not infallible.

Conclusions

A reduced complexity flow model was presented and used to simulate the flow of services in three different classes of network (i.e., random, small-world, and scale-free). Because many infrastructure networks belong to the scale-free class (Da Costa et al. 2011),

J. Infrastruct. Syst. 2013.19:157-165.

it is argued that the results are applicable to infrastructure networks. The resulting flows were then used to test whether graph theory metrics could be used to inform one of the behaviors of infrastructure systems. The results of the simulations show that in all three classes of network there is a correlation between the average flow through the nodes of the network and the average path length of the network, indicating that at least parts of graph theory are applicable to the analysis of infrastructure networks. It was also shown that scale-free networks show a strong correlation between the three centrality measures considered in this paper and the flow through the corresponding node. In contrast, both small-world and random networks showed little or no correlation between the centrality measures and flows through the nodes. To demonstrate the utility of using graph theory metrics in real flow networks, a hydraulic model (EPANET) was used to analyze how flows are redistributed when nodes are removed from a sample 15-node network (i.e., nodes are ranked in order of the effect they have when removed from the network and compared to various measures). In these simulations, it was shown that a combination of both physically based and graph theory metrics provide greater predictive skill in this task than physically based measures alone. The reason for this is that flow-based metrics indicate the important components in a network for a given supply–demand scenario, whereas graph theory metrics indicate the importance of components for a given network architecture. A reduced complexity model was used in an attempt to consider all types of flow problems rather than a specific one (such as a hydraulic network); however, the applicability of the new metrics to these other real infrastructure networks still needs to be proven.

Acknowledgments

This research was funded by the Engineering and Physical Sciences Research Council, UK, and its support is gratefully acknowledged. All of the networks used in this paper were generated using *Network Workbench*, the shortest average path length was also calculated using *Network Workbench*, and the three centrality measures were calculated using *Pajek* (Batagelj and Mrvar 2003).

References

Albert, R., Jeong, H., and Barabasi, A. L. (2000). "Error and attack tolerance of complex networks." *Nature*, 406(6794), 378–382.

Albert, R., and Barabasi, A.-L. (2002). "Statistical mechanics of complex networks." *Rev. Modern Phys.*, 74(1), 47–97.

Barabasi, A. L., Albert, R., and Jeong, H. (2000). "Scale-free characteristics of random networks: The topology of the world-wide web." *Phys. Stat. Mech. Appl.*, 281(1–4), 69–77.

Barabasi, A.-L., and Albert, R. (1999). "Emergence of scaling in random networks." *Science*, 286(5439), 509–512.

Barabasi, A.-L., and Oltvai, Z. N. (2004). "Network biology: Understanding the cell's functional organization." *Nat. Rev. Genet.*, 5(2), 101–113.

Batagelj, V., and Mrvar, A. (2003). "Pajek: Program for large network analysis." ⟨http://vlado.fmf.uni-lj.si/pub/networks/pajek⟩ (Jul. 1, 2011).

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., Hwang, D. U. (2006). "Complex networks: Structure and dynamics." *Phys. Rep.*, 424(4–5), 175–308.

Cadini, F., Zio, E., and Petrescu, C.-A. (2009). "Using centrality measures to rank the importance of the components of a complex network infrastructure." *Critical information infrastructure security*, R. Setola and S. Geretshuber, eds., Springer, Berlin, 155–167.

Choi, J. H., Barnett, G. A., and Chon, B.-S. (2006). "Comparing world city networks: a network analysis of Internet backbone and air transport intercity linkages." *Global Network.*, 6(1), 81–99.

Crucitti, P., Latora, V., and Marchiori, M. (2005). "Locating critical lines in high-voltage electrical power grids." *Fluctuation Noise Letters*, 5(2), L201–L208.

Crucitti, P., Latora, V., and Porta, S. (2006). "Centrality in networks of urban streets." *Chaos*, 16(1), 015113.

Da Costa, L. F., et al. (2011). "Analyzing and modeling real-world phenomena with complex networks: A survey of applications." *Adv. Phys.*, 60(3), 329–412.

De Nooy, W., Mrvar, A., and Batagelj, V. (2005). *Exploratory social network analysis with Pajek*, Cambridge University Press, Cambridge, UK.

Erdös, P., and Renyi, A. (1960). "On the evolution of random graphs." *Publ. Math. Inst. Hung. Acad. Sci.*, 5, 17–61.

Everett, M. G., and Borgatti, S. P. (1999). "The centrality of groups and classes." *J. Math. Sociol.*, 23(3), 181–201.

Freeman, L. C. (1979). "Centrality in social networks conceptual clarification." *Social Networks*, 1(3), 215–239.

Genesi, C., Granelli, G., Innorta, M., Marannino, P., Montagna, M., and Zanellini, F. (2007). *Identification of critical outages leading to cascading failures in electrical power systems*, IEEE, New York.

Guimera, R., Mossa, S., Turtschi, A., and Amaral, L. A. N. (2005). "The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles." *Proc. Natl. Acad. Sci. U.S.A.*, 102(22), 7794–7799.

Lewis, T. G. (2009). *Network science: Theory and practice*, Wiley, Hoboken, NJ.

Milgram, S. (1967). "The small-world problem." *Psychol. Today*, 1(1), 61–67.

Newman, M. E. J. (2003). "The structure and function of complex networks." *SIAM Rev.*, 45(2), 167–256.

Newman, M. E. J. (2004). "Analysis of weighted networks." *Phys. Rev. E*, 70(5), 056131.

Novak, P., Guinot, V., Jeffrey, A., and Reeve, D. E. (2010). *Hydraulic modelling—an introduction: Principles, methods and applications*, Spon Press, London.

Network Workbench [Computer software]. Indiana Univ., Bloomington, IN; Northeastern Univ., Boston; and Univ. of Michigan, Ann Arbor, MI, ⟨http://nwb.slis.indiana.edu⟩.

Opsahl, T., Agneessens, F., and Skvorets, J. (2010). "Node centrality in weighted networks: Generalizing degree and shortest paths." *Social Networks*, 32(3), 245–251.

O'Rourke, T. D. (2007). "Critical infrastructure, interdependencies, and resilience." The Bridge, 27–29.

U.S.–Canada Power System Outage Task Force. (2004). *Final Rep. on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations*, Washington, DC.

U.S. Environmental Protection Agency. (2008). "EPANET." ⟨http://www.epa.gov/nrmrl/wswrd/dw/epanet.html⟩ (Jul. 1, 2011).

Watts, D. J., and Strogatz, S. H. (1998). "Collective dynamics of 'small-world' networks." *Nature*, 393(6684), 440–442.

J. Infrastruct. Syst. 2013.19:157-165.

APPENDIX C

Network Theory for Infrastructure Systems Modelling

Engineering Sustainability
Volume 166 Issue ES5

Network theory for infrastructure systems modelling
Dunn, Fu, Wilkinson and Dawson

ice | proceedings

Proceedings of the Institution of Civil Engineers
Engineering Sustainability 166 October 2013 Issue ES5
Pages 281–292 http://dx.doi.org/10.1680/ensu.12.00039
Paper 1200039
Received 08/11/2012 Accepted 06/06/2013
Keywords: disaster engineering/infrastructure planning/safety & hazards

ice Institution of Civil Engineers publishing

Network theory for infrastructure systems modelling

Sarah Dunn MEng, GradICE
Researcher, School of Civil Engineering & Geosciences, Newcastle University, Newcastle upon Tyne, UK

Gaihua Fu BSc, PhD
Research Associate, School of Civil Engineering & Geosciences, Newcastle University, Newcastle upon Tyne, UK

Sean Wilkinson MEng, PhD
Senior Lecturer, School of Civil Engineering & Geosciences, Newcastle University, Newcastle upon Tyne, UK

Richard Dawson MEng, PhD
Chair of Earth Systems Engineering, School of Civil Engineering & Geosciences, Newcastle University, Newcastle upon Tyne, UK

Currently, there is a great deal of interest in assessing the resilience of infrastructure systems. Much of this interest stems from the realisation that these systems are not only critical to civil defence but also, given the correct set of circumstances, can fail catastrophically. Three case studies are presented that show how network theory, which has been successfully applied to other fields, can also be used to help understand potential vulnerabilities in infrastructure systems. Through these case studies it is shown that traditional network theory can be extended to analyse infrastructures that are large, spatially distributed systems, or that carry flows of resources or are interconnected with other infrastructure systems. These methods demonstrate how this approach can help infrastructure designers, owners and operators to make rapid assessments of vulnerabilities in their systems and to identify components that are more important to the functioning of the these networks. Furthermore, this approach provides a basis for identifying and prioritising appropriate measures to improve the reliability of infrastructure at the systems scale.

1. Introduction

Infrastructure systems, such as water, transport, communication and energy networks, are crucial to the functioning of a modern society (Murray and Grubesic, 2007). The reliability and integrity of these physical assets and the services they provide is vital for ensuring national security, public health and productivity (HM Treasury and Infrastructure UK, 2011). As society becomes more developed, they not only place greater reliance on these systems but also become increasingly complex, so they have the potential to create larger impacts on both the environment that they are coupled to and the socioeconomic changes that they (in part) enable. This increased complexity and reliance is making these networked infrastructure systems harder to manage (Royal Academy of Engineering, 2011) as disruptive events can be propagated between networks and thus spread their impact far beyond the immediate footprint of a disturbance. For instance, the 2007 UK floods led to the inundation of energy and water facilities in the flood plain. This subsequently led to a regional loss of these services as well as the loss of electricity-dependent information communication technology (ICT) networks and reduced emergency response capacity as a result of transport network disruption (Pitt, 2008). On 28 September 2003 in Italy, a blackout that affected much of the country (Rosato *et al.*, 2008) was magnified by bi-directional interactions between ICT and energy systems because the ICT systems required an electricity supply, while power stations were dependent on the communication systems for their operation (Buldyrev *et al.*, 2010).

Such events, that have manifested themselves over large spatial areas and across infrastructure sectors, have highlighted the importance of developing earth system engineering approaches to improve the management and analysis of physical infrastructure systems. Traditional approaches to engineering design do not capture the necessary system scale behaviour, requiring the development of new broad scale analyses that can capture interactions between physical infrastructures and the natural and social systems to which they are intrinsically coupled. Network theory provides a rigorous mathematical basis for the analysis of connected elements and enables aspects of the aggregate performance of networked systems to be rapidly calculated. It therefore has great potential as an earth systems engineering tool.

Network models are increasingly being employed to help us understand social (Amaral *et al.*, 2000; Arenas *et al.* 2003; Newman *et al.*, 2002), neural (Sporns, 2002; Stam and Reijneveld, 2007), biological (Rual *et al.*, 2005) and computer science networks (Valverde and Solé, 2003). More recent work has applied network theory to analyse infrastructure systems (Holmgren, 2006; Lhomme *et al.*, 2013; Wilkinson *et al.*, 2012)

and demonstrated their potential to support broad scale infrastructure network design and management.

After a brief introduction to network theory, this paper presents the results of three applications of network analysis to demonstrate using the flexibility and scalability of the method to understand a wide range of infrastructure problems. The first case study subjects a spatial network to different hazards, aiming to assess the resilience of the network to each hazard. The second case study shows the role of supply and pipe (network edge) resistances in mediating infrastructure performance. Finally, the authors demonstrate how these approaches can be extended to consider the implications of interdependencies between networks before discussing the potential of network modelling for earth systems engineering and for supporting the design and management of infrastructure systems.

2. Network analysis and graph theory systems for infrastructure

Network theory is an area of applied mathematics and part of graph theory that concerns itself with the representation of relations between discrete objects. Before describing how to build a network model, it is useful to define some basic terminology relevant to all the case studies. A network is a set of items, referred to as nodes, which are connected by links. There may be several types of node or link in a network with differing properties. The degree of a node is the number of connections it has with other nodes and the degree distribution of a network is the probability distribution of these degrees over the whole network (see Figures 1–3).

2.1 Infrastructure as a network

There has been a great deal of recent work using network theory to analyse naturally occurring networks, including infrastructure systems. Most of this research has focused on defining the degree distribution of the network by studying its nodal connectivity and using this information to identify its network class. In network theory there are four main classes of network, each of which describes a different pattern of nodal connectivity

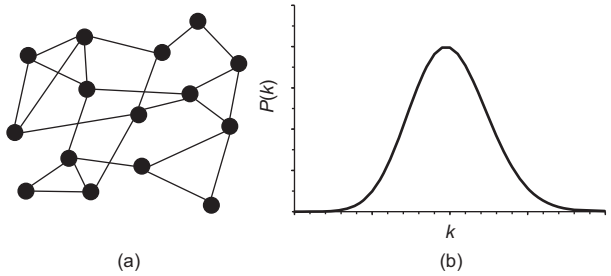


Figure 1. (a) A sample random network and (b) the shape of its degree distribution

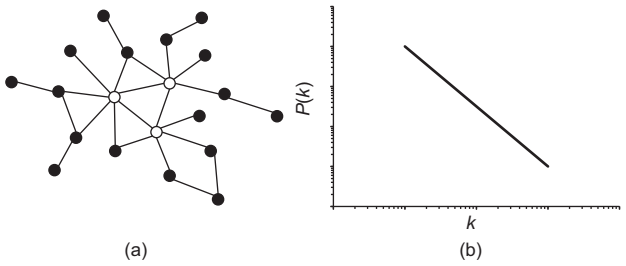


Figure 2. (a) A sample scale-free network and (b) its degree distribution (plotted on a log–log axes)

and has distinctive degree distributions, which are introduced below. That many infrastructure networks fit into only a small number of network classes may be surprising, as an airline network appears to be significantly different from an electrical power grid, but in fact they share similar characteristics.

The first documented network class was the random graph model (Erdos and Renyi, 1960) (Figure 1). Although this type of network has been shown to be a poor representation of real-world network architectures (Newman, 2003), random networks are widely studied and, in part because nodes have a similar degree that follows a Poisson distribution (Figure 1(b)), are often used for comparison with more structured networks (Batagelj and Brandes, 2005; Lewis, 2009) (Figure 1).

To model real-world systems more accurately, Watts and Strogatz (1998) modified the random graph model using the concept of six degrees of freedom (Milgram, 1967) to form

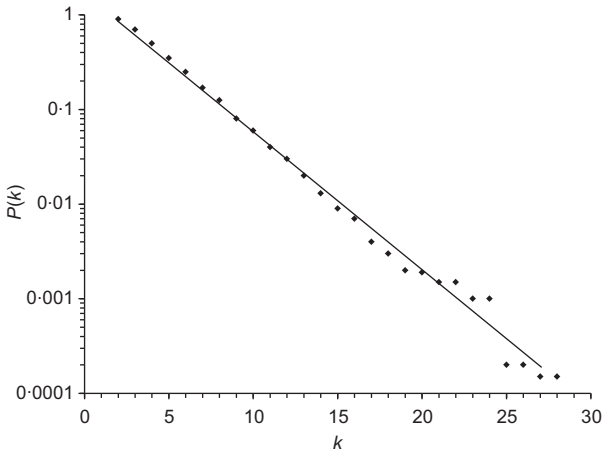


Figure 3. Degree distribution for the North American power grid: a real-world example of an exponential network plotted on a log-*y* axis (using data from Deng *et al.* 2007)

small-world networks. The main characteristic of small-world networks is that most nodal pairs are not directly connected, but can be reached by way of traversing very few links. The degree distribution is very similar to that of a random network (Figure 1(b)) (Barthelemy, 2011). Small-world networks have been shown to replicate a range of real-world networks, including subway systems (Latora and Marchiori, 2002).

Many real-world networks (including the world wide web (Barabasi and Albert, 1999; Barabasi *et al.*, 2000)) tend to form a power law degree distribution, more commonly known as a scale-free network. These are characterised by a small number of highly connected nodes (nodes with a high degree) and a large number of poorly connected nodes (nodes with a small degree), as shown in Figure 2.

Other real-world networks such as power grids have been found to have an exponential degree distribution and are termed exponential networks (Albert *et al.*, 2004; Amaral *et al.* 2000; Bompard *et al.*, 2011; Liu and Tang, 2005). The degree distribution for an exponential network is shown in Figure 3.

Some real-world networks do not neatly fit one network class in particular, as they include elements from several classes. The most well documented of these are air traffic networks (Figure 4(a)), which include elements of both scale-free and exponential network architectures. Their network architecture has been classed as a truncated scale-free distribution (or a scale-free distribution with an exponential tail) (Wilkinson *et al.*, 2012).

The degree distribution of a network can also provide insight into network resilience. For example, the architecture of scale-free networks is such that they are quite resilient to random hazards but vulnerable to targeted attack. This is because a random hazard has a small chance of removing one of these few highly connected nodes in the network, while a targeted attack will often remove these nodes in seeking to cause maximum disruption to the network (Albert *et al.*, 2000).

2.2 Network model development

Transforming a real-world infrastructure network into a network model and assessing its hazard tolerance can be broken down into four steps.

Step 1 is to define basic network structure. This involves abstracting the key features of the real-world infrastructure system as a network model. According to the issue under investigation or the availability of data, two approaches are available. In case study 1 it is possible to apply (a), but for case studies 2 and 3, where more general insights are sought, only option (b) is applicable.

(*a*) When the analysis of the existing network is the only objective, this is conceptually relatively straightforward: components of an infrastructure system responsible for consuming, generating or regulating a resource or service are represented as nodes. Network links connect these nodes if there is a mechanism for them to exchange their resource or service. This might be a logical supply (e.g. a communication signal) or a flow of resource (e.g. power, water or vehicles).

(*b*) Frequently, it is of interest to analyse systems that are representative of real-world networks in order to test the resilience of alternative network structures and adapta-

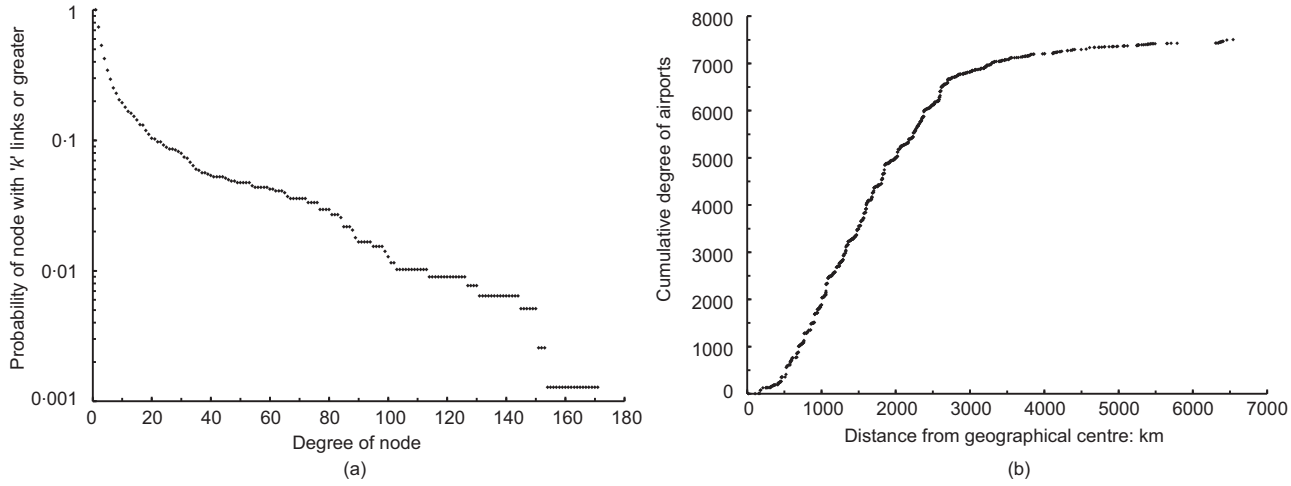


Figure 4. Graphs showing (a) the degree distribution and (b) the spatial degree distribution for the North American air traffic network

tions. If required, network generation algorithms (described in detail by Barabasi and Albert, 1999; Erdos and Renyi, 1960; Liu and Tang 2005; and Watts and Strogatz, 1998) can be used to produce synthetic but realistic networks according to rules that define properties such as spatial distribution and connectivity.

Step 2 is to define component behaviour. Different infrastructure systems, and indeed their individual components, exhibit a range of engineering behaviour and subsequently mediate the performance of the network. For example, pipes and wires typically have varying capacities. Likewise, individual structures have different supply capabilities, demands and likelihoods of failure under extreme conditions. Network models are flexible and can be parameterised to represent only limited physical processes (e.g. a component is on or off), and are therefore computationally very efficient, but they can also incorporate detailed engineering behaviour. For example, in case study 2 flow is introduced into a network model. This step is crucial for the design of the network analysis as it is important to provide enough detail to capture important system behaviour for the issue under investigation, while avoiding unnecessary complexity.

Step 3 is to subject the model to a series of disruptions. To understand system performance it is crucial to analyse a series of attack strategies that represent different possible hazards or events. These could include random failures (e.g. corresponding to a lack of maintenance), a contagion (e.g. representing a computer virus in ICT systems), a targeted attack at an important location (e.g. representing a terrorist attack) or a spatial hazard (e.g. a flood or wind storm).

Step 4 is to analyse subsequent performance. This final stage is to quantify the impact of each disruption on the infrastructure network. A prerequisite to this is the selection of appropriate metrics to quantify the change in performance of the network. These might measure subsequent system size (e.g. the number of remaining components), output (e.g. a drop in total power supplied) or impact (e.g. the number of people without service).

In this paper the three case studies are used to demonstrate how this four-step process can be applied to analyse a range of infrastructure performance issues. For clarity, one issue is isolated in each case study. The first case study considers the effects of the spatial properties of the infrastructure network, the second incorporates resource flows through a network and the third considers interdependency between two infrastructure networks. In reality many infrastructures might include all of these, and other, factors. However, by presenting three different studies it is possible to explore the significance of infrastructure performance to each factor separately and also demonstrate the flexibility of network modelling for the large-scale analysis of infrastructure systems.

3. Case study 1: using network topology to identify vulnerability in binary networks

In case study 1 the authors demonstrate how a network model of the North American air traffic network is created and consider how the spatial structure of the network affects its hazard tolerance. This network is subjected to three different types of hazard and the change in performance/connectivity of the network is quantified using graph theory metrics.

The North American air traffic network consists of 781 airports and 3751 air routes (the data were obtained from Openflights (2010)). To transform this air traffic network into a network model the airports are modelled using nodes and the connecting air routes are modelled using links.Using the network model, the degree of each node can be easily calculated, as it is equal to the number of links (air routes) attached to it and from this the degree distribution can be obtained (Figure 4(a)). From Figure 4 it can be seen that the network forms a truncated scale-free distribution, similar to other air traffic networks and, as discussed previously, should be resilient to random hazard but vulnerable to targeted attack.

The spatial degree distribution of these nodes (airports) has also been plotted (Figure 4(b)). This distribution was obtained by first calculating the geographical centre of the airports (weighted by their degree) and then plotting the cumulative degree of airports within a given radius. For the North American air traffic network the geographical centre of the network is located in Missouri, USA (approximately 190 km west of St Louis). The spatial distribution of airports in the North American air traffic network can be seen visually in Figure 5. This figure also indicates the degree of the node (the larger the circle the higher the degree) and the geographical centre of the network. From Figure 5 it can be seen that the high degree airports (or hub airports) are fairly well dispersed throughout the North American states but are less evident in northern Canada.

The resilience of this network is assessed by exposing it to three different types of hazard to assess its hazard tolerance under a range of conditions, as listed below.

- *Random node failure* – nodes are removed randomly from the network.
- *Degree attack* – nodes are removed from the network in the order of the highest to lowest degree. Previous studies have used this attack strategy to simulate a targeted attack, that is, the worst-case scenario.
- *Spatial hazard* – this hazard is based entirely upon the spatial layout of the network (unlike the other two attack strategies,

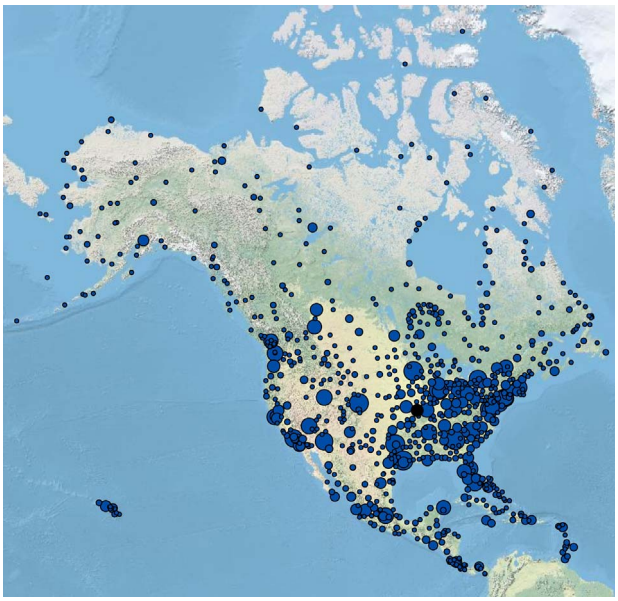


Figure 5. The location of real-world North American airports, where the size of the node indicates its degree (i.e. the number of air routes attached to it) (the larger the node the higher the degree)

which are based upon topological measures). For both networks the hazard starts in the geographical centre of the North American air traffic network (Figure 4(b) and Figure 5) and then grows outwards, removing nodes in order of distance from the geographical centre.

Following failure, nodes are removed from the network, which in turn will remove their connecting links (as it is not possible to operate an air route to a closed airport). To assess the hazard tolerance of the North American air traffic network to these three hazard types the percentage of links removed have been plotted against the percentage of nodes removed (Figure 6(a)). For the spatial hazard the percentage of links removed have also been plotted against the radius of the hazard, expressed as the percentage of distance from the geographical centre of the North American air traffic network to the edge of the network (Figure 6(b)). Two network theory measures have also been applied to the degraded networks to observe how the connectivity changes when different hazards are applied. The number of clusters is used to quantify how many unconnected parts (or clusters) that the network has broken into and the maximum cluster size (MCS) is used to indicate the size of the largest cluster in the network (Figures 6(c) and 6(d)).

From these results, it is clear that the degree attack strategy has the most devastating effect to the North American air traffic network, both in terms of the higher percentage of links removed for the same percentage of nodes removed (Figure 6(a)) and a significantly lower MCS (Figure 6(c)). This seems intuitive, given the degree distribution of the network and considering the presence of a few highly connected nodes in the network.

The results for the random node failure and the spatial hazard to the network are broadly similar. This is due to the spatial dispersion of high degree nodes in the North American air traffic network, which can be seen in Figure 5. Therefore, to remove one high degree node a large proportion of low degree nodes must also be removed, which produces similar cluster sizes to a random attack. This spatial dispersion arises from the existence of a number of separate, densely populated areas across the USA (for example, the two large population areas on the east and west coasts). Given the spread of high degree airports, a hazard that is seeded from the sparsely populated centre of the USA is unlikely to be a worst-case location. Shifting the spatial hazard over a location with more high degree airports (e.g. along the east coast) the network's performance would be quite different, as has been shown for the analysis of the European air traffic network by Wilkinson *et al.* (2012).

4. Case study 2: using network topology to identify vulnerability in a flow-based network

The first case study does not consider passenger, freight or aircraft movements. Instead, the effective proportion of the network following a disruption was considered. Given the availability of people, freight and aircraft movements, this analysis could be extended to incorporate these issues using the approach described in case study 2. Here, using a synthetic network of $n = 15$ nodes and 23 links for illustrative purposes, flow is incorporated into the network analysis. In the previous study degree was a suitable proxy for identifying important nodes but when flow is also considered this ranking changes.

Flow around this network model is simulated using the reduced complexity flow model of Dunn and Wilkinson (2012). This model has been shown to represent the flows in infrastructure networks in general, rather than focusing on the flows in a specific type of infrastructure system. Therefore, the present sample network could represent such networks as a power grid or a water distribution system. To generate flow around the network, one node is designated as the supply node (in the case of a water distribution system this would be the reservoir) and the remaining nodes as demand nodes (areas of housing requiring a supply of water, for example). The value of demand is assigned to the demand nodes in proportion to their degree. Given suitable water infrastructure data this demand would be the actual amount of service required by the node. It is assumed that the supply node has enough capacity to meet

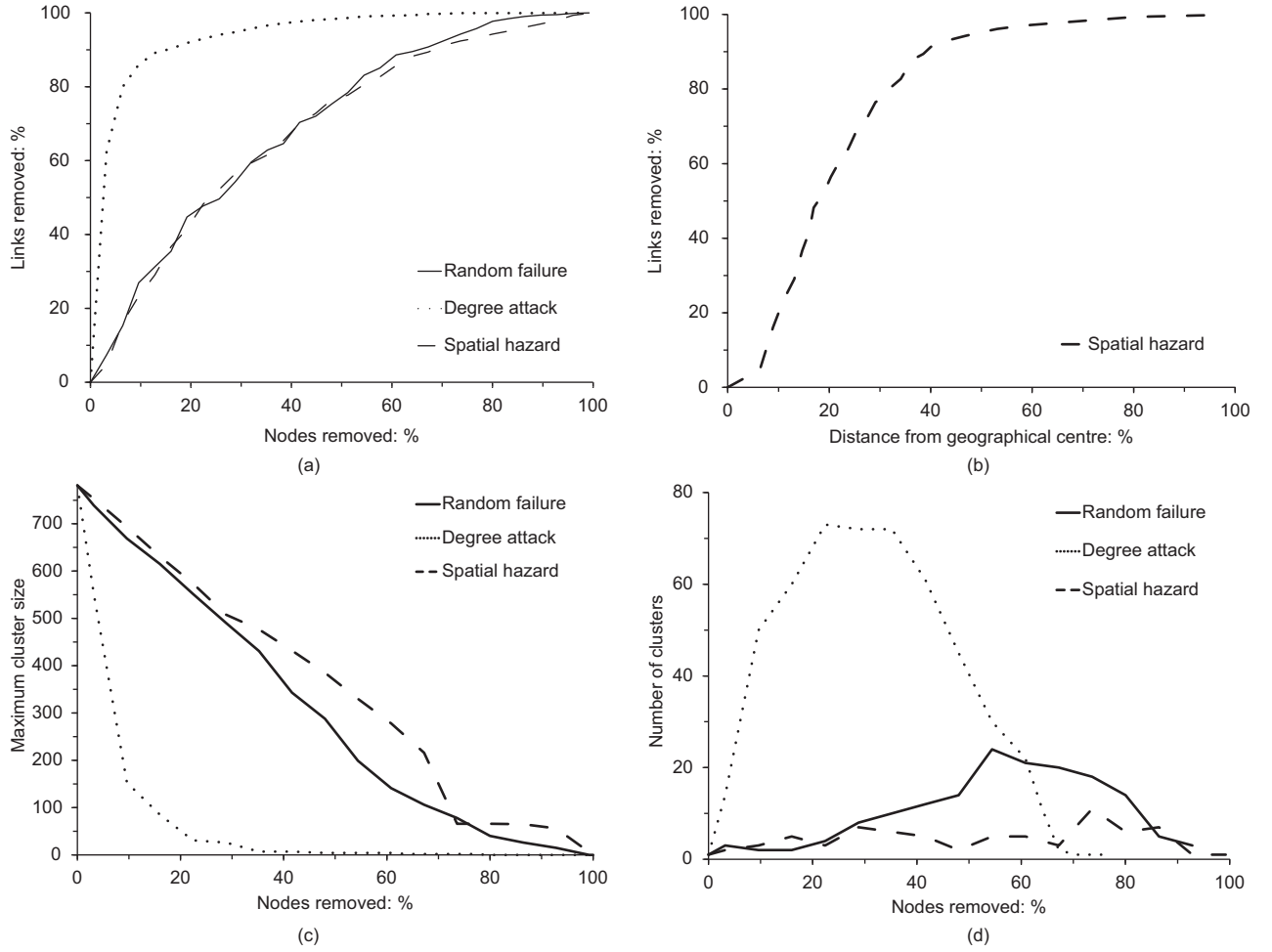


Figure 6. The response of the North American air traffic network to three disruptive events

the demand of the other nodes in the network (e.g. for a water distribution network, it is assumed that the reservoir contains enough water to supply the required demands).

In their study Dunn and Wilkinson (2012) were not considering weighted networks, and therefore set the weight of each link to be equal (also equalling the resistances of each link in the reduced complexity flow model). The weight of a link can be used to represent different pipe lengths and/or resistances in a water distribution network, for example. Here the present authors consider the impact of flow on the ranking of vulnerable components in the network and therefore alter the weight of each link using two methods. The first method assigns weight to the links based on their proximity to the supply node (Figure 7(a)). A link that is connected to the supply node will have a resistance of 1, links that are connected to these links have a resistance of 2 and so on. In the second method, values of weight/resistance are assigned to the links randomly (Figure 7(b)).

The authors also use the concept of a roving supply node used by Dunn and Wilkinson (2012). In the absence of a real-world network this method is used to negate the effect that the proximity of the supply node has to the demand nodes (i.e. demand nodes directly connected to the supply node will not only have their demand flowing through them but will also transfer flow to those not directly connected to the supply node). The vulnerability of each node is determined by analysing the $n - 1$ possible demand node failures for each of the n ($n = 15$ here) possible supply node locations (210 simulations in total). The location of the supply node, v_{si}, is fixed (e.g. at node $i = 1$, as shown in Figure 7) and the flows across the network as a function of this supply node location, $Q(v_{si})$, are evaluated. A single demand node, v_d, is removed and

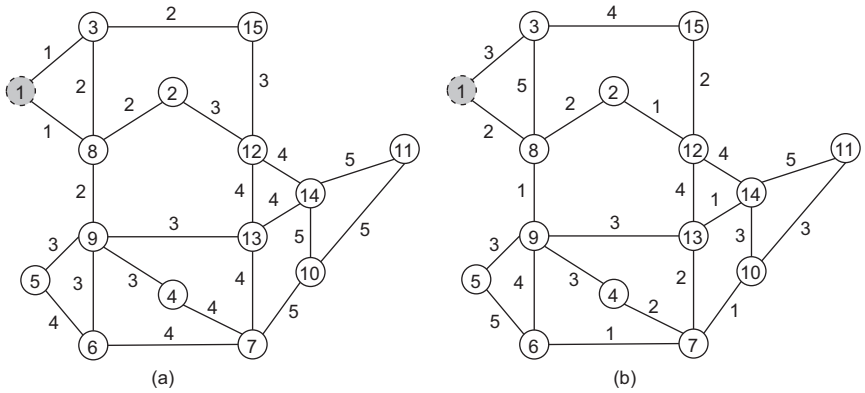


Figure 7. The synthetic network, with the links weighted (a) with distance and (b) randomly

the flows as a function of this diminished network, $Q(v_s,v_d)$, recalculated. Flows are subsequently calculated for each of the n possible supply node locations and $n-1$ single demand node failures to understand the influence that the supply node can have. The change in flow over the entire network, ΔQ, for the ith supply node is calculated as the square root of the sum of the squares of the change in flow across the remaining demand nodes in the network.

$$1. \quad \Delta Q(v_{si}) = \sqrt{\sum_{j=1,\, j\neq 1}^{n} \left(Q_j(v_{si}) - Q_j(v_{si},v_d)\right)^2}$$

To test the predictive skill of the model, $\Delta Q(v_{si})$ is correlated against the original flow, Q_j (the flow through the demand node prior to its removal), node degree (k_j), weighted betweenness centrality, $C(v_j)$, and a combined measure as alternative metrics of network performance. The R^2 from these correlations is plotted in Figure 8. The betweenness centrality of a node is equal to the number of shortest paths between all other nodes that pass through the node (Freeman, 1979; Lewis, 2009). As flow preferentially chooses the shortest path between areas of supply and demand it could be argued that the measure that accounts for the shortest distance between pairs of other nodes indicates the important nodes in the network. The $C(v_j)$ is calculated as follows (Brandes, 2001)

$$2. \quad C(v_j) = \sum_{v_j \neq v_a \neq v_b} \frac{c(v_a, v_b, v_j)}{c(v_a, v_b)}$$

where $c(v_a, v_b)$ is the number of shortest paths between a pair of nodes v_a and v_b and $c(v_a, v_b, v_j)$ is the number of shortest paths from v_a to v_b that pass v_j. The final measure used is a combined measure, CM_j, developed by Dunn and Wilkinson (2012), and again this measure is modified to account for the weight/resistance of each link.

$$3. \quad CM_j = \frac{Q_j \times C(v_j)}{v_j}$$

When the network is unweighted, Dunn and Wilkinson (2012) showed that this combination of Q_j (a physically based measure) and betweenness centrality (a measure derived from graph theory) improved the predictive skill at identifying vulnerable nodes (Figure 8).

First, the skill of each method compared to the others is shown for each position of the supply node (but the results are ranked in descending order for the CM_j to enable an easier comparison) (Figures 8(a) and 8(c)). Each measure is also ranked individually to identify the performance of each measure for ranking the most vulnerable nodes (Figures 8(b) and 8(d)).

For the networks where the link weights/resistances were added with distance from the supply node, the CM_j appears to most consistently identify the vulnerable nodes (Figure 8(a)). The measures of Q_j and $C(v_j)$ achieve better correlations for a few positions of the supply node, but also noticeably weaker in most other correlations. Ranking all the measures (Figure 8(b)) shows that the degree of a node is not a good indication of the vulnerability of that node, defined as the change in flow across the network after its removal.

The combined measure appears to most effective, although not consistent, at identifying the most important nodes for overall network performance in both situations. Ranking these results, for all measures, shows that $C(v_j)$ is not a good indicator of node vulnerability, which therefore reduces the performance of the combined measure.

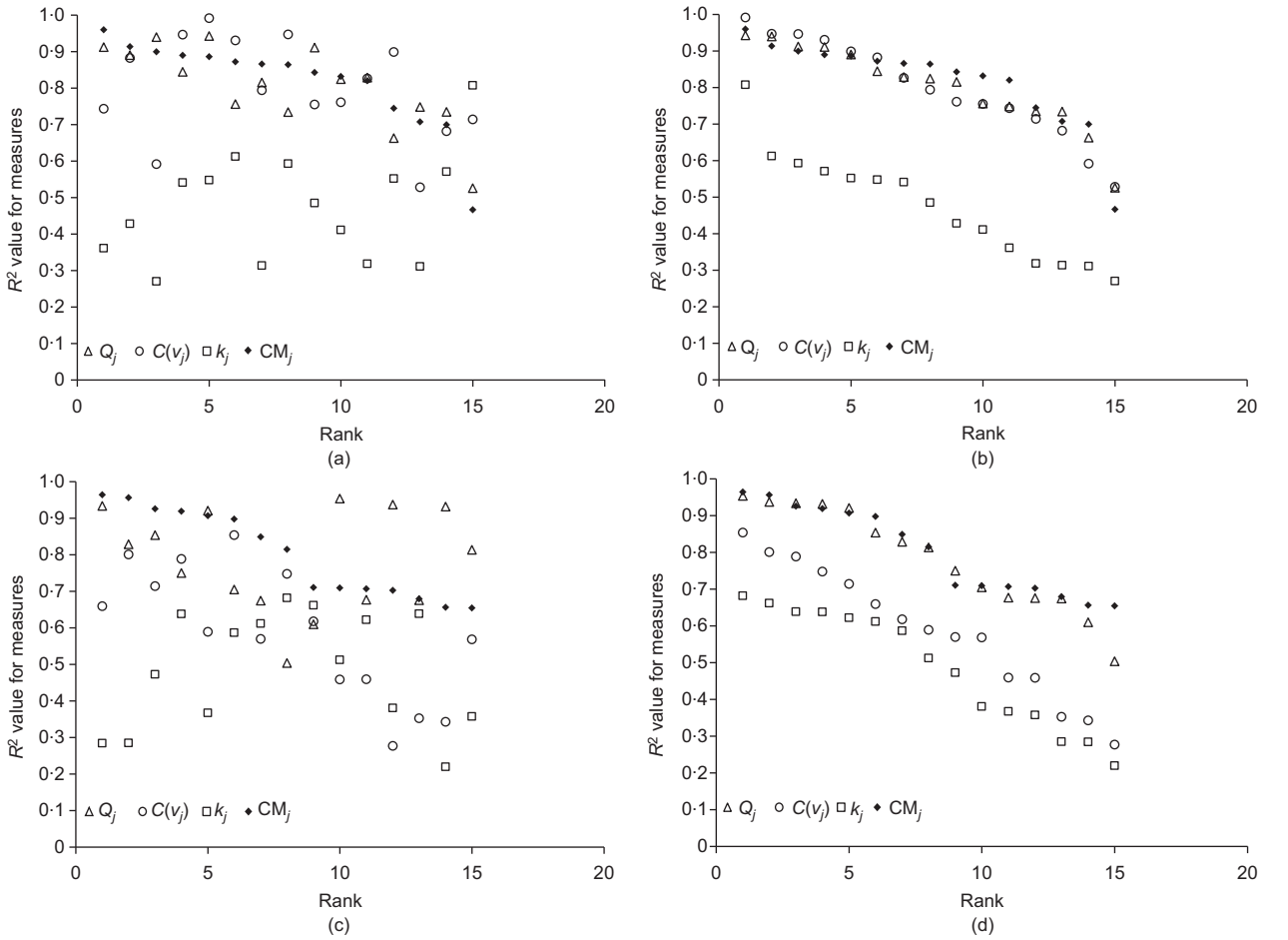


Figure 8. The skill of four approaches to predicting network performance where link resistances are (a, b) weighted with distance or (c, d) assigned randomly. Results are ranked in descending order according to R^2, for (a, c) all measures are ranked according to CM_j, while for (b, d) each measure is ranked independently

5. Case study 3: using network topology to understand the impact of interdependency on the performance of binary networks

The previous two case studies assumed the networked infrastructure was isolated from other infrastructure systems. In many instances this is an appropriate simplifying assumption to make. However, more recently approaches to networks of networks analysis (i.e. modelling the dependence of one system on another) have started to emerge (Gao *et al.*, 2011; Pederson *et al.*, 2006). For example, the successful operation on an electrical distribution system relies on a supply of water for cooling and ICT systems for control and management. The final case study seeks to understand the impact that interdependency can have on the performance of interconnected networks. As with the other two studies, the focus is on a single issue of interest, interdependency, and so space or flows are not considered.

Data on infrastructure interdependencies are not typically available but, as described by Hall *et al.* (2013), this situation is improving. With this in mind the present authors have developed a simplified network model to explore cascading failure in interdependent networks (Figure 9). First a number of isolated networks are established, each representing an infrastructure system. In this example two networks with random topology have been produced using the approach outlined in step 1(b). Interdependencies between networks are represented by a number of links, each connecting a node in one network with a node in another. Figure 9(a) shows an interdependent system that couples two networks, A and B. The set of nodes in network A are labelled (u_1, u_2, …), while the set of nodes in network B are

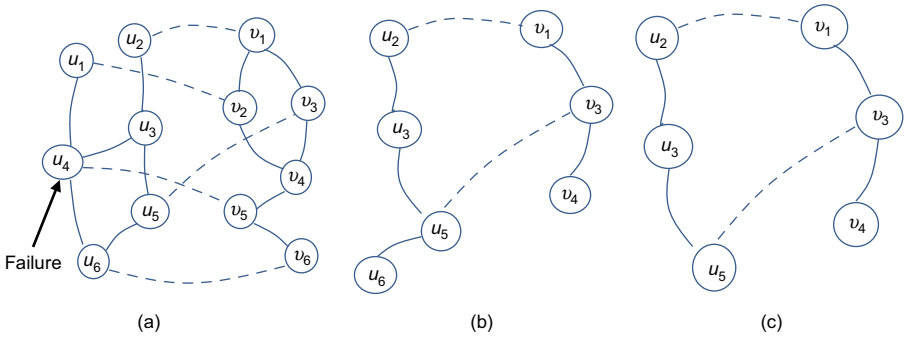


Figure 9. An interdependent system: (a) in its initial state, subject to failure of node u_4; (b) after the first iteration of cascading failure; (c) the stabilised system

labelled (v_1, v_2, …). An intra-network link is represented as a solid line. An inter-network dependency is represented as a dashed line.

This model allows inter-network dependencies to be configured along a few dimensions so as to provide the capacity to model various network coupling modes. First, inter-network dependencies can be generated according to different criteria, including random connections, or co-related connections according to spatial proximity or node degree. Second, the dependencies between two networks can be customised with three parameters, $< F, K, D >$. F specifies the extent of inter-network dependencies, that is, the portion of nodes that a network has and depends on another network. K specifies the redundancy of dependencies, that is, the number of supporting nodes that a node has from another network. D specifies the directionality of dependencies. An interdependent link is bi-directional if its inter-network dependencies are symmetric, for example, when a node u in network A supports a node v in network B, v also supports u. A link is uni-directional when these dependencies are not mutual. That is, when a network A node, u_1, supports a network B node, v_1, and v_1 in turn may support a different network A, node, u_2. For example, the system in Figure 9(a) is a bi-directional system, and a link between node u_1 and v_2 means that they mutually depend on each other.

To function properly, it is assumed that a dependent node requires the availability of at least one of its supporting nodes from each of its supporting networks. Failures happen in a system in the following three cases. First, a node fails if it is attacked directly. Second, a node fails if it is a dependent node and it loses all of its supporting nodes from at least one of the networks that it is supported by. Finally, in line with percolation theory approaches (Albert and Barabasi, 2002), a node fails if it is disconnected from the largest component of the network to which it belongs (Figure 9).

An attack on network A is modelled that disables some proportion of the network nodes directly and indirectly brings about a cascade of additional node failures in network B as a consequence of compromised interdependencies. Such additional node failures happen recursively and may result in system failure extending far beyond the original attack footprint. For the system in Figure 9(a), suppose that the node u_4 is attacked. When u_4 fails, all links connected to u_4 also fail. The failure of u_4 also disconnects u_1 from the giant component of A, and therefore u_1 fails. The failure of u_4 and u_1 triggers the failure of v_5 (supported by u_4) and v_2 (supported by u_1). The failure of v_5 disconnects v_6 from the largest component of network B, hence v_6 fails. The resulting system at this stage is shown in Figure 9(b). The failure of v_6 causes the failure of u_6. As no further failure occurs, the system reaches a stabilised state and the remaining functioning component of the system is shown in Figure 9(c).

To measure the performance of such an interdependent system, the connectedness of a system is calculated in terms of the relative size of the largest component, P, of the final stabilised system after the cascading failure.

$$4. \quad P = \frac{\sum_i N_T^i}{\sum_i N_0^i}$$

where N_0^i is the numbers of nodes from network i before cascading failure, and N_T^i are the number of nodes in the largest components of network i after cascading failure. The largest component can be an important quantity in, for example, a communication network where it represents the largest fraction of the network within which communication is possible and hence is a measure of the effectiveness of the network to provide its communication service. The aggregate performance, IP, characterises the behaviour of an interdependent

system when network disruptions of different magnitude are considered, and is calculated as the integral of P with respect to attack size, q.

$$5. \quad IP = \int_0^1 P(q)$$

The larger P and IP, the more nodes remain in the largest connected component of a system, the better the system performs and the easier the system is to recover or repair.

The study was carried out over systems that couple two random networks, A and B, each comprising 10 000 nodes, and with an average degree of 4. Network disruption was initiated by removing a randomly selected fraction q of network A nodes. Figure 10 plots relative size, P, of giant components as function of, q, the size of initial disruption to network A, when $F = 1{\cdot}0$ and $K = 2$ for a bi-directional system. The results are compared against that of a system in which networks A and B are isolated from each other. It shows that an interdependent system has smaller P and therefore is more vulnerable than an isolated system. While an isolated network undergoes continuous transition at the failure threshold q_c (the point when a system collapses or P becomes zero), an abrupt transition is observed at q_c for an interdependent system. That is, P at q_c is non-zero, and abruptly drops to zero when $q > q_c$ (Figure 10).

These results demonstrate that the interdependent system is most vulnerable when $K = 1$ and $F = 1{\cdot}0$, that is, when both networks are fully connected to each other and each node has only one supporting node from the other network. The performance of the interdependent system improves when the number of supporting nodes that a node has is increased (i.e. increasing K) or the extent a network depends on another network is decreased (i.e. decreasing F). When either K is sufficiently large or F is sufficiently small, the performance of an interdependent system approaches that of a system in which each of its sub-networks is isolated from or independent of the others (Figure 11).

Figure 11 shows the performance difference, $IP_{bi} - IP_{uni}$, of uni-directional and bi-directional systems, where IP_{bi} and IP_{uni} are aggregate performance of a bi-directional and a uni-directional system, respectively. It can be seen that a uni-directional system is more vulnerable than a bi-directional system, and the bigger F or/and smaller K are, the more remarkable is the difference of performance between a bi-directional and a uni-directional system. The main reason for the worse performance of a uni-directional system is that it presents more possibilities for the existence of longer dependency chains than a bi-directional system. These dependency chains run back and forth between the interconnected networks. A failure of one node compromises the robustness of all downstream nodes in the dependency chain, potentially triggering their failure and a possible cascade (described by Fu *et al.*, 2012).

6. Conclusions

Modern infrastructure systems are complex, interconnected networks. In this paper the authors have demonstrated the applicability of network theory on three different case studies. These examples have shown that the resilience of an infrastructure system is sensitive to a number of factors, including the

- spatial distribution of infrastructure nodes (such as airports and power stations)

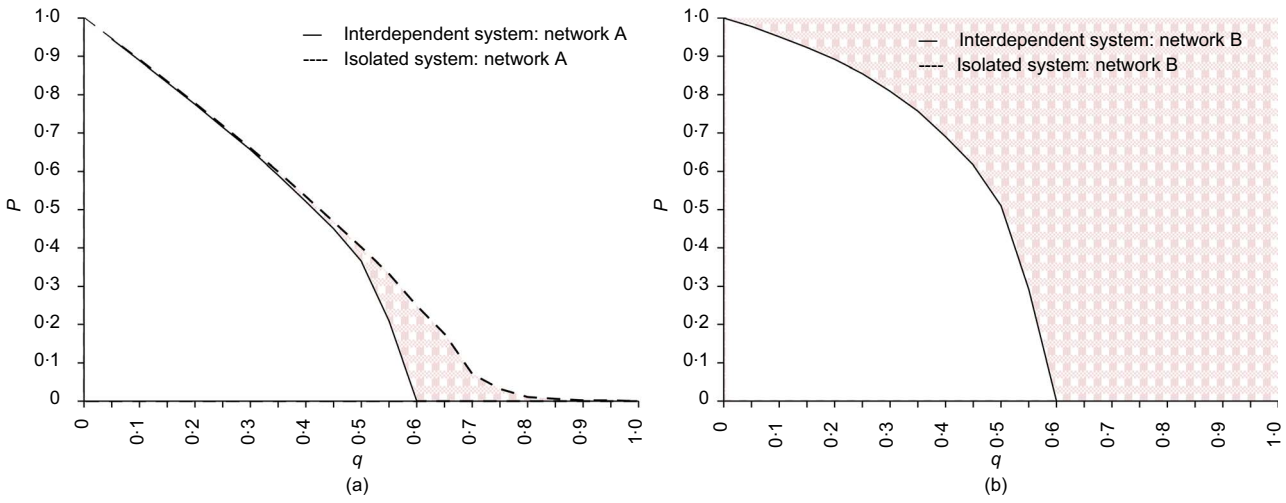


Figure 10. Comparison of the performance of interdependent systems against isolated systems

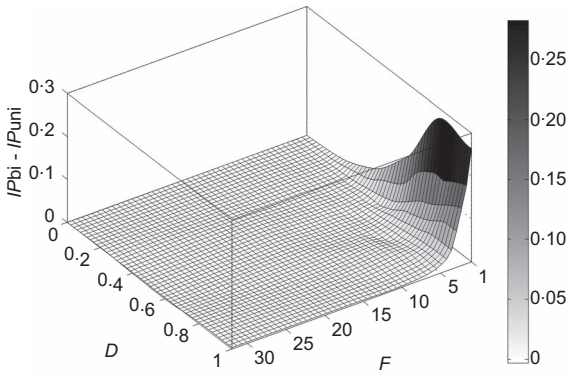


Figure 11. Comparison of the performance of bi-directional and uni-directional systems for a range of interdependent configurations

- type and magnitude of disruptive event to which the infrastructure is exposed (whether it is random, targeted or a spatially coherent hazard)
- degree of connectivity in an infrastructure network
- number of connections between infrastructure networks and their directionality
- capacity, and other properties, of the links that connect nodes.

In the first case study network graph theory was used to assess the vulnerability of the North American air traffic network to spatial and topological hazards and it was demonstrated that the degree attack strategy had the most devastating effect. For spatial hazards this network was found to have a similar spatial vulnerability to a random hazard. This is because the high degree hubs in the network are geographically distributed relatively evenly and therefore a spatial hazard must become relatively large before it has a significant impact on the network. In the second case study various network graph theory measures, flow based metrics and combinations of these were tested to better identify vulnerable nodes in a weighted network. In this example it was demonstrated that at times flow-based measures were superior and at other times graph theory measures were superior, but in general a combination of the two had the best predictive capabilities. Finally, a system of interdependent networks was analysed and it was demonstrated that an interdependent system is most vulnerable when both networks are fully connected to each other in a uni-directional manner and each node has only one supporting node from the other network. This case study highlighted the need to identify and characterise interdependencies and, where appropriate, add in redundancy or other mitigation measures.

While the authors recognise that the characterisation of the reliability of individual components in a system is important to understanding its behaviour, an earth systems engineering approach that considers system-level interactions is essential for understanding impacts on the wider environment. A priority for future work should be to identify, for different infrastructure design problems, the right balance between the computational efficiency of network (or other broad scale) analyses and the full representation of the physical processes. The case studies presented here show the potential for network theory to address a wide range of challenges such as broad scale risk assessment, national infrastructure planning and the development of adaptation plans, as well as understanding the potential impact of cascading impacts from random failure, spatial hazards such as floods, malicious attack or fragilities due to interdependencies. The authors therefore conclude that systems-scale analysis of infrastructure networks must be an important stage in infrastructure design, planning and management in the context of resilience and sustainability.

Acknowledgements

This work has benefited from funding support from Resilient Futures project that was funded by the Engineering and Physical Sciences Research Council and Economic and Social Research Council (EP/I035781/1). Richard Dawson is funded by an Engineering and Physical Sciences Research Council Fellowship (EP/H003630/1) and Sarah Dunn is partially funded by an Engineering and Physical Sciences Research Council studentship.

REFERENCES

Albert R and Barabasi AL (2002) Statistical mechanics of complex networks. *Reviews of Modern Physics* **74(1)**: 47–97.

Albert R, Jeong H and Barabasi AL (2000) Error and attack tolerance of complex networks. *Nature* **406(6794)**: 378–382.

Albert R, Albert I and Nakarado GL (2004) Structural vulnerability of the North American power grid. *Physical Review E* **69(2)**, http://dx.doi.org/10.1103/PhysRevE.69.025103.

Amaral L, Scala ANA, Barthelemy M and Stanley HE (2000) Classes of small-world networks. *Proceedings of the National Academy of Sciences of the United States of America* **97(21)**: 11 149–11 152.

Arenas AL, Danon A, Diaz-Guilera P, Gleiser M and Guimera R (2003) Community analysis in social networks. *European Physical Journal B* **38(2)**: 373–380.

Barabasi AL and Albert R (1999) Emergence of scaling in random networks. *Science* **286(5439)**: 509–512.

Barabasi AL, Albert R and Jeong H (2000) Scale-free characteristics of random networks: the topology of the world-wide web. *Physica A* **281(1–4)**: 69–77.

Barthelemy M (2011) Spatial networks. *Physics Reports – Review Section of Physics Letters* **499(1–3)**: 1–101.

Batagelj V and Brandes U (2005) Efficient generation of large random networks. *Physical Review E* **71(3)**, http://dx.doi.org/10.1103/PhysRevE.71.036113.

Bompard E, Wu D and Xue F (2011) Structural vulnerability of power systems: a topological approach. *Electric Power Systems Research* **81(7)**: 1334–1340.

Brandes U (2001) A faster algorithm for betweenness centrality. *Journal of Mathematical Sociology* **25(2)**: 163–177, http://dx.doi.org/10.1080/0022250X.2001.9990249.

Buldyrev SV, Parshani R, Paul G, Stanley HE and Havlin S (2010) Catastrophic cascade of failures in interdependent networks. *Nature* **464(7291)**: 1025–1028.

Deng K, Zhao HP and Li DJ (2007) Effect of node deleting on network structure. *Physica A – Statistical Mechanics and Its Applications* **379(2)**: 714–726.

Dunn S and Wilkinson S (2012) Identifying critical components in infrastructure networks using network topology. *Journal of Infrastructure Systems* **19(2)**: 157–165, http://dx.doi.org/10.1061/(ASCE)IS.1943-555X.0000120.

Erdos P and Renyi A (1960) On the evolution of random graphs. *Publication of the Mathematical Institute of the Hungarian Academy of Sciences* **5**: 17–61.

Freeman LC (1979) Centrality in social networks conceptual clarification. *Social Networks* **1(3)**: 215–239, http://dx.doi.org10.1016/0378-8733(78)90021-7.

Fu G, Khoury M, Dawson R and Bullock S (2012) Vulnerability analysis of interdependent infrastructure systems. *Proceedings of ECCS20112 European Conference on Complex Systems*, *Brussels*, *Belgium*, p. 18.

Gao J, Buldyrev SV, Havlin S and Stanley HE (2011) Robustness of a network of networks. *Physical Review Letters* **107(19)**, http://dx.doi.org/10.1103/PhysRevLett.107.195701.

Hall JW, Henriques JJ, Hickford AJ and Nicholls RJ (2013) Systems-of-systems analysis of national infrastructure. *Proceedings of the Institution of Civil Engineers – Engineering Sustainability* **166(5)**: 281–292, http://dx.doi.org/10.1680/ensu.12.00028.

HM Treasury and Infrastructure UK (2011) *National Infrastructure Plan*. Stationery Office, London, UK.

Holmgren AJ (2006) Using graph models to analyze the vulnerability of electric power networks. *Risk Analysis* **26(4)**: 955–969.

Latora V and Marchiori M (2002) Is the Boston subway a small-world network? *Physica A – Statistical Mechanics and Its Applications* **314(1–4)**: 109–113.

Lewis TG (2009) *Network Science: Theory and Practice*. John Wiley, Oxford, UK.

Lhomme S, Serre D, Diab Y and Laganier R (2013) Analyzing resilience of urban networks: a preliminary step towards more flood resilient cities. *Natural Hazards and Earth Systems Sciences* **13(2)**: 221–230, http://dx.doi.org/10.5194/nhess-13-221-2013.

Liu JZ and Tang YF (2005) An exponential distribution network. *Chinese Physics* **14(4)**: 643–645, http://dx.doi.org10.1088/1009-1963/14/4/001.

Milgram S (1967) The small-world problem. *Psychology Today* **1(1)**: 61–67.

Murray A and Grubesic T (2007) *Critical Infrastructure: Reliability and Vulnerability*. Springer, Berlin, Germany.

Newman MEJ (2003) The structure and function of complex networks. *Siam Review* **45**: 167–256.

Newman MEJ, Watts DJ and Strogatz SH (2002) Random graph models of social networks. *Proceedings of the National Academy of Sciences of the United States of America* **99**: 2566–2572.

Openflights (2010) OpenFlights.org. See http://openflights.org/ (accessed 13/08/2010).

Pederson P, Dudenhoeffer D, Hartley S and Permann M (2006) *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Idaho National Laboratory, Idaho, USA.

Pitt M (2008) *The Pitt Review: Learning Lessons from the 2007 Floods*. Cabinet Office, London, UK.

Rosato V, Issacharoff L, Tiriticco F *et al*. (2008) Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures* **4**: 63–79.

Royal Academy of Engineering (*RAE*) (2011) *Infrastructure, Engineering and Climate Change Adaptation – Ensuring Services in an Uncertain Future*. RAE, London, UK, see http://www.raeng.org.uk/news/publications/list/reports/Engineering_the_future_2011.pdf.

Rual JF, Venkatesan K, Hao T *et al*. (2005) Towards a proteome-scale map of the human protein-protein interaction network. *Nature* **437(7062)**: 1173–1178.

Sporns O (2002) Network analysis, complexity, and brain function. *Complexity* **8(1)**: 56–60.

Stam CJ and Reijneveld JC (2007) Graph theoretical analysis of complex networks in the brain. *Nonlinear Biomedical Physics* **1(3)**: 1–19.

Valverde S and Solé RV (2003) Hierarchical small worlds in software architecture. *Arxiv*: preprint cond-mat/0307278.

Watts DJ and Strogatz SH (1998) Collective dynamics of 'small-world' networks. *Nature* **393(6684)**: 440–442.

Wilkinson S, Dunn S and Ma S (2012) The vulnerability of the European air traffic network to spatial hazards. *Natural Hazards* **60(3)**: 1027–1036.