

ABSTRACT

Title: SELF-ORGANIZATION AND TOPOLOGY
CONTROL OF INFRASTRUCTURE SENSOR
NETWORKS

Michael J. Casey, Doctor of Philosophy, 2005

Directed By: Professor Gregory B. Baecher
Department of Civil and Environmental Engineering

Infrastructure networks are complex, interconnected, and inter-dependent systems on which modern society has become almost totally dependent. They provide for cost-effective and efficient distribution of energy, communications, and transportation, yet are increasingly fragile and rapidly propagate failure caused by natural or man-made hazards. Despite our reliance on these networks and our awareness of their risks, an understanding of their survivability and methods for mitigating the risks inherent in their spatial and topologic organization has been lacking.

Infrastructure sensor networks are coupled with infrastructure for health, performance, or surveillance monitoring. They detect the precursors of hazards and allow response to prevent cascading failure. These co-located, dependent sensor networks are themselves susceptible to disruption and require control methodologies to maintain surveillance capability (i.e, survivability) should disruption occur.

This research quantifies the risk and vulnerability associated with dependent sensor networks and investigates the role of topology control and self-organization behavior in mitigating that risk. Simulated random and targeted attacks are performed on spatial and lifeline infrastructure topologies. Spatial topologies are shown to exhibit attack resistance, while lifeline topologies undergo percolation sooner and more frequently resulting in significantly higher vulnerability.

Topology control, or dynamic reconfiguration of the network in response to disruption, is shown to significantly mitigate the vulnerability of infrastructure sensor networks. Its application, however, is limited based on the critical spatial density of nodes placed around infrastructure networks. The critical density of dependent sensor networks is computed and a framework for the self-organization of infrastructure sensor networks is discussed.

SELF-ORGANIZATION AND TOPOLOGY CONTROL OF INFRASTRUCTURE
SENSOR NETWORKS

By

Michael J. Casey

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2005

Advisory Committee:
Professor Gregory B. Baecher, Chair
Professor Christopher C. Davis
Assistant Professor Steven A. Gabriel
Professor Ali Haghani
Research Professor Stuart D. Milner

© Copyright by
Michael J. Casey
2005

Dedication

This dissertation is dedicated to my grandfather, Mr. George Sepsie. His intellectual curiosity and call to achieve great things have inspired me throughout my life.

Acknowledgements

I wish to acknowledge and thank the many individuals and groups who have contributed directly or indirectly to the completion of this research. First and foremost, I thank Dr. Gregory Baecher for his guidance and optimism throughout my doctoral studies. He has been a mentor and a friend for which I am truly grateful. The assistance of Dr. Steven Gabriel, who provided valuable feedback on this manuscript, is much appreciated.

I wish to thank all of the faculty and staff of the Department of Civil and Environmental Engineering. Specifically, Mr. Alan Santos and Dr. Glenn Moglen have offered me confidence and wisdom when I have needed it the most.

I am grateful for the support of Drs. Stuart Milner and Christopher Davis and the many students of the Center for Networking of Infrastructure Sensors and the Maryland Optics Group. This research was made possible because of the successful interdisciplinary collaboration between students and faculty working in civil, communications, and optical engineering.

The National Science Foundation has provided me support as a graduate assistant throughout my doctoral studies. Their investment in me and U.S. academic research is gratefully acknowledged.

Finally, I would like to thank my family and wife Colleen for their patience and encouragement. Without their support, none of this would be possible.

Table of Contents

| | | |
|-------|--|----|
| 1 | Chapter One - Introduction | 1 |
| 1.1 | Problem Definition | 3 |
| 1.2 | Goals and Objectives | 4 |
| 1.3 | Approach and Overview of the Dissertation..... | 5 |
| 1.4 | Overview of Research Outcomes | 6 |
| 2 | Chapter Two – Background and Literature Review | 7 |
| 2.1 | Infrastructure Context..... | 9 |
| 2.2 | Models of Network Systems..... | 10 |
| 2.2.1 | Definitions and Representation..... | 10 |
| 2.2.2 | Random Graphs and Equilibrium Networks..... | 13 |
| 2.2.3 | Non-Equilibrium Networks | 15 |
| 2.2.4 | Power-law and Heavy-tail distribution networks | 17 |
| 2.2.5 | Highly Optimized Tolerance (HOT)..... | 22 |
| 2.2.6 | Network Survivability..... | 25 |
| 2.3 | Spatial Networks..... | 28 |
| 2.3.1 | Shape and efficiency | 29 |
| 2.3.2 | Degree and Accessibility | 32 |
| 2.4 | Efficiency and Risk..... | 35 |
| 2.4.1 | Structural Vulnerability | 36 |
| 2.4.2 | Flows and Network Utilization..... | 39 |
| 2.4.3 | Trading-off Efficiency and Survivability..... | 41 |
| 2.5 | Network Topology Control..... | 42 |
| 2.5.1 | Physical Layer Optimization..... | 44 |

| | | |
|-------|---|----|
| 2.5.2 | Network Layer Optimization | 45 |
| 2.5.3 | Multi-Objective Optimization and Trade-off..... | 46 |
| 2.5.4 | Challenges in Topology Control | 47 |
| 2.6 | Summary | 50 |
| 3 | Chapter Three – Vulnerability Analysis of Sensor Network Infrastructure | 52 |
| 3.1 | Network Sensitivity to Topologic and Spatial Perturbations..... | 54 |
| 3.1.1 | Dependent Topologies | 54 |
| 3.1.2 | Derived Vulnerability | 56 |
| 3.1.3 | Quantifying Derived Vulnerability | 59 |
| 3.1.4 | Towards Dependent Topology Survivability | 61 |
| 3.2 | Approach..... | 66 |
| 3.3 | Topology Generation | 68 |
| 3.3.1 | Random Network Generator | 68 |
| 3.3.2 | Exponential Network Generator | 69 |
| 3.3.3 | Power-law Generator | 69 |
| 3.3.4 | Proximal topology generator..... | 70 |
| 3.3.5 | Other generators..... | 70 |
| 3.3.6 | Implementation | 71 |
| 3.4 | Verification of Topologic Statistics | 72 |
| 3.4.1 | Verification of Topology Generators..... | 72 |
| 3.4.2 | Variance in Graph-theoretic statistics | 79 |
| 3.5 | Network Vulnerability Analysis | 82 |
| 3.5.1 | Sensitivity of networks to random failure or attack..... | 82 |
| 3.5.2 | Sensitivity of networks to targeted failure or attack | 88 |
| 3.5.3 | Sensitivity of networks to spatial attack | 91 |

| | | |
|-------|---|-----|
| 3.5.4 | Independent Risk Curve Determination..... | 96 |
| 3.6 | Dependent Topology Vulnerability Analysis | 99 |
| 3.6.1 | Lifeline-Dependent Sensor Topologies | 99 |
| 3.6.2 | Lifeline Topology Generator | 101 |
| 3.6.3 | Lifeline Spatial Attack | 104 |
| 3.7 | Estimating Derived Vulnerability | 108 |
| 3.8 | Summary | 111 |
| 4 | Chapter Four – Self-Organization and Topology Control | 114 |
| 4.1 | Survivability of Infrastructure Sensor Networks with Topology Control | 116 |
| 4.1.1 | Lifeline Topology Control Algorithm | 116 |
| 4.1.2 | Lifeline Attack with Topology Control | 118 |
| 4.2 | Limitations on Topology Control Scalability | 122 |
| 4.2.1 | Critical Density | 123 |
| 4.3 | Self-organization of Infrastructure Sensor Networks | 125 |
| 4.3.1 | Heterogeneous architecture..... | 126 |
| 4.3.2 | Evolutionary design | 128 |
| 4.3.3 | In-situ processing..... | 128 |
| 4.4 | Summary | 129 |
| 5 | Chapter Five – Summary and Conclusions..... | 130 |
| 5.1 | Assessment of Goals and Objectives | 132 |
| 5.2 | Summary of Findings..... | 134 |
| 5.2.1 | Infrastructure graph context..... | 134 |
| 5.2.2 | Spatial-Topologic context for infrastructure..... | 134 |
| 5.2.3 | Infrastructure Risk | 135 |
| 5.2.4 | Independent and Dependent Topologies..... | 135 |

| | | |
|--------|--|-----|
| 5.2.5 | Derived Vulnerability | 135 |
| 5.2.6 | Topology Generators | 136 |
| 5.2.7 | Spatial and Lifeline-based Attack Modes | 137 |
| 5.2.8 | Lifeline Attack Resistance with and without Topology Control | 138 |
| 5.2.9 | Critical Percolation Density for Sensor Networks..... | 139 |
| 5.2.10 | Balance of Self-Organization and Topology Control | 139 |
| 5.3 | Principal Conclusions | 140 |
| 5.4 | Recommendations for Future Work | 141 |
| 6 | Appendix A: Properties of the Pareto distribution..... | 143 |
| 7 | Bibliography | 146 |

List of Tables

| | |
|--|-----|
| Table 1-1: Dissertation research outcomes and relevant sections. | 6 |
| Table 3-1: Derived vulnerability criteria for Infrastructure sensors. | 56 |
| Table 3-2: Summary of simulation analyses and survivability results. | 112 |
| Table A-1: Low-order moments of the Pareto distribution. | 144 |

List of Figures

| | |
|---|----|
| Figure 2-1: Decomposition of infrastructure and graph models. | 9 |
| Figure 2-2: Schematic graph of US Interstate Highway System with random graph structure. | 14 |
| Figure 2-3: Smallworld network where hubs have above average number of links... .. | 18 |
| Figure 2-4: Summary of random graph forms, parameters, and properties. | 21 |
| Figure 2-5: Cases of site percolation on an $N \times N$ lattice (Carlson et al. 2000). | 24 |
| Figure 2-6: Cumulative Distribution of events (Carlson et al. 2000). | 25 |
| Figure 2-7: Topologic structures for a distributed communications system (Baran 1964). | 26 |
| Figure 2-8: Conceptual representation of geographic and logical views of a network (Zeiler 1999). | 29 |
| Figure 2-9: Simulated failure/attack for different topologies (Dorogovtsev et al. 2003). | 37 |
| Figure 2-10: Connectivity loss in the North American electric power grid based on simulated failure/attack (Albert et al. 2004). | 40 |
| Figure 2-11: Example of physical/network layer mismatch (Zhuang et al. 2004). | 46 |
| Figure 3-1: Conceptual risk curves (CCDFs) (Baecher et al. 2003). | 58 |
| Figure 3-2: Conceptual network decay curve. | 63 |
| Figure 3-3: Conceptual risk curves based on derived vulnerability. | 64 |
| Figure 3-4: Overview of analysis procedure. | 66 |
| Figure 3-5: Typical generated random topology ($N=100$, $E=100$). | 73 |
| Figure 3-6: Degree distribution of random (ER) Topology. | 74 |
| Figure 3-7: Typical Exponential topology ($N = 100$, $E = 100$). | 74 |
| Figure 3-8: Typical Exponential Degree Distribution. | 75 |
| Figure 3-9: Typical topology from BA topology generator ($N=50$, $E=93$). | 75 |
| Figure 3-10: Typical Scale-free (Power-law) degree distribution. | 76 |

| | |
|--|-----|
| Figure 3-11: Typical spatial organization from proximal topology generator ($N=1000$)..... | 77 |
| Figure 3-12: Typical Degree distribution from proximal topology generator ($N=1000$) with 1000 x 1000 random field..... | 79 |
| Figure 3-13: Variation of diameter in largest component for edge/node ratio. | 80 |
| Figure 3-14: Simulation results from random attack on random topologies. | 83 |
| Figure 3-15: Diameter network decay (random attack on random topology). | 85 |
| Figure 3-16: Simulation results from random attack on Exponential topologies. | 86 |
| Figure 3-17: Simulation results from random attack on Power-law topologies. | 87 |
| Figure 3-18: Simulation results of Targeted attack on Random topologies. | 89 |
| Figure 3-19: Simulation results of Targeted attack on Exponential topologies..... | 90 |
| Figure 3-20: Simulation results of Targeted attack on Power-law topologies..... | 91 |
| Figure 3-21: Conceptual spatial network topology subject to spatial attack. | 92 |
| Figure 3-22: Simulation results for Spatial Attack on Random topologies. | 93 |
| Figure 3-23: Simulation Results for Spatial Attack on Exponential topologies. | 94 |
| Figure 3-24: Simulation results for Spatial Attack on Power-law topologies. | 94 |
| Figure 3-25: Proximal topology subjected to spatial attack ($N = 1000$). | 96 |
| Figure 3-26: CCDF of simulation results from spatial attack on proximal topology. | 97 |
| Figure 3-27: Conceptual infrastructure lifelines and impact buffers. | 100 |
| Figure 3-28: Infrastructure sensor network from lifeline generator. | 102 |
| Figure 3-29: Typical lifeline topology degree distribution..... | 104 |
| Figure 3-30: Infrastructure lifeline layout with route factor impact buffers..... | 105 |
| Figure 3-31: Network decay curve for lifeline attack (dependent topology)..... | 107 |
| Figure 3-32: Distribution of dependent topology percolation thresholds..... | 109 |
| Figure 3-33: Comparison of Dependent and Independent CCDFs..... | 110 |
| Figure 4-1: Illustration of Lifeline Topology Control. | 117 |

| | |
|---|-----|
| Figure 4-2: Network decay of lifeline topology subject to lifeline attack with topology control. | 119 |
| Figure 4-3: Percolation threshold distribution for lifeline attack with topology control. | 121 |
| Figure 4-4: Experimentally derived critical density determination for lifeline dependent topologies. | 124 |
| Figure 4-5: Conceptual heterogeneous (hierarchical) network architecture. | 127 |
| Figure 5-1: Sensor network survivability "layer cake" | 131 |

List of Abbreviations

| | |
|----------------------------------|--|
| \bar{k} | Mean degree of a vertex. Mean degree of a vertex. Mean degree of a vertex. |
| \bar{l} or $\langle l \rangle$ | Mean shortest path between two vertices i, j . |
| N | Number of nodes in a graph |
| C | Clustering coefficient – a measure of the extent to which the neighbors of a particular vertex are connected with one another. |
| c_{ij} | Physical layer cost between nodes i and j (e.g., bit-error rate). |
| γ | Exponent of power-law distributed data (e.g., $f(x) = x^{-\gamma}$) |
| q | Route-factor indicating relationship between path distance and Euclidean distance for a given graph. |
| ER | Erdos-Renyi |
| BA | Barabassi-Albert |
| d | Diameter – the distance between the two vertices of a connected graph which are furthest from each other. |
| f | Fraction of nodes removed. |
| Ω | Universal set of the triplet; scenario, likelihood, and consequence |
| p_c | Percolation threshold |
| w | Consequence variable in measuring risk. |
| \bar{w} | Average component size. |
| W | Size of the largest component relative to the undamaged network. |
| DTCN | Designated Topology Control Node |
| θ | Network throughput |
| CA | Cellular Automata |
| CCDF | Complimentary Cumulative Distribution Function |

1 Chapter One - Introduction

Infrastructure is the basic facilities, services, and installations needed for the functioning of society, such as water supply, fuel and electric energy supply, transportation, telecommunication, the Internet, government and emergency services, financial services, and others (CIAO 1997). Whether substations connected in an electricity grid, or wireless base stations forming a communications backbone, infrastructure systems are represented by network models of connected nodes and links. Modern society has become almost totally dependent on these increasingly complex, but also increasingly fragile, lifeline networks (O'Rourke 1993). We have developed tightly-coupled, non-redundant systems which rapidly propagate failure and interact in complex, interdependent ways.

The advent of mathematical models of networks has enabled research in fields as varied as project scheduling and vehicle routing. Where most research has focused on determination of the shortest path or maximum flow through a given network, less emphasis has been placed on the logical and spatial organization of the networks themselves. The recent emergence of very large contiguous networks such as the World Wide Web (WWW) has prompted research in the topologic structure of network systems. It has been shown that the shape and efficiency of many real world networks is based on *self-organizing* behavior that yields topologic structures with a unique resistance to random failure and a particular susceptibility to deliberate attack or infection. Research in the spatial properties of these networks has revealed unintended vulnerabilities where infrastructure systems are co-located and deployed

for long-haul connectivity. The interplay of spatial and topologic properties provides a context for studying the relative influence of network cost, performance, and risk for infrastructure management.

The capability of sensor networks to monitor the performance and security of infrastructure systems in-situ enables real-time response, emergency preparedness, and effective allocation of scarce resources. However, since the response of different infrastructure systems to different perturbations can have negative effects ranging from performance degradation to cascading failure (locally, globally, or both), sensor networks require control mechanisms to de-couple themselves from the underlying systems they are deployed to monitor. *Topology control*, used for example in wireless communication networks, allows topology to be dynamically reconfigured in response to disruption or degradation. Autonomous nodes can determine a new topology to maintain connectivity and maximize performance, and then execute changes by physically moving and reconnecting their communications interfaces. The ability to compute optimal topologies is limited, however, by computational complexity and unknown conditions in other heterogeneous parts of the network. Locally optimal topologies may introduce undesired vulnerabilities in the broader network. Trade-offs between competing objectives form the basis for topology control techniques in sensor networks.

1.1 Problem Definition

The problem of complex interdependency and response of infrastructure systems has been captured succinctly by Mendes et al:

“Is it possible to develop tools to address in a systematic fashion the robustness and vulnerability of large technological and infrastructural networks? Complex networks react in different ways to different perturbations. In general they are robust to random damages but weak to attacks targeting some key elements of the system. A systematic theory of network resilience and robustness needs to address both local (individual failures) and global vulnerabilities (cascading failures).” (Mendes et al. 2004)

Sensors and sensor networks have become intertwined with all types of infrastructure systems to facilitate monitoring and control. Sensor networks (both wired and wireless) have become vital to the modeling of complex infrastructure systems. The sensor networks often become coupled to the infrastructure systems themselves and suffer potential failure and degradation when perturbations to the infrastructure system occur. Failure is the destruction or incapacitation of nodes while degradation is a decrease in communications capability (i.e., throughput) caused by physical constraints or network congestion. A key research need is to study the topologic structure of the infrastructure system coupled with the sensor network put in place for monitoring and control.

1.2 Goals and Objectives

This research has the overriding goal of contributing fundamental knowledge in the modeling of sensor networks deployed for critical infrastructure protection. No previous study of sensor network survivability and re-configurability in the combined context of infrastructure risk and graph-theoretic modeling are known to exist.

Aligned with this goal, this research will address the following objectives:

1. Quantitatively assess the vulnerability and survivability of different spatial/topologic structures to random, targeted, and spatially-based perturbations.
2. Investigate the dependency relationships between sensor and infrastructure networks with respect to risk and re-configurability.
3. Demonstrate the application of topology control and self-organization behavior in infrastructure sensor networks and fundamental limits on their use.

The trade-off between efficiency, performance, and risk is a central theme in this work given the integrated spatial and topologic structure of infrastructure networks and the sensor networks put in place to monitor them. While all engineered systems incorporate similar trade-offs, the unique importance of inter-connected and inter-dependent, yet fragile infrastructure systems in our society makes investigation of this trade-off crucially important.

1.3 Approach and Overview of the Dissertation

The scope of this dissertation spans the fields of communications engineering, civil engineering, and systems engineering. It uses simulation modeling in an exploratory context to demonstrate the unique challenges in the development of sensor network technology for infrastructure systems management.

Chapter Two provides a survey of literature in network theory, spatial networks and infrastructure topology planning, design, and control. The relevant theory in complex network topology is presented in addition to previous research in the vulnerability of infrastructure and lifeline networks. A brief survey of network control is presented as well.

Chapter Three investigates vulnerability and survivability of independent and dependent sensor networks based on different spatial and topologic structures and in-response to random and targeted attack. It includes analyses on infrastructure network hazards using GIS-based simulation techniques and a risk modeling approach.

Chapter Four is a presentation of network topology control applied to infrastructure sensor networks. The mitigating effects of topology control on sensor network survivability and vulnerability are presented as well as the role of self-organization behavior of sensors to manage spatial density limitations on scalability.

Finally, Chapter Five is a summary of the major findings of the dissertation, principal conclusions and recommendations for future work.

1.4 Overview of Research Outcomes

Ten specific research outcomes were developed in this research. Table 1-1 presents a summary of the outcomes with the corresponding section(s) in the Dissertation that discuss each outcome. Although these are sections that deal most directly with each outcome, general discussion of each topic can be found throughout the Dissertation. Additionally, the outcomes are summarized with specific findings and explanations in Section 5.2.

Table 1-1: Dissertation research outcomes and relevant sections.

| | RESEARCH OUTCOMES | DISSERTATION SECTION(S) |
|----|--|--------------------------------|
| 1 | Infrastructure graph context | 2.1 |
| 2 | Spatial-topologic context for infrastructure | 2.3 |
| 3 | Infrastructure risk | 2.4, 3.1 |
| 4 | Independent and dependent topologies | 3.1.1, 3.6.1, 3.7 |
| 5 | Derived vulnerability | 3.1.2, 3.1.3, 3.7 |
| 6 | Topology generators | 3.3, 3.6.1, 3.6.2 |
| 7 | Spatial and lifeline-based attack modes | 3.5.3, 3.6.3 |
| 8 | Lifeline attack resistance with and without topology control | 3.6.3, 4.1.2 |
| 9 | Critical percolation density for sensor networks | 4.2 |
| 10 | Balance of self-organization and topology control | 4.3 |

2 Chapter Two – Background and Literature Review

Increases in computing power have enabled us to map the structure of networks and measure their properties in a way that has never been possible. Previously, large networks or those with uncertain structure have been represented by statistical models based on certain limiting assumptions. Empirical studies of the interconnectivity of information networks such as the World Wide Web (WWW) and the fiber optic backbone communications network have revealed unexpected properties related to their performance and vulnerability. The *topology* of the network (i.e., the organization of nodes and links) is the principal factor in understanding the cost, efficiency, and risk associated with different network structures.

There is now a convergence of theories surrounding flows in networks, modeling of the underlying topologic structure, and the spatial organization of networks.

Understanding of network cost, performance, and risk cannot be complete without bringing these interdependent contexts together. *Infrastructure*, which includes physical pipes, roads, and wires as well as wireless communication links is an appropriate arena for the study of these converging theories. As a society we design, build, operate, and secure infrastructure assets to provide efficient means for commerce, quality of life, societal and government needs.

The drive to develop efficient built and manufactured systems has been a hallmark of 20th and 21st century engineering, delivering low cost, resilient systems with appropriate factors of safety. Infrastructure networks have the same requirements of low cost and resilience yet a comprehensive understanding of their static and dynamic

properties has been elusive without simplifying assumptions such as independence of behavior. Infrastructure network systems have become interconnected and interdependent and thus boundaries (i.e., spatial and logical separations) have become difficult to create. This complexity does not relieve the engineer from applying tried principles to the design and operation of efficient, high-performance, and safe infrastructure systems.

The purpose of this chapter is to provide an overview of the relevant literature in network theory and to provide a basis for the following chapters. A significant amount of work has been done recently on the topological properties of large networks specifically with regard to their efficiency. An overview of this literature is presented as well as work on the spatial structure of networks. The structural vulnerability of networks due to topological and spatial organization is surveyed and a discussion of hazard, vulnerability, and risk analysis in the context of infrastructure *lifelines* is presented. Work on the application of network and topology control to dynamically re-configure a network in response to disruption is presented in the context of sensor networks for monitoring critical infrastructure. Finally, the current capabilities and challenges of network and topology control are surveyed for their applicability to infrastructure sensor networks.

2.1 Infrastructure Context

All distributed physical infrastructure (e.g., roads, pipelines, electrical grid) and information infrastructure (e.g., Internet, World Wide Web) can be abstracted to geometric and mathematical models known as *graphs*. Graphs are composed of nodes (vertices) connected by edges (links). Edges can be directed or undirected and can represent simple connectivity or may represent a weight or capacity for transmitting flow over the link (e.g., gallons of water per minute or cars per hour). Figure 2-1 shows a conceptual class decomposition of infrastructure systems into graph theoretic models.

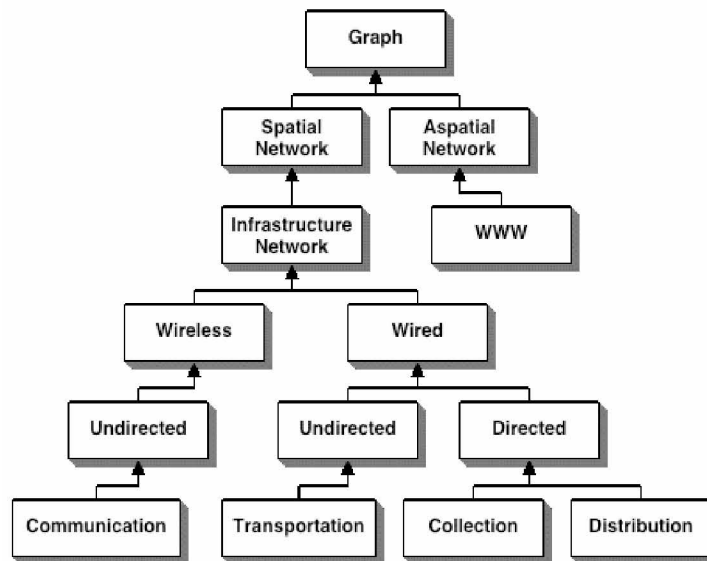


Figure 2-1: Decomposition of infrastructure and graph models.

In this research, all wired and wireless infrastructure networks are represented spatially. This decomposition shows us that the physics of each network are unique and that general properties and behavior of complex infrastructure systems may be difficult to assign.

2.2 Models of Network Systems

Graph theory is a theoretical framework for examining the relationships between collections of elements that are connected together, but logically or spatially distributed. Euler is credited with the first formulation of a graph problem, when, in 1736 he developed a mathematical proof that a person could not cross the seven bridges of Königsberg to reach four land areas without crossing the same bridge twice (Barabási 2002). His contribution was the novel abstraction of the problem as a *graph* with the four land areas as *nodes or vertices* and the seven bridges as *edges or links*.

The abstraction of the bridge system as a graph was a fundamental contribution to mathematics, science, and engineering. Shortest path, maximum flow, minimum cost flow, and minimum spanning tree are all classes of problems that use the graph model as a basis for calculation. Given a model of the structure of the network, the appropriate physical processes can be applied to model the dynamics of traffic flow (e.g., traffic, electricity, fluid) over the network.

In contrast to the above approach, the current research considers the structure of the network itself and the consequences of topological and spatial organization on cost, performance, and risk rather than taking the topology as simply a basis for computing flows.

2.2.1 Definitions and Representation

A *graph*, $G = (V, E)$ is a non-empty set of V vertices and E edges. In this research the terms node and link are used interchangeably for vertex and edge, respectively. The

order or size of the graph is the total number of vertices and is denoted by N . The *diameter* of the graph is the number of edges separating the two vertices that are furthest from one another (i.e., the largest number of edges separating disparate nodes). Graphs are usually drawn as a set of points connected by lines, either undirected or directed, using arrows pointing from source to destination. A *subgraph* of a graph G is a graph whose vertex and edge sets are subsets of those of G .

A graph is *planar* if it can be drawn on a plane without edge intersections except at nodes. Most physical infrastructure is planar, as roads cross at intersections and sewer pipes intersect at manholes. Highways, pipelines, or the power grid, however, may also be *non-planar* as overpasses allow these systems to cross while not intersecting.

The *degree* of a vertex is the number of edges connecting to it. For directed graphs, the *indegree* and *outdegree* are the number of edges entering and leaving a vertex, respectively. A *path* is a collection of edges represented by a sequence of vertices without repeated elements (i.e., without cycles). The *shortest path*, l , is the unique path between source and destination with the fewest number of edges. A *tree* is a type of graph that contains no cycles and that has a *root* such that there is a distinct path in G from the root to each node.

A *degree distribution* is a frequency distribution function describing the relative frequency of the degree of nodes in the graph. The probability of k edges connecting to a node is $P(k)$. The distribution of $P(k)$, the degree distribution, has a characteristic *mean degree*, \bar{k} which is the average number of edges connecting to a node. The

clustering coefficient, c , of a vertex is the ratio between the total number y of edges connecting to its nearest neighbors and the total number of all possible edges, z , between its nearest neighbors:

$$C = \frac{2y}{z(z-1)} \quad (2-1)$$

In other words, the clustering coefficient C_i for a vertex v_i is the proportion of edges common to the vertices within its neighborhood divided by the number of edges that could possibly exist between them.

The *betweenness* or *centrality* $\sigma(m)$ of a vertex m is the total number of shortest paths between all possible pairs of vertices (i,j) that pass through vertex m :

$$\sigma(m) = \sum_{i \neq j} \frac{B(i, m, j)}{B(i, j)} \quad (2-2)$$

where $B(i, m, j)$ and $B(i, j)$ are the path lengths from i to j that do and do not include vertex m , respectively. Vertices that occur on many shortest paths between other vertices have higher betweenness than those that do not.

A *source* is any vertex that generates flow on a directed graph and a *sink* is any vertex that receives flow. A *relay* is a node that transmits flow without contributing or removing from that flow. These terms and definitions represent the basic properties for describing the topologic structure of networks as used in this research.

2.2.2 Random Graphs and Equilibrium Networks

For the analysis of large graphs or graphs for which the topology is unknown, stochastic properties can be used instead of deterministic properties (i.e., combinatorics) to characterize structure. Erdos and Rényi (E-R) developed a theory of random graphs in the 1950s (Chung et al. 1998). Their interest was in estimating the number of links separating nodes chosen at random in a large network. The E-R theory postulates that the placement of edges throughout a finite graph is a stochastic process where an edge can exist between any two nodes in a graph with equal probability p . Since any vertex can have between 0 and $N - 1$ attached edges, probability theory can be used to characterize the mean degree \bar{k} and the form of the degree distribution.

Dorogovtsev and Mendes (2003), Bornholdt and Schuster (2003), and others have provided the formal derivation of the degree distribution of the E-R random graph.

Briefly, the degree distribution, $P(k)$ is binomial with the average degree

$$\bar{k} = p(N - 1).$$

$$P(k) = \binom{N-1}{k} p^k (1-p)^{N-1-k} \quad (2-3)$$

The network contains, on average $pN(N - 1)/2$ edges. For large N and fixed \bar{k} , the distribution assumes the Poisson form:

$$P(k) = \frac{e^{-\bar{k}} \bar{k}^k}{k!} \quad (2-4)$$

The Poisson distribution is described by its characteristic scale, \bar{k} which is the average degree, and has variance also equal to \bar{k} . In practical terms, this means that for large E-R graphs, on average, most vertices have approximately the same number of links.

Figure 2-2 is a schematic of the US Interstate Highway System. The graph representing the network has 46 nodes ($N = 46$) and 57 edges. The graph is fully connected. The minimum, maximum, and mean node degree are 1, 4, and 1.24 respectively. The mode is 3.

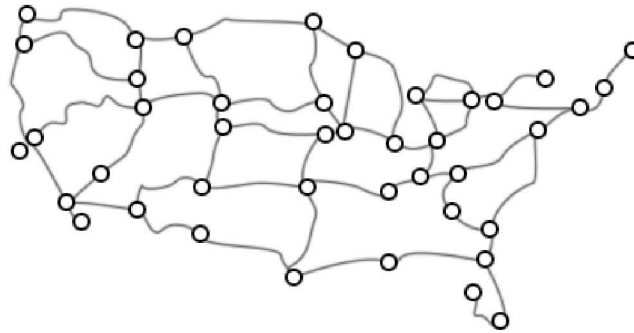


Figure 2-2: Schematic graph of US Interstate Highway System with random graph structure.

Since this graph is small, the degree distribution is approximately Binomial rather than Poisson. However, even for small random graphs, the central tendency of the degree distribution indicates that there are no unconnected nodes, relatively few low degree nodes, and no highly connected nodes, or hubs, in the graph.

In a large graph, the separation distance between any two nodes of average degree one can be large if \bar{k} is small, but as \bar{k} increases, this separation distance decreases rapidly. Short separation distances of this sort are popularly called a *smallworld* phenomenon (Milgram 1967). For a randomly chosen node, the separation distance between it and another randomly chosen node can be surprisingly small even for a very large network. This was popularized by the work of Stanley Milgram, who in 1967 studied the structure of social networks. His research empirically suggested that the average separation between any two people in the United States was 5.5, which when rounded up, led to the popular expression “six degrees of separation.” The efficiency exhibited by low separation distance and high \bar{k} is an artifact of the topological structure of the network.

A graph is said to be an *equilibrium network* if the network does not grow or decay (i.e., no nodes or edges are added or deleted with respect to time). There is a fixed number of vertices and the distribution of edges, once established, does not change. E-R graphs are usually deemed to be equilibrium networks.

2.2.3 Non-Equilibrium Networks

Until the late 1990s, the application of random graph theory to describe large networks was limited to E-R-type models. As data for large graphs (i.e., 10^6 nodes and larger) of communication and biological networks became widely available in electronic form, empirical studies revealed that the Poisson form failed to capture the observed degree distribution of large networks. One failure of the E-R model is its

assumption that the network is stationary with a fixed distribution of edges over a fixed number of vertices.

Most biological systems exhibit some form of growth whereby the network evolves according to the addition of vertices and edges with respect to time. Consider a growth scenario that begins with a small number of nodes on a substrate network. A substrate network is a single root node of a set of connected nodes. At each time step, a vertex is added to the network and an edge is placed between that vertex and a randomly chosen existing vertex. As with E-R theory, edges are connected with equal probability $p(k)$ which has the effect of the oldest (relative to the current node) nodes receiving a greater number of links. This is in contrast to the equilibrium E-R model in which the Poisson degree distribution imposes a narrow distribution of the number of links. The degree distribution of a growing random network is more purely approximated by an Exponential distribution:

$$P(k) \propto e^{-k/\bar{k}} \quad (2-5)$$

where, \bar{k} is the mean degree and the scale parameter of the exponential distribution. Although the degree distribution is over a discrete scale, the continuous Exponential probability density function (pdf) provides a good approximation for large \bar{k} . As infrastructure networks frequently evolve by phased expansion, it might be hypothesized that their non-equilibrium degree distribution is similarly Exponential.

Unfortunately, from empirical data the Exponential model of a non-equilibrium network appears an inadequate model for the structure of certain real world networks.

The Exponential distribution decays rapidly as k increases, such that very few nodes have a high number of links. Watts and Strogatz (1998) addressed this by using a *clustering coefficient* to explain why, in social networks, some individuals have a very high number of acquaintances than would be predicted by the Exponential graph. Their research suggests the existence of *hubs* in networks, where a significant number of nodes have a degree much higher than average. This behavior can be modeled by neither the E-R model nor Exponential structure.

2.2.4 Power-law and Heavy-tail distribution networks

Building on the non-equilibrium case, a further complicating factor is the method by which new vertices, added at each time step, attach themselves to the old network. E-R theory postulates that existing vertices have an equal chance to receive edges attached to new nodes. In practice, many networks exhibit a process of *preferential attachment*. Preferential attachment means that, the higher the degree of a node, the more likely that node will be to receive future attachments (i.e., “the rich get richer” or “popularity is attractive”). Equation (2-6) provides an expression for a linear preferential attachment process, in which the probability of attachment is proportional to degree (Barabási et al. 1999):

$$p(k_i) = \frac{k_i}{\sum_j k_j} \quad (2-6)$$

where k_i is the degree of the current, or new node and k_j is the degree of any existing or previous node in the network

Figure 2-3 depicts the relationship between hubs and other vertices in a network grown by preferential attachment. The seven colored nodes have the highest degree and are called hubs. These nodes are older relative to the lower degree nodes in addition to having higher than average degree.

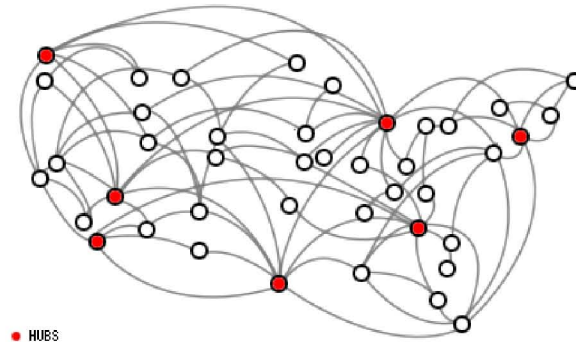


Figure 2-3: Smallworld network where hubs have above average number of links.

Networks with high-degree hubs, which are often generated by preferential attachment, are called smallworld networks because average separation distances within them can be surprisingly short. The short separation distance characterizes the efficiency in these topological structures over their Random (non-equilibrium) counterparts. Barabási (2002) presents an example demonstrating this efficiency using graph models representing WWW structure. Starting from the highest degree nodes or hubs, 67% of the nodes in the graph are reachable within one hop (i.e., separation distance of 1 edge). By contrast, in a similarly sized Random (E-R) network, only 27% of the nodes can be reached in one hop from the highest degree nodes.

Barabási and Albert (1999) were among the earliest authors to suggest that a Power-law rather than Exponential distribution might provide a suitable fit to the degree distribution in networks that grow by preferential attachment. Power-law distributions exhibit a distinctive “heavy tail” toward higher values of k . This heavy tail reflects the presence of hubs. Unlike the Poisson or Exponential distributions, Power-law distributions lack a characteristic scale and are thus said to be *scale-free*. Scale-free is a property used in the physics literature to describe functions that satisfy the property:

$$f(ax) = g(a)f(x) \quad (2-7)$$

Newman (2005) explains this property by showing that an increase by a factor in a in the units of measurement of x results in no change in the overall density $f(x)$ except for a multiplicative scaling factor.

The general form of the Power-law degree distribution for large N (e.g., Gurumohan and Hui (2003)) is:

$$P(k) \propto k^{-\gamma}, k > 0, 2 < \gamma < \infty \quad (2-8)$$

Thus, the simplest form of the Power-law distribution is the asymptotic form of the Pareto distribution:

$$f(x) = \frac{a}{x^{a+1}}, x \geq 1 \quad (2-9)$$

Where a is a shape parameter and $\gamma = a + 1$. Moments of order ν only exist for this distribution for $a > \nu$ thus the mean and variance are:

$$E(k) = \frac{a}{a-1}, a > 1 \quad (2-10)$$

and

$$Var(k) = \frac{a}{((a-1)^2(a-2))} \quad (2-11)$$

Usually, the Power-law distribution is said to be *heavy-tailed* when $a \leq 2$ and the variance (i.e., loosely called *degree of fluctuation* in the literature) is undefined. In this case, the distribution is considered to be scale-free. Further properties and statistical moments of the Pareto distribution are given in Appendix A.

Figure 2-4 summarizes the functional forms and properties of the E-R, exponential and Power-law degree distributions. Note that although degree distributions are defined over the discrete variable, k , for large k it is common to approximate the distribution by continuous processes.

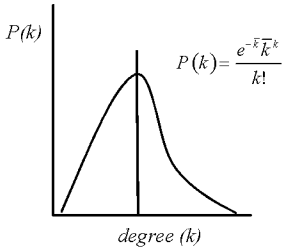
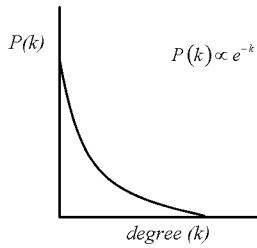
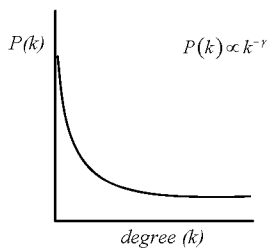
| Erdos-Renyi (Poisson) | Exponential | Scale Free (Power law) |
|---|---|---|
|  |  |  |
| Equilibrium (N fixed) | Growth w/ random linking | Growth w/ Pref. Attachment |
| Most nodes have the same number of links. | The oldest nodes have more edges, but hubs absent. | Some nodes have large degree (hubs). |

Figure 2-4: Summary of random graph forms, parameters, and properties.

Perhaps the most convincing examples of scale-free networks are that of the Internet and WWW. The WWW is a directed graph, the largest currently known to exist, with approximately 10^9 vertices representing web pages connected by 10^{10} edges representing hyperlinks (Yook et al. 2002). Empirical studies by Barabási and Albert (1999) examined the WWW pages at the University of Notre Dame to map the topology of the *nd.edu* domain. Based on a graph containing 325,729 vertices and 1,469,680 edges they found that a Power-law distribution fit the degree distribution with $\gamma = 2.1$ (indegree) and average separation distance (\bar{l}) of 11.2 nodes. This means that, on average, a web page is 11.2 clicks away from another web page chosen at random. Faloutsos et al. (1999) conducted a similar study of the topology of the Internet where the vertices are routers and the edges are the communication lines (e.g., Ethernet, fiber, etc.) connecting them. In examining ~150,000 routers connected by ~200,000 edges, they verified a Power-law structure with $\gamma = 2.3$ and average separation distance (\bar{l}) of 10 nodes.

An extensive literature (Watts et al. 1998; Barabási et al. 1999; Albert et al. 2000; Bush et al. 2001; Yook et al. 2002; Bornholdt et al. 2003; Newman 2003) has emerged over the past several years on the empirical properties of networks ranging from human sexual contacts to author citation relationships. Throughout this literature, there is an increasing collection of insights that can be discerned from the topologic structure of scale free networks. Of interest in this research are the qualities of random graphs (which include scale-free networks) that make them efficient in connecting disparate nodes and survivable in cases of degradation or attack.

2.2.5 Highly Optimized Tolerance (HOT)

Although statistical mechanics has provided a good basis for the existence of Power-laws and heavy-tails in networks, there are other frameworks which attempt to explain the existence of these extreme value distributions and “robust yet fragile” behavior. *Highly Optimized Tolerance (HOT)* suggests that complex, engineered systems such as computer networks and control systems maintain robustness to performance variation against that for which they were designed, but are unexpectedly fragile to extreme, unforeseen events (Carlson et al. 2000).

As an example, a framework has developed based on the classic percolation model of a 2-dimensional lattice (Stauffer et al. 1994). In this problem, the goal is the identification of the state at which percolation occurs. Percolation in this context is the transition from the state where all sites (i, j lattice or array locations) are connected contiguously, to the state of fracture or separation of sites into disconnected clusters. Exact solutions (i.e., the Harris-Kesten Theorem) have been found for the percolation

threshold of the site and bond (represented by occupied or unoccupied links between nodes in a lattice) percolation problems of 0.5 (Bollobas et al. 2005). In this context, percolation threshold is the critical density of sites or bonds above which a connected cluster spanning the entire lattice exists with high probability. Below the percolation threshold of 0.5, the lattice is more likely composed of disconnected clusters. The HOT framework posits that the sub-critical scaling of clusters (i.e., Power-law distribution), contributes unexpected vulnerability depending on how the clusters are organized.

Consider the example in Figure 2-5 (a-d). An $N \times N$ lattice (grid) represents a landscape susceptible to forest fires, where occupied sites correspond to trees (black) and unoccupied sites are vacant land (white). A perturbation to the lattice is defined as the setting of fire in a cell which burns it and its contiguous (i.e., connected) neighbors, called a cluster (c). The Yield, Y , is defined as the average density of trees left unburned after a perturbation occurs. Perturbations (i.e., sparks) occur according to a probability distribution, $p(i, j)$ where i and j are the lattice or array indices. By computing Y for each event, the distribution of losses due to fire is $f(c)$. The cumulative distribution of events of size greater than or equal to c is $F(c)$.

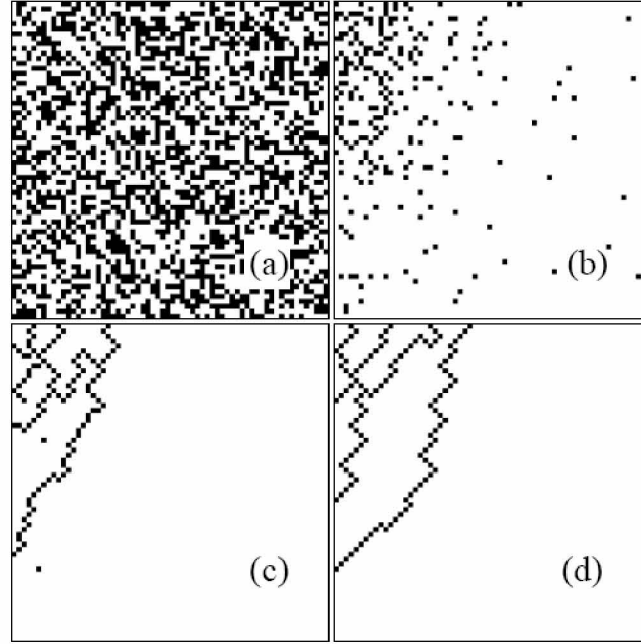


Figure 2-5: Cases of site percolation on an $N \times N$ lattice (Carlson et al. 2000).

A design parameter, D , is used to indicate the number of configurations in the lattice with Figure 2-5 (a), Figure 2-5 (b), Figure 2-5 (c), and Figure 2-5 (d) representing $D = 1$ (random percolation), 2, N and, N^2 (all possible configurations associated with the addition of one occupied site are tested), respectively.

As D increases from 1 to N^2 , the so called *tolerant* states emerge indicating patterns or organized “tree lines” optimally configured to separate clusters by open areas, not susceptible to fire. The events are shown to be power-law distributed by the form, $F(c) \sim c^{-\alpha}$, shown graphically in Figure 2-6.

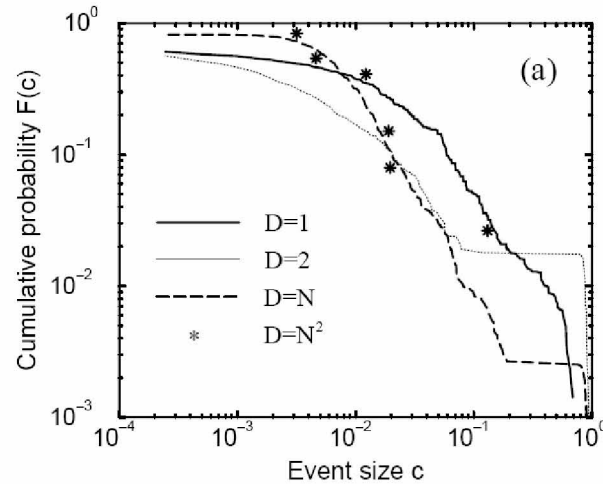


Figure 2-6: Cumulative Distribution of events (Carlson et al. 2000).

In successive iterations of the model, the *self-organized criticality* exhibited is similar to network evolution, but from a separate perspective. In the highly-optimized states, the “tree lines” of Figure 2-5 (d) are unlikely to catch fire, but should they, the entire tree line will be lost.

2.2.6 Network Survivability

Peter Baran, an engineer with RAND corporation is credited with the first practical conception of a distributed communications system such as the Internet (Baran 1964). Under the cold-war era threat of nuclear attack, the need for a *survivable* communications network was apparent. *Survivability* is the capacity of a network to retain end-to-end connectivity if nodes or edges are destroyed.

Figure 2-7 depicts three topologic structures Baran considered for forming a survivable communications system: (A) centralized, (B) decentralized, and (C) distributed. If portions of a survivable network were to be disabled, the system as a whole would continue to function. He concluded that cases A and B would not be

survivable in a deliberate attack and that only a distributed mesh topology such as C would endure because of the large number of redundant paths available between any source and destination pair. What Baran did not consider, however, was the capital cost required to establish physical connections among the then proposed nodes of the Internet (called ARPANet at the time). In considering that high cost, a decision was made to use the decentralized case (scale-free topology) instead (Barabási 2002).

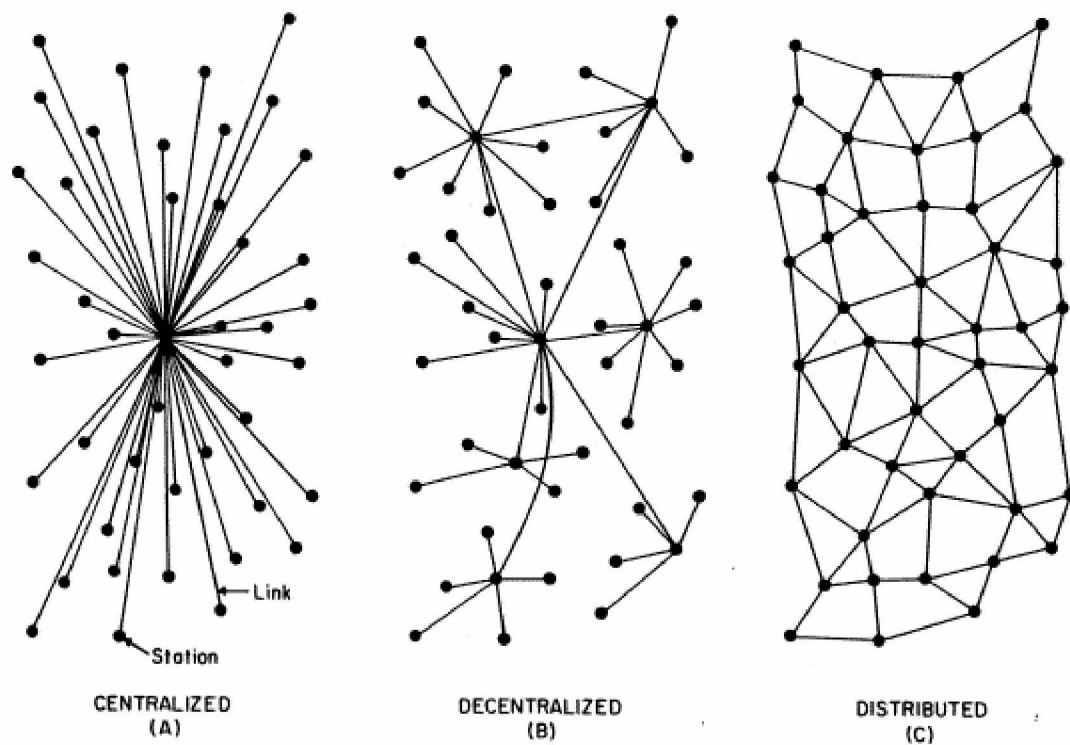


Figure 2-7: Topologic structures for a distributed communications system (Baran 1964).

The integrity of a network is characterized by the presence of its *giant component* (Dorogovtisev et al. 2003). A giant component or *giant connected component* is the largest connected subgraph of a network. For an undirected graph, it contains the largest set of mutually reachable vertices in a graph. Directed graphs feature an *in-component* and an *out-component* where the giant component is defined as the set of

vertices which are mutually reachable by a directed path. If a giant component is removed, partition in the network occurs and all that remains is a set of disconnected clusters (i.e., smaller components or “islands”).

Albert et al. (2000) hypothesized that scale-free networks are resistant to random failure, but highly vulnerable to deliberate disruption (attack). If a fraction of randomly chosen vertices were removed from a growing network at each time step, Albert et al. found that over 80% of the vertices needed to be removed before the giant component was destroyed. However, if a fraction of the most connected vertices (i.e., those with the highest degree) were simultaneously deleted (i.e., the hubs), the giant component was eliminated quickly.

The point at which the network undergoes partition and the giant component is destroyed is called the *percolation threshold* (Wilson 1985). The high percolation threshold for scale-free networks makes them simultaneously resistant to random attack and susceptible to deliberate attack.

Graph models and the properties of their topologies may not be useful unto themselves. For infrastructure networks, we want be able to correlate topologic features of the network with spatial properties in order to answer questions about their underlying growth and degradation processes. The next section describes previous work in modeling the spatial organization of networks.

2.3 Spatial Networks

The WWW and the network of scholarly author citations are abstract graphs that do not strictly exist in geographic space. The WWW is a large directed graph where web pages are nodes and hyperlinks are edges. Similarly, citations are directed edges and authors are nodes in the scholarly author network. Although web servers and authors are spatially (geographically) distributed, their location is not a parameter of their respective graphs and they can be thought of as *aspatial*. Because of their logical-only structure, there are no constraints on the number of edges that can be connected to a vertex, edges do not interfere with one another, and the graphs are non-planar. Spatial networks, on the other hand, are constrained by the limitations of geography, terrain, the natural and the built environment. The physical space surrounding a vertex where an edge may attach is limited and edges are relatively short because an edge can not go far without crossing another edge. It is believed, for example, that the primary problem with the reliability and capacity of the electrical power grid is the lack of suitable locations to build additional transmission lines (edges) (Holmgren et al. 2003). There are environmental, social, geo-political, and cost restrictions on the formation of new nodes and vertices. The costs of building and maintaining a network are proportional to the total length of its edges.

Spatial networks feature a dual topology depending on, for example, the infrastructure system they represent. Figure 2-8 shows a geographical and a logical view of the same conceptual region with highway, air, rail, and waterway networks.

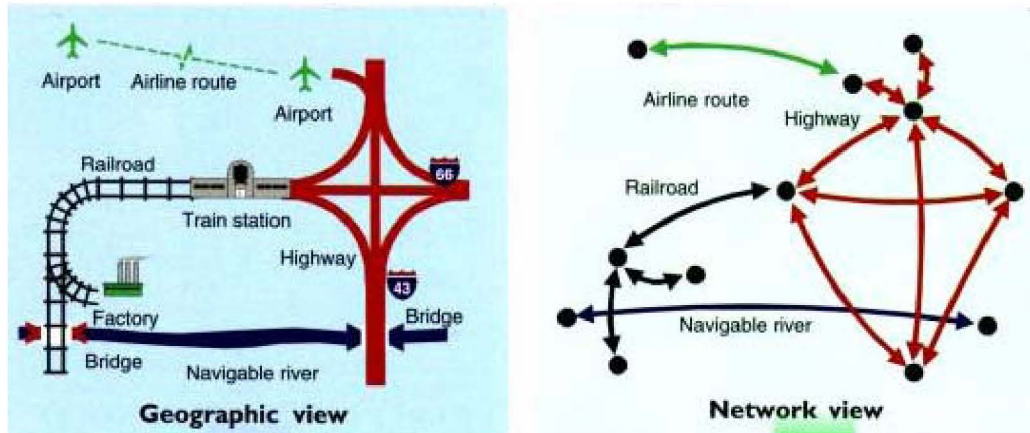


Figure 2-8: Conceptual representation of geographic and logical views of a network (Zeiler 1999).

The real world network is abstracted into two related graphs; a topologic graph composed of logical connections between nodes and links, and a geometric network consisting of *spans* and *span nodes* (Bhandari 1999). These related topologies can be quite different as the logical links between nodes (e.g., state roads) are composed of multiple geometric links between intersections. As was seen in the previous discussion of topologic structure, the incorporation of even a few long edges (i.e., long-haul connections bypassing intermediate nodes) dramatically reduces the network diameter for spatial networks as well.

2.3.1 Shape and efficiency

Geography presents constraints which prevent spatial networks from gaining the efficiency of exponential or smallworld networks. As will be seen, the constraints of planarity and Euclidean distance dominate the non-equilibrium behavior of spatial networks evolving over time.

Network evolution has been studied in the transportation geography literature by Black (2003), Kansky (1963) and others. Transportation network evolution occurs by a growth process over decades. Assuming m stages of growth, the graph during any stage t denoted by G^t , is a function of the previous stage graph G^{t-1} , yielding:

$$G^t = f(G^{t-1}, G^{t-2}, \dots, G^{t-m}) \quad (2-12)$$

The network topology at any time t is a function of the network topologies that preceded it, but this evolution must be placed in the context of the network's spatial and topologic structure.

Gaster and Newman (2004) compared the spatial shape of the US Interstate highway system, the domestic US airline network, and the location of Internet routers comprising the Autonomous Systems (AS) backbone. They focused on edge length, network diameter, and vertex degree. The authors demonstrate the planarity of the road network and cite a theoretical relationship by West (1996) showing that planar networks must have \bar{k} less than 6. For comparison, $\bar{k}_{road} = 2.86$, $\bar{k}_{airline} = 8.82$, and $\bar{k}_{router} = 3.93$. Whereas the road network is clearly planar and the airline network non-planar, there is some uncertainty about the spatial structure of the internet router topology which is discussed later. The authors establish an *effective edge length* (d_{ij}) relationship between the distance traveled along a path and Euclidean distance:

$$d_{ij} = \lambda\sqrt{n} + (1 - \lambda) \quad (2-13)$$

Where the indices i and j represent two arbitrary nodes and λ is a preference parameter with $\lambda = 0$ indicating long edge lengths with hubs and $\lambda = 1$ indicating short edges comparable to a mesh or E-R topology. The \sqrt{n} term compensates for scaling of nearest neighbor distances with network size, n . Using this relationship, the authors simulate the formation of each observed network and find mean degree values comparable with those found in the observed networks. They conclude that preference for spatial (Euclidean) distance, along with planar constraints, are important factors that contribute to the mean degree of spatial networks.

The shape and efficiency of spatial networks can be expressed as an integrated measure of path length and Euclidean distance called the *route factor* (Gastner et al. 2004):

$$q = \frac{1}{n} \sum_{i=1}^n \frac{l_{i0}}{d_{i0}} \quad (2-14)$$

where l_{i0} is the path length from vertex i to root 0 on a directed tree graph and d_{i0} is the Euclidean length from vertex to root. Gastner and Newman (2004) calculated route factors for the Boston commuter rail network and compared them with hypothetical topologies for a star topology and for a minimum spanning tree (MST) topology connecting the rail stations at their existing geographic locations. Figure 2-7 (A) is an example of a star-graph structure. A MST is a subgraph which connects all vertices together exactly once. The goal of the researchers was to assess the efficiency of the rail topology in terms of path (topologic) distance and Euclidean distance. An efficient spatial network should have two properties; 1) the mean path

length should be short to the root vertex and 2) the sum of all the edge lengths in the network should be low (i.e., the network is inexpensive to build and maintain). A star topology is the most efficient (optimal) topologically and in terms of route factor with $q=1$. A direct route exists from any source to destination in no more than two hops. The star topology is the most expensive to build as well, as a dedicated link is necessary from each vertex to the route. A MST topology is by definition the most inexpensive to build, but is inefficient in terms of route factor with $q \sim 2$ (i.e., on average, the shortest path length to the root is twice as long as the Euclidean length). The authors conclude that many spatial (and infrastructure) networks feature route factors on the order of 1.5 indicating surprising efficiency.

2.3.2 Degree and Accessibility

The efficiency inherent in networks has been previously discussed in relation to the characteristic shape of the degree distribution. Smallworld or scale-free networks tend to follow the functional form $P(k) \sim k^{-\gamma}$ with $2 < \gamma < 3$, but how the nodes are organized and differentiated isn't captured in the degree distribution. In considering spatial in addition to topological structure, other metrics are useful for describing the degree to which a topology exhibits smallworld or scale-free behavior.

The *accessibility index* is the primary measure used in transportation planning to assess the “reachability” of a node on a directed network. It is defined as A_j : for a given node, the sum of the shortest path distances to all other nodes in the network (path distance or travel time, d_{ij}) by:

$$A_j = \sum_{i=1}^n d_{ij} \quad (2-15)$$

The average shortest path is defined for the entire network giving the average length of the shortest path from every node i to every other node j .

$$\bar{\ell} = \frac{1}{N(N-1)} \sum_{i,j} d_{ij} \quad (2-16)$$

Note that $\bar{\ell}$ is defined for a connected a graph. In the case when partition in the network occurs and the graph is separated into disconnected subgraphs or clusters, $\bar{\ell}$ is measured for the largest remaining component.

These measures can be used to describe the organization of the *nodal hierarchy* (i.e., the rank ordering of hubs based on criticality). Nodal hierarchies can be constructed based on degree alone, but accessibility or accessibility normalized by average shortest path provides a more accurate picture of topologic organization for directed graphs.

For spatial networks such as infrastructure, the nodal hierarchy should also reflect the local and global connectivity and relationship between regional service areas. For example, are nodes acting as sources or sinks, or relays (hubs)? Nodes that have high degree (connectivity) may not be highly accessible if there are few paths to reach it from disparate parts of the network.

Gorman (2004) investigated the spatial and topologic structure of the US fiber optic infrastructure to determine the vulnerability of critical nodes. To create a nodal

hierarchy, he performed a regional analysis to assess the local ($q_{i(r)j(r)}$) connectivity of node i in region r and global ($g_{i(r)k(s)}$) connectivity of node k in region s . The *global connectivity index* ($C_{i(r)}$), then, is the ratio between a node's local and global connections, weighted by the total number of global and local connections for the entire network:

$$C_{i(r)} = \left(\frac{\sum_{s \neq r}^m \sum_{k(s)} g_{i(r)k(s)}}{1 + \sum_{j(r), j \neq i} q_{i(r)j(r)}} \right) \times (G + L) \quad (2-17)$$

The ratio of global to local links provides an indicator of how well a node (in this case a city) acts as a global connector in the network normalized by the total number of links. Gorman compared nodal hierarchies based on degree, accessibility, and regional (spatial) connectivity and found differences in the rank ordering suggesting that the spatial organization influences the criticality of nodes in the network with direct implications on vulnerability. He further studied the role of node species (e.g., source, sink, relay) and the distribution of aggregate capacity which will be discussed in the following sections. The general conclusions were that the spatial nodal hierarchy provides a more complete representation of information infrastructure distribution and that spatial location can be just as or more important than topologic connectivity for understanding vulnerability.

2.4 Efficiency and Risk

The efficiency gained from certain topologic structures does not come without added vulnerability. Baran's (1964) work on suitable topologies for a distributed communication system was based on survivability and the capacity of a network to absorb loss of nodes, links, and paths while maintaining an acceptable level of performance. The vulnerability of networks, especially information infrastructure, has received recent attention based on the work of Gorman (2004; Gorman et al. 2004) and Albert et al. (2000; 2004).

The consideration of infrastructure vulnerability in a risk context can be broadly divided into infrastructure hazard analysis, vulnerability analysis, and risk analysis. The focus in hazard analysis (or hazard identification) is in identifying threats to an infrastructure system, its users, and surrounding people and resources. The term 'hazard' is often used to refer to a natural or terrorist phenomenon that might have adverse impacts on a network. Vulnerability analysis focuses on the susceptibility to loss from hazards. Vulnerability, somewhat similar to the concept of fragility in reliability theory, can be viewed as the inverse of resilience, as resiliency implies less susceptibility to perturbations in the network. For example, identifying the lifelines in a given area that might be compromised by a failure would be infrastructure vulnerability analysis. Risk analysis incorporates the likelihood of a hazard occurring in addition to the vulnerability of a network should the hazard occur. The loss of a lifeline to an event, or a reduction in its service, will have varying consequences depending on the design of the lifeline, its importance in the system, and the spatial-economic consequences to the region. Analyzing this variation would constitute

consequence analysis. In risk analysis, the likelihood of an event, the corresponding vulnerability of the network, and its consequences associated with that vulnerability are all incorporated. Risk is quantified as the product of probability and consequence often with the goal of identifying potential disruptions that represent an “unacceptable” risk.

The standard risk-based approach stresses that resources should be allocated to protect against events that have the highest risk calculated as described above. In networks, this requires an integrated view of the spatial and topologic structure as well as the composition of the nodes and edges and utilization of the pathways through the network (i.e., flows).

2.4.1 Structural Vulnerability

Albert et al. (2000) studied error and attack tolerance on graphs of Internet topologies with 3.3×10^5 vertices and 1.5×10^6 links. They hypothesized that smallworld (i.e., heavy-tail) distributed networks have resistance to random failure, but susceptibility to intentional damage. Random failures were modeled by the instantaneous removal of a fraction of randomly chosen vertices. Attack was modeled by the instantaneous deletion of the highest degree nodes based on a nodal hierarchy. The average shortest path (\bar{l}) and the size of the largest connected component (W) relative to the undamaged state were used to measure the resistance of the network.

Figure 2-9 depicts the results of their simulations for an exponential and scale-free topology. For failure due to the random deletion of nodes (represented by the solid line), a critical threshold (f_{cr}) is reached for the exponential topology when two thirds

of the nodes are deleted. At this point the average shortest path spikes upward and the diameter goes to zero as partition in the network has occurred. For failure due to intentional deletion of nodes (targeting of the hubs, dotted line), the critical threshold (f_{ci}) is reached when only one third of the nodes are removed. In contrast, the scale-free network experiences no appreciable increase in average shortest path until almost all of the nodes are removed. For intentional attack however, the scale-free network undergoes partition (very rapid increase in average shortest path and precipitous fall in diameter) when 10-15% of the highest degree vertices are removed. This result is consistent with their hypothesis that scale-free topologies are vulnerable to deliberate attack.

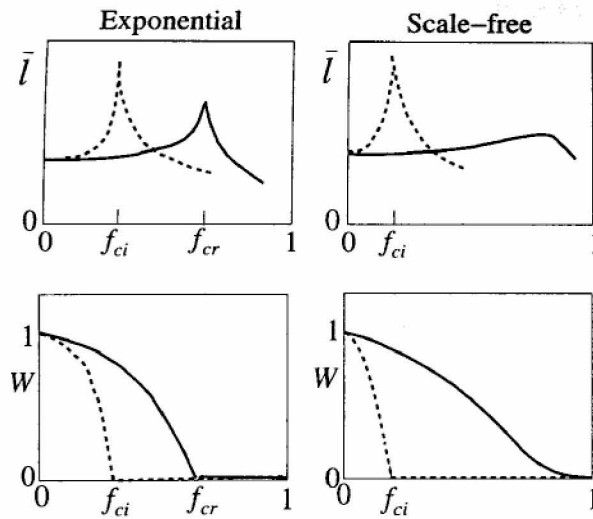


Figure 2-9: Simulated failure/attack for different topologies (Dorogovtsev et al. 2003).

Gorman et al. (2004) extended this hypothesis to include the role of spatial organization in the nodal hierarchy for simulated failure and attack tolerance. He concluded that the most connected hubs do not always lead to the same percolation rate (i.e., rate of decay of connectivity with respect to fraction of nodes removed)

under simulated attack as attacks based on spatial nodal hierarchies. Clearly, there are other factors that contribute to attack or failure resistance when the full context of spatial organization, topologic connectivity, network flows, and utilization are considered.

Albert et al. (2004) studied the structural vulnerability of the North American Electrical power grid. The network, as studied, consisted of 14,099 nodes (substations) and 19,657 edges (transmission lines) with a total length of over 1 million kilometers. Vertices in the analysis were classified as generators (electricity sources), distribution points (voltage transformers located near end-users) or relays (high-voltage transmission points). The analysis was similar to their previous work (Albert et al. 2000) except that in this case they specifically considered the flows over the network and the requirement that electrical loads be re-disturbed to neighboring infrastructure in the event of a failure. They found that the complementary-cumulative degree distribution (CCDF):

$$P(k > K) = \sum_{k>K} P(k) \quad (2-18)$$

follows an Exponential form:

$$P(k > K) \sim e^{-0.5K} \quad (2-19)$$

indicating that the probability of high degree nodes is less than in scale-free networks, but higher than in random E-R networks.

Betweenness $\sigma(m)$ (i.e., the number of shortest paths traversing a node) was used as a proxy for the cumulative electrical load being carried across the relay nodes and revealed that 40% of the relay nodes participate in only tens or hundreds of paths, while 1% participate in more than a million paths each. These relays were found to have less than average degree indicating they are not hubs yet still present significant vulnerability should disruptions occur in these nodes. A lack of redundant paths in the long-haul distribution network was hypothesized and evaluated by measuring the edge range. *Edge Range*, ED_{ij} , is defined as the distance between two endpoints of an edge if the edge connecting them is removed:

$$ED_{ij} = 1 - \frac{\sum l_j}{\sum l_i} \quad (2-20)$$

Albert et al. (2004) conclude that the availability of short alternative paths is sufficient, however 15% of the edges in the power grid have in infinite edge range indicating no redundant paths exist for those long-haul edges.

2.4.2 Flows and Network Utilization

Albert et al. (2004) continued their analysis of the North American electrical power grid to consider local and global electrical load distribution in the event of single and multiple failures and considering the utilization of nodes. Instead of average shortest path or diameter, they measured connectivity loss (i.e., the loss in ability of distribution substations to receive power from generators) as nodes were removed according to a degree-based nodal hierarchy. Figure 2-10 shows the connectivity loss

for four failure scenarios with fraction of transmission nodes removed (%) on the horizontal axis and connectivity loss to the power grid (%) on the vertical axis..

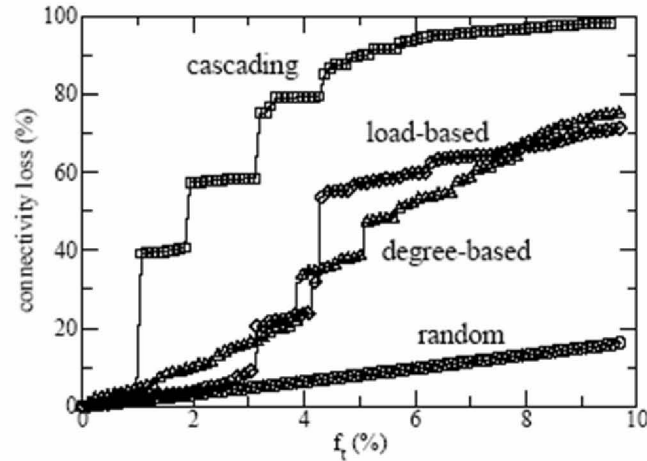


Figure 2-10: Connectivity loss in the North American electric power grid based on simulated failure/attack (Albert et al. 2004).

In the random case, the removal of transmission nodes resulted in a linear, gradual loss in connectivity (i.e., 10% of nodes removed resulted in approximately 20% power grid connectivity loss). In the degree-based case, transmission nodes were selected and deleted from the graph based on a nodal hierarchy (rank ordering from highest to lowest degree). Note the discontinuous jumps in connectivity loss corresponding with percolation and destruction of the largest components in the network. In the load-based case, transmission nodes were targeted based on their electrical load. Finally, in the cascading case, nodes with the highest electrical load were attacked, but their load is redistributed to the neighboring infrastructure resulting in cascading failure as automatic electrical switching equipment removes elements of the network once carrying capacity has been exceeded preventing physical damage to the network. In explicitly considering the topology, flows, and

utilization of nodes in the network, the effects of targeted attack can be greatly amplified as seen in this example.

2.4.3 Trading-off Efficiency and Survivability

The consideration of cost and efficiency trade-off has been discussed for topological and spatial properties in the transportation geography literature (Black 2003) and for the shape and efficiency of spatial networks research done by (Gastner et al. 2004; Gastner et al. 2004). The vulnerability of scale-free topologic structures has been shown by (Albert et al. 2000). and the role of spatial organization in network vulnerability has been show by Gorman and Kulkarni (2004) and Gorman et al. (2004).

The efficiency and survivability trade-off has not been covered extensively in the literature. Bhandari (1999) has presented work on algorithmic techniques for ensuring redundant paths, but knowledge of a fixed underlying topology is assumed. An important research problem is the consideration of the efficiency and survivability trade-off in the context of dynamic, reconfigurable topologies.

2.5 Network Topology Control

Routing has always been the principal means for network control in transportation, distribution (e.g., natural gas) and communication systems. In these infrastructure networks, topologies are designed based on minimum cost (e.g. minimum length of cable), the availability of land (e.g., right of ways), and necessary extent (e.g., required service areas). Often these networks evolve over time, although not continuously. Planned expansions and maintenance, and capacity upgrades are common to keep up with increasing demand. However, the topology of the oldest part of the network, the so-called backbone, remains fixed.

The ability to globally alter the pathways of flow to enable the creation of more efficient or more survivable routes when disruptions or capacity limitations occur is a unique feature of wireless networks used in sensors and communications. Base station architectures (e.g., cellular telephony) and peer-to-peer architectures (e.g., MANETs (Mobile Ad-hoc Networks)) both involve broadcast radio communication where topologies can be manipulated for better spatial-temporal spectrum utilization, lower interference, or better power conservation. Base-station architectures are efficient in spatial coverage and for handling mobile hosts (e.g., call “hand-off”). Their backbones (i.e., landlines) are fixed, however, leading to network layer limitations (e.g., localized congestion) and physical layer vulnerability. Peer-to-peer architectures are highly survivable, but have limited power and bandwidth and are inefficient for long-haul communication due to multi-hop routing. Further, these networks have been proven to be non-scalable for large N . Gupta and Kumar (1999)

found that when N identical, randomly positioned nodes form an ad-hoc wireless network, the maximum possible throughput (θ) per node is:

$$\theta \sim \frac{1}{\sqrt{N \log N}} \quad (2-21)$$

with the maximum bit-distance product that can be transported by the network per second is $O(\sqrt{n})$. The limited bandwidth and scalability of peer-to-peer networks and the congestion and survivability concerns of fixed-backbone base station networks require a new paradigm for promoting survivable high bandwidth infrastructure sensing capability.

Point-to-point, directional wireless communications technology has evolved from high-frequency microwave RF, to Free Space Optical (FSO), to hybrids of both RF and optical. High bandwidth fixed FSO links have been deployed in military and commercial applications over the past 10 years. Wireless-bridging of fiber networks from building roof tops is a common deployment, but range and atmospheric attenuation limitations have hindered widespread adoption of the technology. The advent of reconfigurable, hybrid, point-to-point networks with hardware/software systems for *topology control* presents an opportunity for research in the application of this combined network architecture for the security of critical infrastructure networks (Milner et al. 2003).

Topology control combines algorithms for topology reconfiguration with pointing acquisition and tracking (PAT) techniques to dynamically reform the network thereby

improving quality of service (QoS) and throughput (Davis et al. 2003). The software that collects link state information from the network, re-calculates the topology, and disseminates the new topology to the rest of the network is the primary interest in this research.

Optimal topologies are arrangements of nodes and FSO or hybrid FSO/RF links with 2- (i.e., ring), 3-, or 4-degree, that produce the best performance with the fewest number of links. Performance is separated into the physical and the network layers.

2.5.1 Physical Layer Optimization

Physical layer topology control is concerned with minimizing the cost (expressed in terms of bit error rate) of the graph representing the target topology. Atmospheric attenuation or other obscuration reduces the effective range (i.e. physical separation distance) possible between nodes for a required QoS. In optimizing the topology, the minimum cost ring, for example in 2-degree networks is sought):

$$Cost(T_c) = \min \sum_{(i,j) \in T_c} c_{ij} \quad (2-22)$$

where T_c is the cost-optimal topology and c_{ij} is the individual link cost.

This problem is mathematically equivalent to the Traveling Salesman Problem and has been shown to be NP-Hard (Dantzig et al. 1954). Exact, brute-force solutions feature computational complexity $O(n!)$ with dynamic programming solutions available in exponential time, $O(n^2 2^n)$.

Heuristics for the TSP and for the physical layer optimization problem have been developed with fast (i.e., milliseconds) solutions for networks up to $N=20$. Minimized cost dictates the capacity of each link, but congestion of traffic via the network layer must also be considered.

2.5.2 Network Layer Optimization

Network layer topology control is concerned with minimizing the congestion on the maximally loaded links (expressed as throughput in bits per second). In the event that source or relay traffic at a node causes congestion making routes through that node unavailable, network layer optimization can calculate a new topology which minimizes the congestion on the reconfigured topology:

$$Con(T_R) = \min \left(\max_l \sum_{(i,j) \in l(T_R)} r_{ij} \right) \quad (2-23)$$



where T_R is the congestion-optimal topology, l is a particular path (route) and r_{ij} is the individual link congestion.

The problem consists of first choosing an appropriate topology based on observed traffic demand and then applying routing to minimize congestion on the selected topology. The minimum congestion problem has been shown to be NP-Complete (Desai 2003). Because of the routing process, an analytical expression of computational complexity for the network layer optimization is not available. Fast-performing heuristics have been developed, however, which generate near-optimal topologies with respect to the network layer on the order of milliseconds for $N < 30$.

2.5.3 Multi-Objective Optimization and Trade-off

While the individual heuristics provide fast, near optimal topologies, the physical layer heuristic ignores the behavior of the network layer, and vice versa. This presents a challenge as both the physical and network layers contribute to the selection of an optimal topology.

Consider the example in Figure 2-11. Two candidate topologies are considered for a 4-node system. Topology 1 yields a lower cost (i.e., bit error rate, BER) and is therefore preferable to topology 2 in the physical layer. In the network layer, however, Topology 2 has a lower level of congestion and it is preferable. Given that we wish to minimize cost and congestion for the same 4-node system, which topology is best? When regarding the system as a whole, a third topology may be needed, in which the physical and network layer objectives are jointly optimized. A multi-objective optimization formulation can be used to derive the third topology.


Topology 1 Topology 2

| | | |
|--|-----------|----------|
| Physical layer: Aggregate Network Cost (BER) | <u>10</u> | 12 |
| Network layer: Traffic congestion (BPS) | 15 | <u>5</u> |

Figure 2-11: Example of physical/network layer mismatch (Zhuang et al. 2004).

The topology control problem, then, is formulated as a two-objective optimization problem:

$$\min \left\{ \sum_{(i,j) \in T} c_{ij}; \max \sum_{(i,j) \in I(T)} r_{ij} \right\} \quad (2-24)$$

where T is a typical goal topology by which we seek to jointly minimize the aggregate physical network cost and minimize congestion on the maximally loaded links, $I(T)$. Heuristics have been developed that use a weighted sum of both objectives to arrive at topologies that are joint in both layers. The complexity of these heuristics is comparable to the individual heuristics as they are both utilized in the selection of a topology. These near-Pareto optimal topologies are slightly less efficient with respect to the individual objectives of cost or congestion, but more accurately account for the true behavior of the network.

2.5.4 Challenges in Topology Control

Software algorithms that can produce near-optimal topologies in near-real time are an important component for topology reconfiguration. However, there remains some significant research challenges with respect to the survivability of particular topologies, the scalability of optimization heuristics to very large networks, and the prediction of physical and network layer constraints as the network evolves.

Algorithms for ring, 3-degree, or mesh (e.g., 4-degree) topologies usually contain constraints for bi-connectivity (i.e., degree > 2), to insure redundant paths (Milner et al. 2005). In other words, bi-connectivity insures at least two disjoint paths between any pair of nodes in the network exist. For 2-degree nodes optimizing on minimum aggregate cost, this can be expressed mathematically as:

$$\begin{aligned} & \min \sum_{(i,j)} b_{ij} c_{ij} \\ s.t. & \begin{cases} \sum_j b_{ij} = 2, \forall i \\ b_{ij} = b_{ji}, \forall i, j \end{cases} \end{aligned} \quad (2-25)$$

where b_{ij} is a Boolean variable indicating the presence of a link. The survivability condition adds to the complexity of the optimization problem and is based on steady-state conditions in the network. If link and node state information is not globally known, and network layer behavior not considered, an infeasible or inferior topology solution may result. Conversely, a globally survivable topology may be inefficient locally. Survivability in the context of network evolution may provide more insight into applicability of bi-connectivity constraints network-wide and under dynamic conditions.

The calculation of a topology solution for a given network is independent of the ability to execute a reconfiguration into that topology. One approach involves the use of a Designated Topology Control Node (DTCN) which is responsible for computing an optimal solution with respect to an objective. The DTCN can be advantaged in terms of location within the network (i.e., spatial and topologic) and can possess additional computational capability. However, mechanisms for replication of the DTCN and seamless hand-off to other nodes of its duties are needed if global survivability is required. *Self-organization*-based topology control (i.e., distributed topology control) is the logical approach for meeting this need with some research on bootstrapping of networking topologies already completed (Liu et al. 2005).

Computational complexity and deployed service areas are a concern for large N backbone networks. The current base-station-like architecture envisioned for hybrid RF/FSO sensor networks may be severely limited for large deployments given the effective link ranges available. 1 Gb/s nominal data rates over link ranges of 1 km are presumed given hybrid RF/optical media channels. For adequate performance with respect to near-real time topology solutions, PAT and reconfiguration time notwithstanding, the maximum deployed range of the back bone is on the order of 10 km² for a 20 node system. This assumes each base station has a service area of ~ 0.8 km² with minimal overlap to surrounding base station/transceiver/clusterhead service areas. Near-real time topologies for larger networks over larger areas may be unattainable. By applying topology control locally, and by considering the spatial evolution of the network, more efficient application of the available topology control heuristics may be possible.

2.6 Summary

This chapter has presented a context for representing infrastructure and sensor networks as graph models. Graph theoretic, spatial, structural, and control properties have been discussed, as well as implications of these properties on the efficiency and vulnerability of network systems, particularly sensor networks.

The relevant graph theory for statistical models of large networks such as the Internet and WWW was discussed. Smallworld networks (i.e., networks with power-law or scale-free degree distributions) were presented in the context of their small separation distance between nodes (i.e., efficiency), resistance to random attack, and susceptibility to partition when its hubs are specifically targeted. Heavy-tail distributions and their statistical properties (i.e., moments) were discussed as indicators of survivability for homogenous and heterogeneous (i.e., hierarchical network structures).

The spatial properties of networks were discussed especially the physical constraints that limit some of the efficiencies present in abstract logical networks. Planarity and physical space constraints limit the number of connections possible at a node. Spatial properties also contribute to the vulnerability of networks such as the fixed communications backbone where close proximity (e.g., co-location) creates unexpected inter-connections and inter-dependencies in otherwise unconnected infrastructures.

The structural properties of infrastructure networks were presented for the North American power grid. Spatial networks such as the high-voltage electrical

transmission infrastructure feature structural vulnerabilities apart from their topology. Low-degree and isolated nodes are not hubs, but their failure can disrupt significant end-to-end flows of power and cause cases for cascading failures when redundant paths are not available can carrying capacity is exceeded forcing automatic switched isolation.

Network topology control for wireless, point-to-point backbone sensor networks was presented as a significant bridge between the high bandwidth and coverage capacity of base-station oriented networks and the survivability and reconfigurability of peer-to-peer architectures. Fast performing heuristics are available to compute optimal topologies with respect to minimum aggregate network cost of the physical layer, minimum congestion of the network layer, or both. Limitations on computational complexity, scalability, and survivability in the context of evolving network conditions were presented and serve as motivation for the development of self-organization-based topology control techniques.

3 Chapter Three – Vulnerability Analysis of Sensor Network Infrastructure

Civil Infrastructure is vulnerable to natural and man-made hazards and consequently so are the sensors put in place to monitor that infrastructure. New capabilities in infrastructure security are possible through the networking of sensors, but the connections between these sensors are also vulnerable to disruption. In order to understand and quantify the vulnerability of sensor networks for infrastructure security, it is necessary to measure the sensitivity of these networks to random and intentional damage.

Consider the case of video surveillance. The City of London, England maintains a network of 550,000 CCTV (closed circuit television) cameras over 1,572 km² for public safety video surveillance (Renno et al. 2001). The CCTV system includes fixed wire-line communication links connected to dozens of monitoring stations where video feeds are aggregated, archived, and screened. In July 2005, two separate bombing attacks occurred (a third was attempted) on London's underground (subway) and bus transit systems resulting in approximately fifty fatalities and hundreds of injuries. Severe disruptions to the transit and surface transportation systems occurred. What is not known is the extent to which the CCTV network was damaged or disrupted during the attacks and what loss of surveillance capability occurred. What is known is the extent to which the CCTV network was crucial to forensically identifying those responsible for the attacks.

In the event of natural or man-caused disruption to physical infrastructure or lifeline networks, what fraction of the surveillance network is affected? Given that surveillance or other sensors are distributed around critical locations, is the amount of monitoring capability linearly related to the amount of damaged infrastructure? We expect networks of sensors to have different topologies, but does the spatial and logical layout of the underlying infrastructure dominate possible variation? Does the disruption sensitivity of sensor networks resemble that of Internet or WWW topologies featuring power-law-based heavy tail distributions?

These questions motivate the analyses of sensor network vulnerability presented in this chapter. Whereas the previous work in Chapter 2 has discussed graph theoretic, spatial, and structural vulnerability of particular networks, this chapter looks at the unique problem of *dependent topologies* (i.e., sensor networks depending on underlying infrastructure) and their *derived vulnerability* in response to random or targeted attack.

This chapter investigates the sensitivity of sensor networks to various forms of disruption in order to quantify the risk and vulnerability of dependent topologies and provide estimates of derived vulnerability. The hazards to the infrastructure network, and therefore the risks, are spatial, but the consequences of those risks are topologic based on the dependent logical organization of the network. This chapter applies a simulation-based approach for generating sensor network topologies and measuring the variation in connectivity and performance in response to perturbations based on topologic or spatial organization.

3.1 Network Sensitivity to Topologic and Spatial Perturbations

As shown in the previous chapter, numerous studies have examined the topologic structure of real world networks, the efficiencies present as a result of their structure, and the implications of that structure when met with random failure or intentional attack. Few studies have examined the combined spatial and topologic behavior of networks in response to disruption and no study of dependent topologic behavior and derived vulnerability is known to exist.

3.1.1 Dependent Topologies

A *Dependent Topology* is defined as a logical organization of graph elements (nodes and edges) based all or in part on the topology of another graph. Mathematically, a dependent topology can be written as:

$$G(V, E)_D = f(G_I(V, E)) \quad (3-1)$$

where G_D is the dependent graph and G_I is the independent graph. The sets of nodes (vertices) and edges for G_D are physically different, unconnected topologically, and related generally by proximity to the nodes and elements of G_I . This means that an edge in G_D cannot be substituted for an edge in G_I and vice versa as in this context a node in G_I represents an intersection of an infrastructure lifeline (e.g., pipe intersection or electrical transmission node) and a node G_D is a sensor (e.g., surveillance node). Still, a disruption in G_I may cause disruption in G_D .

The constraints, shape, and efficiency of spatial networks discussed in Section 2.3 are relevant to sensor networks composed of dependent topologies. Spatial networks with planarity and physical space constraints limit the number of edge attachments possible or economically practical at a given node location. These constraints which limit some efficiency also contribute to survivability and vulnerability reduction. Design trade-offs between efficiency and survivability occur in the planning process for physical infrastructure. For dependent sensor network topologies, these trade-offs differ and increase in complexity when active topology control is applied in real-time. The network must simultaneously maintain adequate spatial coverage, limit congestion of sensory data, and maintain an adequate level of service in terms of reliability and survivability. As will be discussed in Chapter 4, self-organization behavior and topology control processes are facilitated by the sensitivity of the dependent network and so build upon the analyses of this chapter.

The identification and evaluation of dependent sensor network topologies is achieved in part by examining their sensitivity both separately and in conjunction with associated lifeline infrastructure networks. The sensitivity analyses are used to quantify the derived vulnerability for the dependent sensor network. In treating the sensor network independently, effectively as G_I , the survivability of the network is assessed in terms of variation in graph-theoretic and spatial coverage measures as the network is disrupted. In the dependent case, the sensitivity is assessed using the same spatial and graph-theoretic measures, but in response to disruptions targeting (or randomly occurring) in the independent network only.

3.1.2 Derived Vulnerability

Derived Vulnerability is the vulnerability of the sensor network taken or inherited from the underlying infrastructure network. To revisit the discussion of Section 2.4, the concept of vulnerability analysis can be decomposed into hazard analysis, vulnerability analysis, and risk analysis. Hazard analysis focuses on the identification of specific threats to the infrastructure system (e.g., natural phenomena or terrorist attacks). Vulnerability analysis determines the susceptibility to loss from hazards (e.g. impact or consequence modeling) and risk analysis weights the likelihood of a hazard occurring with the consequences to the network should the hazard occur. For sensor networks, vulnerability can be separated into distinct criteria for the independent topology (i.e., the infrastructure network) and the dependent topology (i.e., the sensor network). The goal is to establish which hazards, vulnerabilities, and risks are attributable to the sensor network itself and which are inherited from the independent topology. Table 3-1 presents the independent and dependent criteria for derived vulnerability.

Table 3-1: Derived vulnerability criteria for Infrastructure sensors.

| VULNERABILITY COMPONENT | INDEPENDENT CRITERIA (LIFELINE NETWORK) | DEPENDENT CRITERIA (SENSOR NETWORK) |
|--------------------------------|---|--|
| Hazards | Service Disruption | Sensing or Surveillance Disruption |
| Vulnerability | Location, co-location, inter-dependency, conveyance | End-to-end connectivity and Coverage |
| Risk | Loss of connectivity or survivable (redundant) pathways | Loss of Sensor/Surveillance capability |

Hazard criteria are used to identify phenomena that could cause disruption and assess their possibility of occurrence. The independent lifeline infrastructure network is affected by natural hazards (e.g., hurricanes, earthquakes, fires, etc.) as well as targeted terrorist attacks. Because of its proximity, the dependent sensor network can share these hazards and also have its own. Bomb blasts in a transit station affect the transit network and the sensor network, while deliberate damage to or jamming of a surveillance sensor are dependent network hazards. The separate criteria exist to distinguish which hazards may disrupt both networks and which may affect the networks separately.

Vulnerability criteria are concerned with estimating the susceptibility to disruption for independent and dependent networks. Natural and man-made hazards are spatial in nature causing an impact over a wide area or at a specific point or series of points. Since infrastructure is often co-located in right-of-ways or transportation corridors, separate systems can be in effect inter-connected. Systems can also be inter-dependent (e.g., electricity and communication) such that disruptions in one system cause cascading failures in other systems. The assessed vulnerability of a network component may be high even without apparent co-location and inter-connection issues if the conveyance (e.g., traffic, power, gas, water flow) passing through the component is large relative to the surrounding network. The vulnerability of the sensor network inherits the co-location criteria from the independent network in most cases, but it is principally susceptible to disruption caused in its own network. Loss of sensor nodes, including any edges attached to those nodes, results not only in lost surveillance coverage but also in loss of end-to-end transmission capability and loss

of routes. This is due to the network's ad-hoc structure (i.e., nodes acting as data sources as well as relays for other nodes).

Risk criteria are concerned with estimating the consequences of disruption weighted by the likelihood of occurrence. Figure 3-1 shows a series of conceptual complementary cumulative distribution functions (CCDFs) or risk curves. CCDFs show exceedance probability (i.e., $P(X \geq x)$) versus consequence. Mathematically:

$$CCDF_X(x) = P(X \geq x) = 1 - \int_{-\infty}^x f_X(u) du \quad (3-2)$$

for $-\infty < x < \infty$. CCDFs are used to estimate exceedance probability (e.g., the probability that fraction of nodes removed will exceed a certain value) (Baecher et al. 2003). A value of x is a consequence, in this case negative. Increasing values represent increasingly negative consequences.

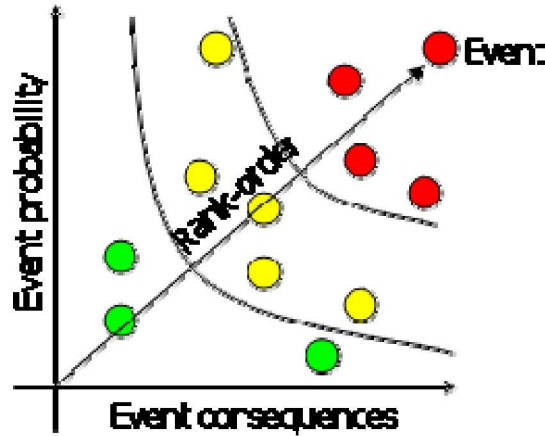


Figure 3-1: Conceptual risk curves (CCDFs) (Baecher et al. 2003).

As can be seen from the figure, even if an event with a high probability of occurring effects a vulnerable infrastructure component, if the consequences of that event are small, then the risk is also small. Risk curves can be used to represent variation in consequences, uncertainty in a particular consequence, or rank events in order of increasing risk. Or, as will be described later, they can be used to classify vulnerable structures (e.g., topologies) based on risk.

In terms of risk criteria, the risks to independent networks are the loss of service. A high consequence event may involve a non-redundant backbone link where a lesser consequence event may be the loss of a redundant path. The dependent network risk criteria are conditional; given the loss of the backbone link, estimating the risk of loss of 1) surveillance capability; and 2) sensor communication with local sensor nodes and long-haul connected nodes forming the sensor network backbone.

3.1.3 Quantifying Derived Vulnerability

Vulnerability analysis is often performed in a scenario context where vulnerability is parameterized by triples. Kaplan (1997) introduces the vulnerability measure (Ω) as the universal set of the triplet; scenario (s_a), likelihood (p_a), and consequence (w_a):

$$\Omega = \{s_a, p_a, w_a\} A \quad (3-3)$$

where the scenario, s_a encompasses the particular hazard and vulnerability (A). In most cases, the vulnerability of a system is evaluated based on value functions assigned to the constituent subsystems. Parameters of the value functions are often assigned by the elicitation of expert opinion and subjective probabilities. Opinions

are aggregated according to the relative importance of system components or disruption impact and assigned measures such as disutility for scenario-based disruptions (Ezell, 2005).

An alternative approach is the application of Monte Carlo simulation where scenarios are generated based on specific hazards and vulnerabilities in the system. Variates (i.e., random variables) from known probability distributions can be used in physically based or empirical models to assess consequences from each scenario. For this research, scenarios are based on the random, deliberate, or spatial selection and deletion of network infrastructure and consequences are measured in terms of connectivity loss through graph-theoretic measures (e.g. diameter) and spatial coverage. Results from each triple (Ω) can be used to rank events, compare the triple-generating structure (e.g., network) and estimate risk. The resulting vulnerability and sensitivity assessments are used in determining the derived vulnerability of the dependent sensor network topologies.

Derived vulnerability is a conditional quantity based on the vulnerability of the independent topology and can be written as:

$$\Omega_{D|I} = \{s_a, p(G_{Da} | G_{Ia}), w_{Ia} - w_{Da}\} A \quad (3-4)$$

where (G_{Da}) is the dependent topology subject to A , (G_{Ia}) is the independent topology subject to A , w_{Ia} is the consequence on the independent topology resulting from A and w_{Da} is the consequence of the dependent topology resulting from A .

A common scenario affects both the independent and dependent topologies. The likelihood of disruption to the dependent topology is conditional on that of the independent one, and the consequences are subtracted allowing for a relative separation of risk curves for the independent and dependent case.

3.1.4 Towards Dependent Topology Survivability

How can derived vulnerability be used to plan and deploy survivable topologies?

Given simulation analyses that can assess the sensitivity of the network to various forms of attack, derived vulnerability can be used to distribute sensor nodes around critical infrastructure and plan survivable topologies.

Sensitivity analysis is used to determine the rate of change of one factor in a model with respect to change in another factor. For example, given the system:

$$I \rightarrow h(p) \rightarrow \Phi \quad (3-5)$$

where $h(p)$ is a transfer function (e.g., an attack), p are the system parameters, and Φ is the output function (e.g., diameter); the parametric sensitivity of the system is:

$$\frac{\Delta\Phi}{\Delta p} = \frac{\Phi' - \Phi}{\Delta p} \quad (3-6)$$

which expresses the effect of change in p on Φ . Similarly, the component sensitivity measures the responsiveness of Φ to change in I :

$$\frac{\Delta\Phi}{\Delta I} = \frac{\Phi' - \Phi}{\Delta I} \quad (3-7)$$

The parameters are contributed by the topologic and spatial organization of both the dependent and independent topologies through, for example, the degree distribution of the topology. For random graphs, p is the mean degree \bar{k} , the parameter of the Exponential distribution, and for Power-law graphs, p is γ , the exponent of the Power-law. By fixing the parameters of the degree distribution, and performing many realizations of an attack scenario, the component sensitivity of the topology can be measured in terms of diameter $P(D > d)$ or fraction of nodes removed $P(F > f)$.

Consequences are measured on a combined relative scale for all network perturbation cases using the fraction of nodes removed, f (i.e., $[0,1]$), from total connectivity to total connectivity loss). Figure 3-2 is conceptual network decay curve used to show the variation in a dependent network parameter as a function of fraction of nodes removed from the network. Dependent parameters include graph-theoretic measures such as diameter or average shortest path, or spatial parameters such as coverage area. In attack simulations, the decay curve captures the fracturing of the largest connected components in the network and the *percolation threshold*, that point when connectivity is effectively lost and precipitous changes in dependent parameters occur.

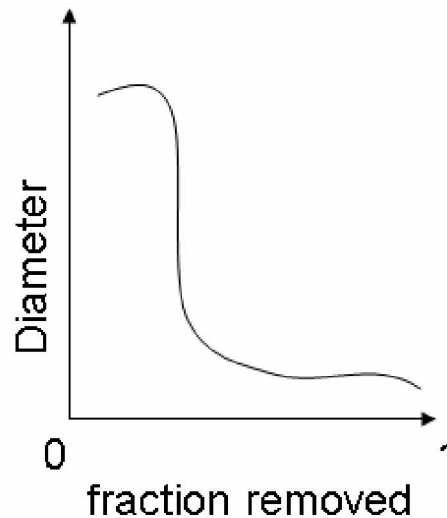


Figure 3-2: Conceptual network decay curve.

Although Figure 3-2 is conceptual, the slight increase in diameter as the decay moved from zero is deliberate. Decay curves are generated for the largest connected component in the graph. As the network breaks down during the course of an attack, the membership of the largest component changes and so do the graph-theoretic properties of that component. In this case, a connected component with higher diameter emerges after the initial largest component is destroyed.

If taken in cumulative form, the decay curve can yield the peak consequence (parameter change) and corresponding node fraction. Realizations of the percolation fraction (i.e. the critical fraction at which percolation occurs), across all topology generating processes and all modes of attack, are used to generate the dependent and independent risk curves or CCDFs.

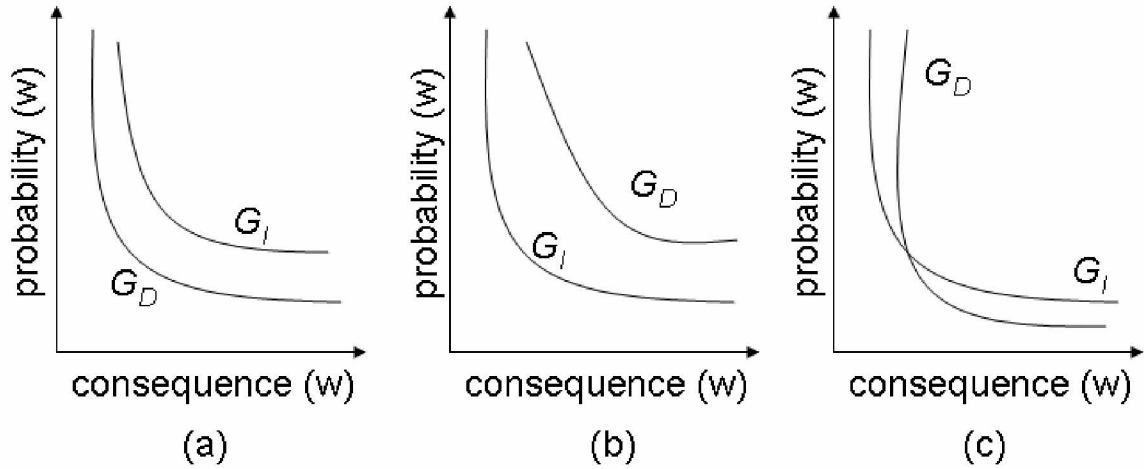


Figure 3-3: Conceptual risk curves based on derived vulnerability.

It was discussed previously how risk curves could be used to measure the uncertainty associated with a given consequence or be used to classify the risk associated with a particular system. Figure 3-3 shows how the risk associated with the dependent topology can be dominated by the risk of the independent topology. Based on the notation in Equation (3-3), w represents a measure of consequence (e.g., fraction of nodes removed due to network perturbation), and $p(w)$ is the cumulative exceedance probability of that consequence. In Figure 3-3(a), the aggregate (i.e., mean) risk curves are generated for the independent topology, G_I and the dependent topology, G_D . In this case, the independent risk curve dominates the dependent curve. That is, the relative consequence of connectivity loss and likelihood of occurrence will for all cases exceed that of the dependent network. In Figure 3-3(b), the dependent risk curve, G_D dominates the independent curve, G_I . In Figure 3-3(c), the dependent risk curve is *non-dominating* (i.e., the mean risk curves are overlapping and indeterminate).

By simulating various attack scenarios and measuring effects (e.g., d, \bar{l}, f) we can generate dependent and independent CCDFs based on the critical values extracted from the network decay curves. The cases in which the dependent topology is dominated represent instances where active topology control and self-organization behavior must be deployed in order to sustain the dependent sensor network.

3.2 Approach

The following sections describe the techniques used to generate topologies, verify the structure and behavior of instances of those topologies, graph statistics, and GIS integration for spatial analysis. The overall approach for the analyses in this chapter is shown in Figure 3-4:

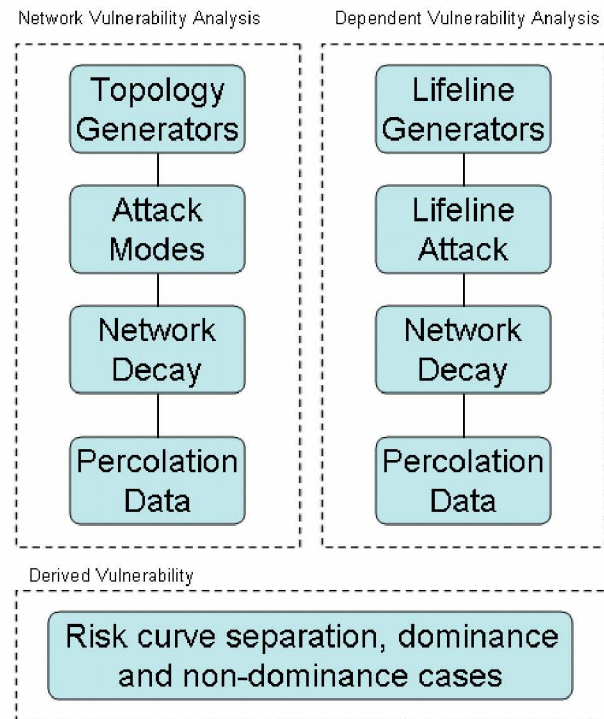


Figure 3-4: Overview of analysis procedure.

The analysis is separated into two parts. The network vulnerability analysis includes topology generation, random and targeted modes of attack, and sensitivity of results leading to decay curves and critical threshold data. The dependent vulnerability analysis looks specifically at the lifeline (i.e., dependent) case for topology generation, attack, and simulated results. Finally, the results of both the dependent and independent analyses are used to generate risk curves and classify the dominance

and non-dominance cases. The approach is centered on simulated topology generation and attack for performing sensitivity analysis. Percolation data for the independent and dependent cases is collected and used to generate, and then compare risk curves.

The following steps describe the analysis process in more detail:

- **Step 1: Topology Generation.** Because actual deployments of wireless sensor networks of the nature envisioned in this research do not exist at present, a series of topology generators were developed to reproduce known degree distributions (e.g., random-uniform, Exponential, and Power) for the non-spatial case. For the spatial case, both independent and dependent spatial topology generators were developed that use a proximity-based (i.e., nearest-neighbor) attachment scheme.
- **Step 2: Validation and Verification.** The performance of the topology generators and their ability to re-create distributions of known types was evaluated and the variability in the simulations performed was examined.
- **Step 3: Network Sensitivity Analysis.** Network attack modes including random, targeted, spatial, and lifeline are subjected to the dependent and independent topologies.
- **Step 4: Derived Vulnerability.** Variation in percolation behavior for independent and dependent topologies were compared to establish risk dominance relationships/

3.3 Topology Generation

The body of literature on empirical analysis of large graphs such as the Internet and WWW also includes work on techniques for synthetic topology generation.

Topologies must be generated because, unlike variates from a known probability distribution which can be assigned based on parameters of that distribution, graphs lack a characteristic population that can be sampled across scales. Whereas exponential and scale-free degree distributions have been fit to actual data, research in topology generators has developed techniques for reproducing these distributions, as well as other graph theoretic statistics, in generated graphs. In general, topologies are generated for N nodes by either random placement of edges or through network evolution (i.e., growth) where at each time step, nodes and edges are added to the graph by a defined random process. Bu and Towsley (2002) and Li, Alderson et al. (2004) provide surveys of topology generators used for simulating Internet graphs. The following sections present the primary topology generators and their use in this research.

3.3.1 Random Network Generator

The random network generator creates an undirected graph with N nodes and E edges. Edges are attached to nodes with equal (i.e., uniform) probability such that most nodes have approximately the same number of links, corresponding to an E-R graph structure and a Poisson degree distribution (see Figure 2-4 for a summary of the prototypical graph degree distributions).

3.3.2 Exponential Network Generator

The Exponential network generator operates by successively adding new nodes and new edges at each time step through a network growth process. One new node and one new edge are added for each time increment. The probability of a node attracting an edge is proportional to the age of that node (i.e., the oldest nodes accumulate a higher number of links). The resulting degree distribution for graphs produced by this generator follow an Exponential form. As with the random network generator, the Exponential topologies are undirected.

3.3.3 Power-law Generator

The power-law generator is based on the Barabási-Albert (BA) (1999) linear preferential attachment scheme. The model begins with a small connected component as a substrate or kernel with $N = 5$. New nodes and edges are added incrementally at each time step of the growth process. Unlike the Exponential generator however, new nodes follow a linear preferential attachment process. Recalling Equation (2-6), the probability of a node gaining an edge is:

$$P(k) = k_i / \sum_j k_j \quad (3-8)$$

where k_i is the degree of the current, or new node and k_j is the degree of any existing or previous node in the network. The resulting degree distribution of the generated undirected topology has a Power-law form.

A variation of this generator called PLRG (Power Law Random Graph) takes as parameters N and γ . Rather than beginning from a kernel, PRLG assigns degrees to N

nodes drawn from a Power-law distribution with exponent γ then connects nodes with matching degree. The performance of these and other power-law topology generators has been shown to be similar, so the BA model was used for these analyses.

3.3.4 Proximal topology generator

A new topology generator was created based on the spatial proximity of nodes during network growth. As implemented, the previous generators allow spatial coordinates to be assigned to each node. However, the spatial placement of the nodes plays no role in the formation of the topology. The Proximal topology generator operates specifically on the assigned location of nodes.

The graph is initially seeded with a root node and assigned a random location (i.e., equally likely position within a random field). At each time step, a new node is added to the graph and a new, undirected edge is added based on minimum Euclidean distance to existing nodes in the graph. The resulting degree distribution of the generated topology has a Power-law form, as will be shown in the following sections.

3.3.5 Other generators

Bu and Towsley (2002) present various other generators focused on the degree to which they reproduce Internet topology, specifically the organization of the AS (Autonomous System) routers that comprise the backbone of the Internet. These generators are frequently evaluated on their ability to replicate Internet topologies at local and global network scaled. Of interest are “re-wiring” generators that allow edges to move to new vertex pairs during the course of the network evolution. A

selection of these generators will be discussed in Chapter 4 in the context of topology control mechanisms.

3.3.6 Implementation

Each of the generators above was implemented in the Python programming language (Python 2005) based on the PyGraphLib graph representation library (Albert 2005). The PyGraphLib library was chosen for its high level abstraction of graph structures and algorithms. Graphs can be created and manipulated using concise script commands rather than low-level, array-based data structures. The Python programming language also provides seamless integration with the ESRI Geoprocessing framework (ESRI 2005) through which the spatial properties of generated graphs were analyzed.

In the Python language, the basic `random()` function generates a random float uniformly in the semi-open range $[0.0, 1.0)$ based on the Mersenne Twister core generator. Although based on some deterministic elements and therefore formally *pseudorandom*, the generator produces 53-bit precision floats and has a period of $2^{19937-1}$ indicating very high performance as a random number generator (Matsumoto, 1997). Edge and node attachment, spatial placement, attack modes, and statistical parameter verification were all performed using the Python `random()` utility.

3.4 Verification of Topologic Statistics

Before performing simulation analysis on the sensitivity of the generated topologies to disruption, it was desired to verify the extent to which the generators were capable of reproducing the normative graph structures and the variability of graph theoretic and spatial statistics across simulations under the no damage condition.

Graph-theoretic statistics were measured including diameter and average shortest path \bar{l} . \bar{l} is also written as $\langle l \rangle$ in the following sections.

3.4.1 Verification of Topology Generators

Simulations were performed to verify the topologies generated. The resulting degree distributions from typical topologies were compared with the intended forms. For the random topology generator, the verification of the topology seems straightforward. For the Exponential, Power-law, and Proximal generators, however, the behavior of the governing random processes is less obvious. Note that in the spatial case, no degree distribution was planned beforehand, only the spatial distribution of nodes.

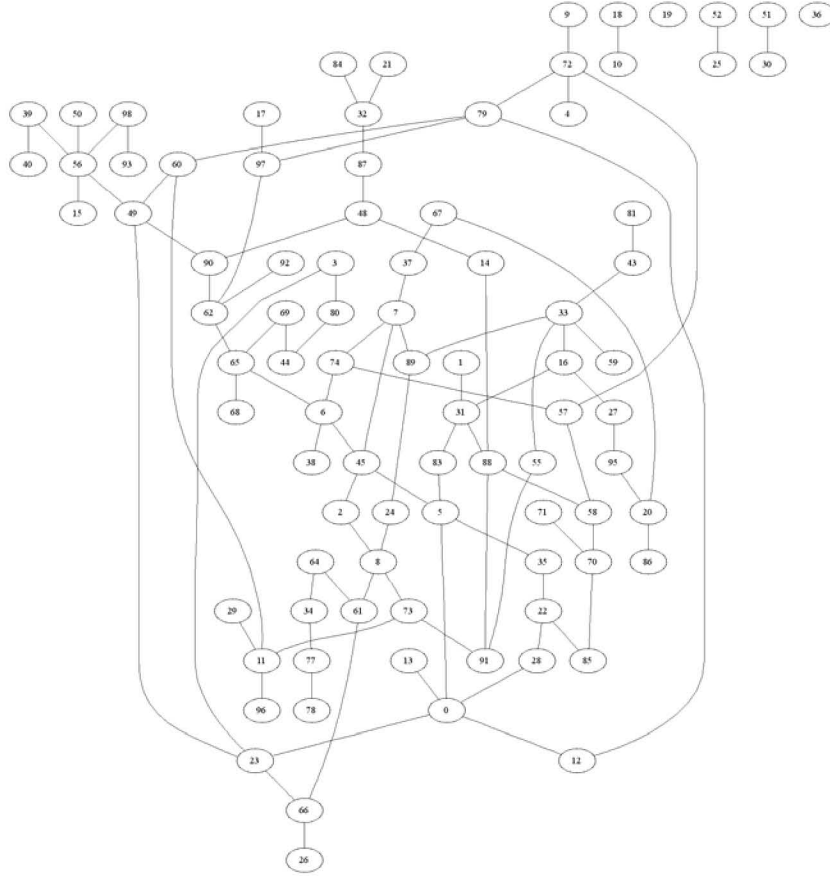


Figure 3-5: Typical generated random topology ($N=100$, $E=100$).

Figure 3-5 shows a typical 100 node undirected topology created by the random topology generator. The maximum, minimum, and mean degrees are 5, 0, and 2.0, respectively. Note that unconnected clusters are also present. Using the PyGraphlib framework (Albert 2005), random topologies were generated up to $N = 10,000$. Because this generator uses no random process to attach nodes (e.g., preferential attachment in discrete time), high order graphs were not a computational burden. Figure 3-6 shows the associated degree distribution in the form of a discrete histogram, which is Poisson distributed.

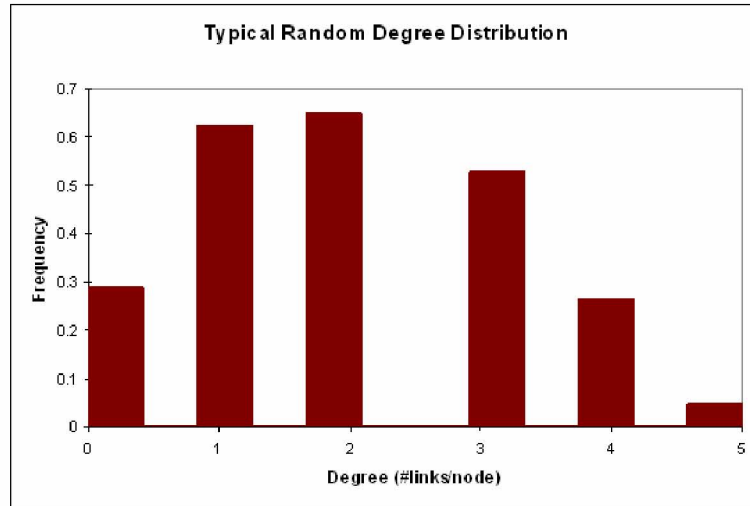


Figure 3-6: Degree distribution of random (ER) Topology.

Figure 3-7 shows a typical 100 node undirected topology from the Exponential Network Generator. The figure typifies the hierarchical, tree-structure of exponential graphs.

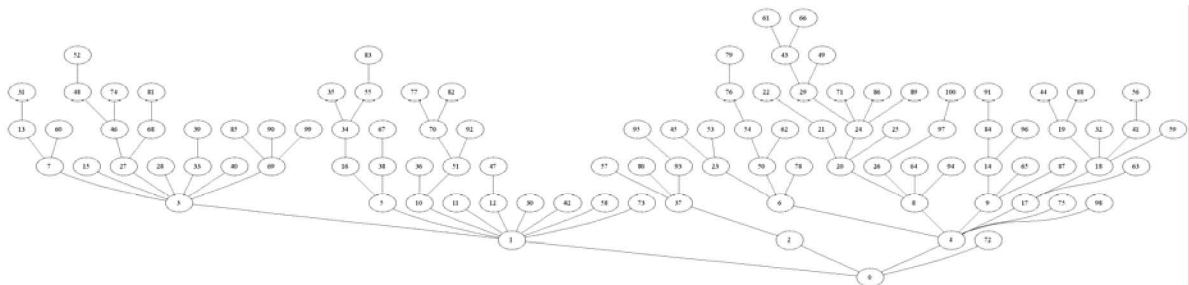


Figure 3-7: Typical Exponential topology ($N = 100$, $E = 100$).

The oldest nodes, those with the lowest numbered label, are located near the bottom, or root of the tree. These nodes also have the highest degree. The maximum, minimum, and mean degrees are 7, 1, and 2.0, respectively. Unconnected clusters are not possible with this generator as a new node must attach to the existing graph as

each successive node and edge is added. Figure 3-8 is a degree distribution of the typical Exponential topology.

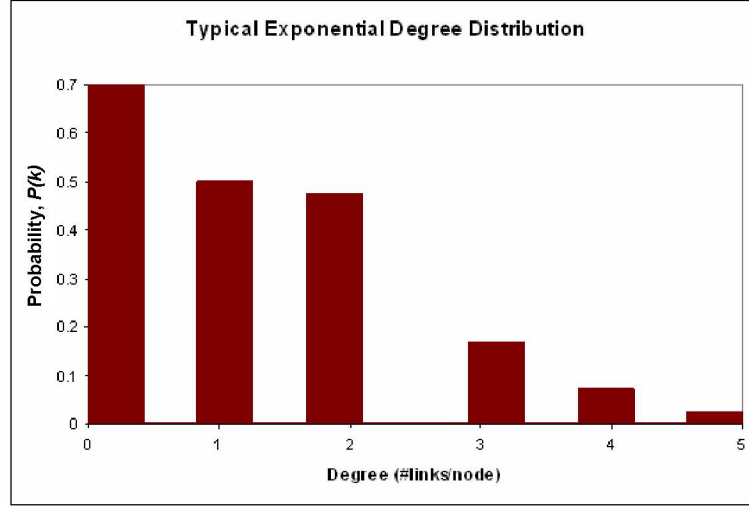


Figure 3-8: Typical Exponential Degree Distribution.

Figure 3-9 shows a typical undirected topology created by the BA Power-law topology generator.

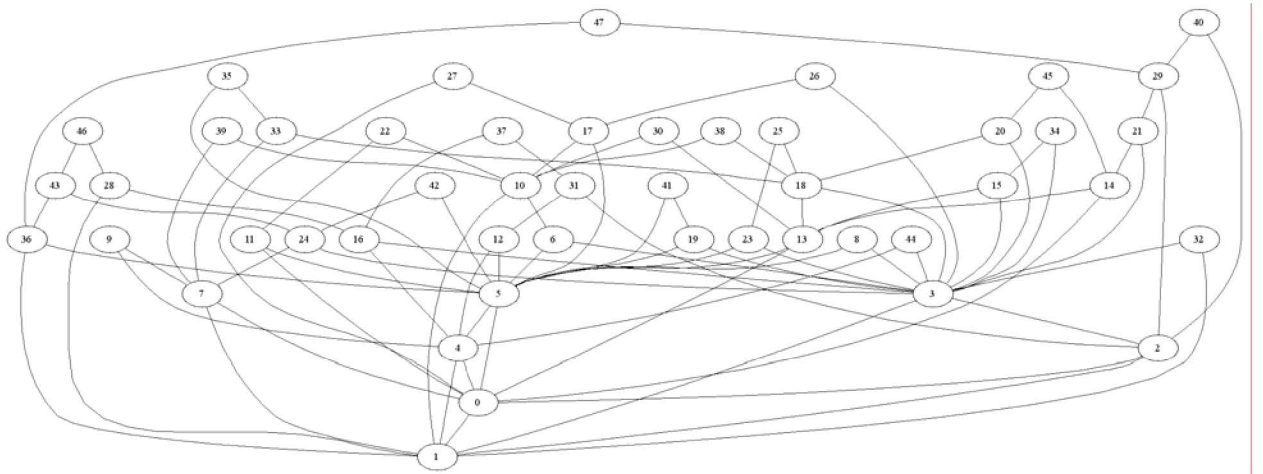


Figure 3-9: Typical topology from BA topology generator ($N=50$, $E=93$).

Unlike in a topology created by the Exponential Generator, the oldest node (i.e, Node 0) does not have the highest degree, but rather Node 3. This confirms the intended preferential attachment behavior of the BA generator. Because the attachment scheme is stochastic, an older node, but not necessarily the oldest node will have the highest degree for a given evolution simulation. The maximum, minimum, and mean degrees for this example are 5, 41, and 9.7, respectively. The distribution corresponds to a Power-law fit with $\gamma = 2.04$.

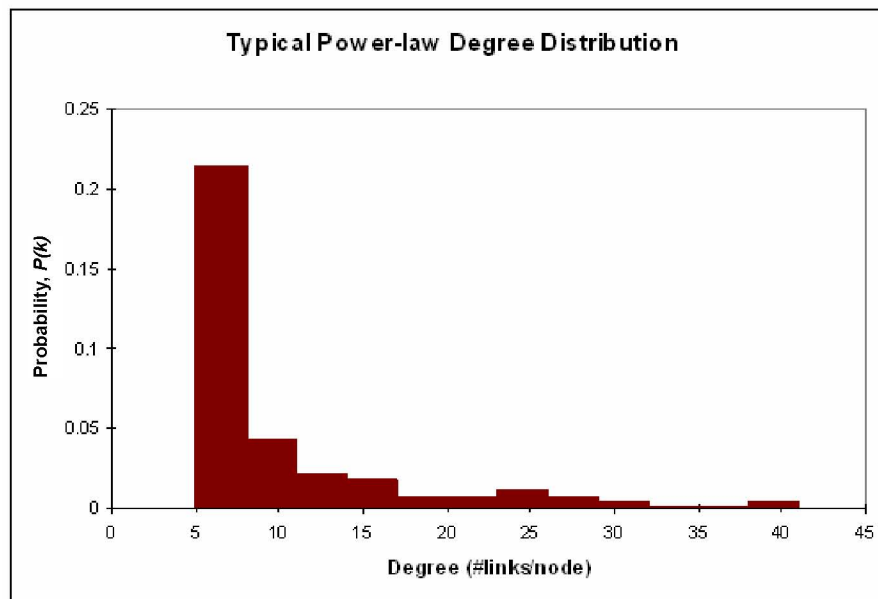


Figure 3-10: Typical Scale-free (Power-law) degree distribution.

It is important to note that the graphs produced by these generators have no inherent spatial organization. The geometric layouts of the graphs shown in Figure 3-5, Figure 3-7, and Figure 3-9 are arbitrary.

The performance of the proximal topology generator was also evaluated. Figure 3-11 shows a typical undirected topology produced by the proximal generator. As previously mentioned, no degree distribution was assumed *a priori* for this generator.

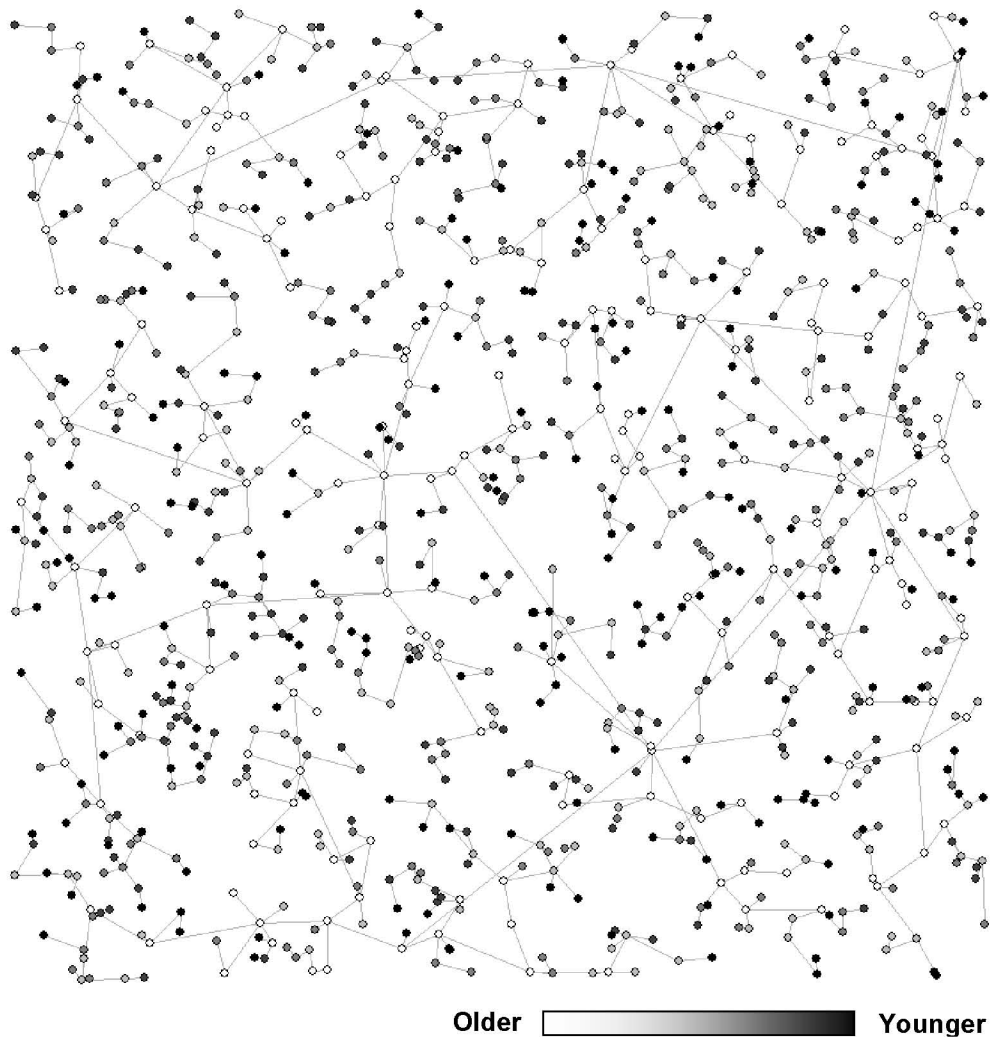


Figure 3-11: Typical spatial organization from proximal topology generator ($N=1000$).

Unlike the previous graphs, Figure 3-11 shows a spatial layout of the graph where the topologic (i.e. logical) connections between nodes also occur in geographic space. The oldest nodes in the graph are shown colored white and the newest nodes are black. As the random field becomes denser when newer nodes are added, the nearest-neighbor attachment scheme leads to local connections that are much closer to one another. Although not colored, the oldest edges in the graph, which connect the oldest nodes, are also the longest. These long-range connections are discussed below as a contributing factor to the attack survivability of proximal topologies.

The degree distribution associated with this topology is shown in Figure 3-12. The maximum, minimum, and mean degrees are 10, 1, and 2.0, respectively. The smaller maximum degree compared to the BA-generated topology is surprising, as is the smaller \bar{k} . A Power-law was fit to the degree distribution of these data with an exponent of $\gamma = 1.93$. Apparently the explicit consideration of spatial organization plays a role in the formation of the topology. The characteristic range of the Power-law form (i.e., $2 < \gamma < 3$) implies Power-law efficiency in terms of low node separation distance (efficiency) and susceptibility to targeted attack (vulnerability). The degree distribution resulting from the proximal generator suggests slightly less efficiency, but perhaps greater survivability as well. The diversity of long and short distance edges is hypothesized as an explanation for this behavior. This hypothesis is tested in the context of the spatial and lifeline attack modes in subsequent sections.

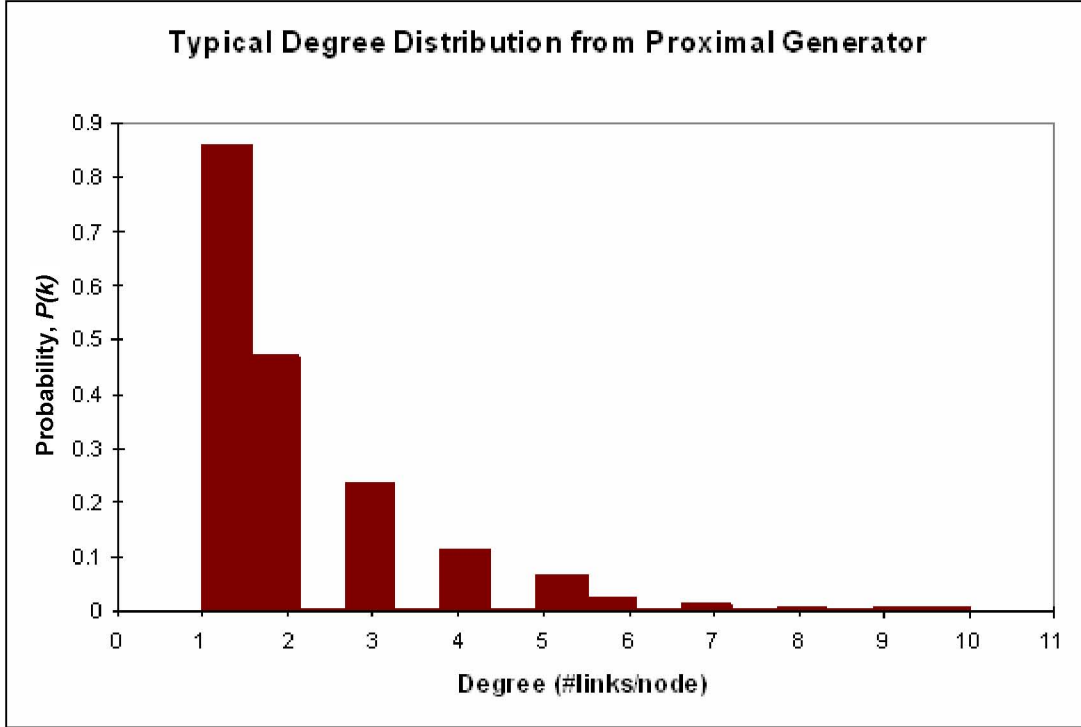


Figure 3-12: Typical Degree distribution from proximal topology generator ($N=1000$) with 1000 x 1000 random field.

3.4.2 Variance in Graph-theoretic statistics

Each of the topology generators were evaluated for their performance under the unperturbed (i.e., no-damage case). In other words, multiple topologies for a fixed N were generated and graph statistics were measured for each realization. The goal was to assess the variance in the topology generators.

Simulations were performed on random graph topologies with $N = 100$ to assess the variation of \bar{l} for 100 realizations. For a random graph topology, \bar{l} was equal to 4.0 in over 80% of cases and 5.0 in the remaining cases, yielding a distinct, discrete pdf. Similar simulations were performed for the unperturbed case for the Exponential, Power, and Proximal topology generators. For these cases, Normal variation was observed for simulated values of diameter and average shortest path. Because the

other generators produced Normal results, the discrete pdf of the random case was surprising. It was hypothesized that because this generator takes as parameters the number of edges and nodes, rather than seeded number of nodes, the ratio of parameters may contribute to graph statistic variation with respect to N .

Three experiments were conducted to evaluate whether the ratio of nodes to edges, R_{NE} , in the random graph generator produced parameter-dependent variance. For, $R_{NE} = 1$, in this case $N = E = 100$ and then, $E = 4N$, and, $E = 10N$, the diameter for each realization of the undirected topology was measured. Figure 3-13 summarizes the results.

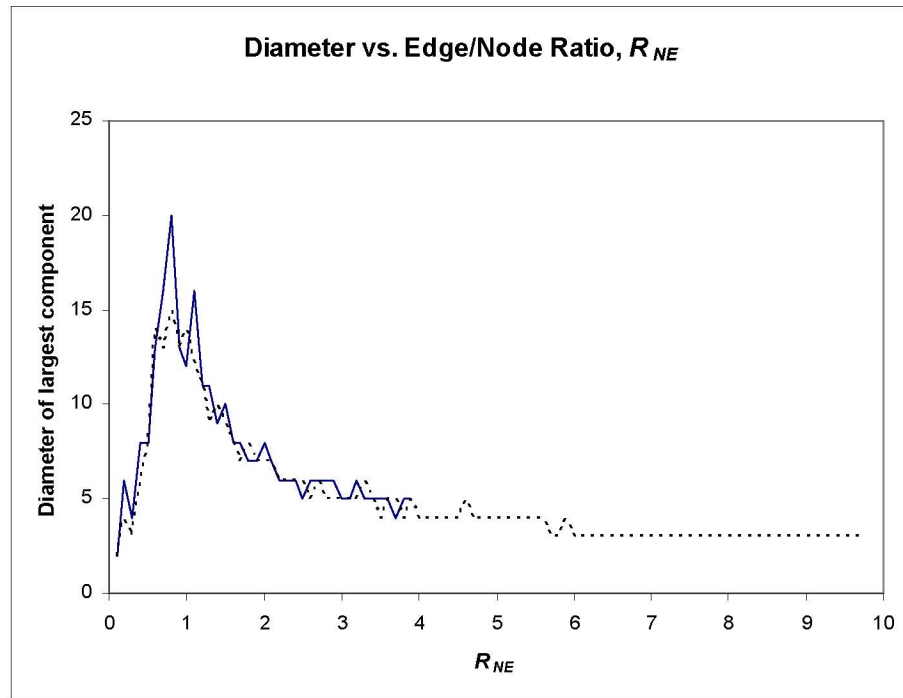


Figure 3-13: Variation of diameter in largest component for edge/node ratio.

Diameter is measured for the largest connected component for each graph. Beginning with 100 nodes and 10 edges and incrementing the number of edges while holding N

constant, we see the diameter of the component increases almost linearly with size until the ratio reaches 1.0. At the point where there are twice as many edges as there are nodes in the random graph, the diameter stabilizes. Additional simulations with the edge/vertex ratio approaching 10 showed no further variation in diameter (i.e., stabilization was persistent). At this convergence point the, graph is “saturated” with edges and the size of the largest connected component is approximately N .

Because of similar performance for other combinations values of R_{NE} , it was concluded that the random generator does produce consistent results and is not subject to parameter-dependent variance.

3.5 Network Vulnerability Analysis

This section presents the results from a series of analyses performed to examine the sensitivity of networks to simulated topologic and spatial perturbations. A perturbation is typically defined as a small change or agitation in a physical system. In this context, a perturbation is more precisely an attack or disruption caused by the loss of connectivity in part of the network. Attacks are based either on topological criteria (e.g., the connective properties of nodes and edges) or on spatial criteria (e.g., the placement of nodes within a synthetic or geographic space). Three attack modes were employed; random, targeted based on topologic connectivity, or targeted based on spatial proximity. For random attacks, it was expected that the results would verify previous research (Albert et al. 2000) in demonstrating increasing resistance to partition (i.e., the fracturing of the network into disconnected clusters) as one moves from random, to Exponential, to Power-law topologies. This resistance should diminish drastically, however, given targeted attacks based on topologic criteria. Resistance to spatial attack has not been extensively studied and so expands in the treatment of the spatial properties of networks and the interdependency of spatial and topologic behavior in response to disruption.

3.5.1 Sensitivity of networks to random failure or attack

Random failure in a network is defined as the random selection and deletion of a node and any edges attached to it. Each node has an equal chance of being selected and therefore deleted. Graph topologies were created using the Random, Exponential, Power-law, and Proximal generators for various sizes and their response to random failure was measured.

Figure 3-14 shows the results of simulations of random failure based on random topologies. The average shortest path, $\bar{l} (\langle l \rangle)$ on the vertical axis was measured for the graph as the fraction of nodes removed (horizontal axis) increased. Attack simulations were performed for random networks with 50, 100, 200, and 300 nodes.

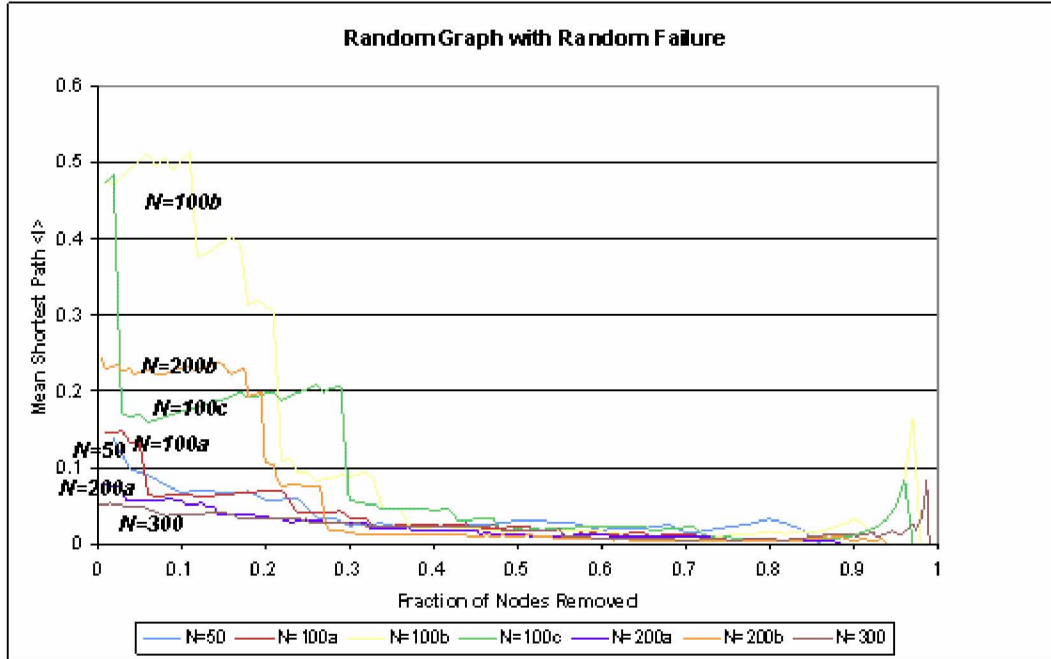


Figure 3-14: Simulation results from random attack on random topologies.

In all cases, percolation (i.e., abrupt loss of connection efficiency) occurs at approximately 25% of the nodes removed. Although a clear discontinuity is visible for each case indicating a percolation threshold (fraction removed), that also corresponds with an approximately 50% drop in the unperturbed magnitude of \bar{l} for each case. In subsequent analyses where the network decay curves are more gradual and lacking a discernable discontinuity, the node fraction after which a 50% reduction in \bar{l} occurs is taken to be the percolation threshold. The decay behavior does not

appear sensitive to network size (N) and the sudden increases in \bar{L} near total removal of nodes are considered anomalous.

\bar{L} is a measure of the efficiency of the connections in the graph. As the graph begins to fracture (i.e., become disconnected) when nodes are removed, the efficiency of the remaining connections changes. As was discussed with Equation (2-16), \bar{L} is calculated for the largest connected component, which can change as nodes are removed from the graph. This explains why the magnitudes of \bar{L} decrease as the decay curves progress from the unperturbed state to total node removal. Note that \bar{L} measured for a disconnected network is undefined.

Figure 3-15 shows the variation of network diameter, d , for the same simulations and range of N . Cases labeled with the suffix a or b represent separate realizations of that simulation of N (i.e., separate randomly generated topologies). Although the magnitudes of \bar{L} and d differ as a function of N , the sensitivity of \bar{L} to node/edge deletion was similar. Computationally, \bar{L} was very similar to d as both use Dijkstra's shortest path algorithm operating on either path distance (i.e., number of edge hops separating two nodes) or Euclidean distance. Many other shortest path algorithms are available, but Dijkstra was selected for its straightforward implementation in the Python programming language. For \bar{L} , the Dijkstra shortest path is computed and averaged for all sets of nodes and for d , the longest path between pairs of nodes is calculated. Because their sensitivity to random and targeted attack were similar, and their computational complexity are equal, \bar{L} was most often used in the subsequent analyses.

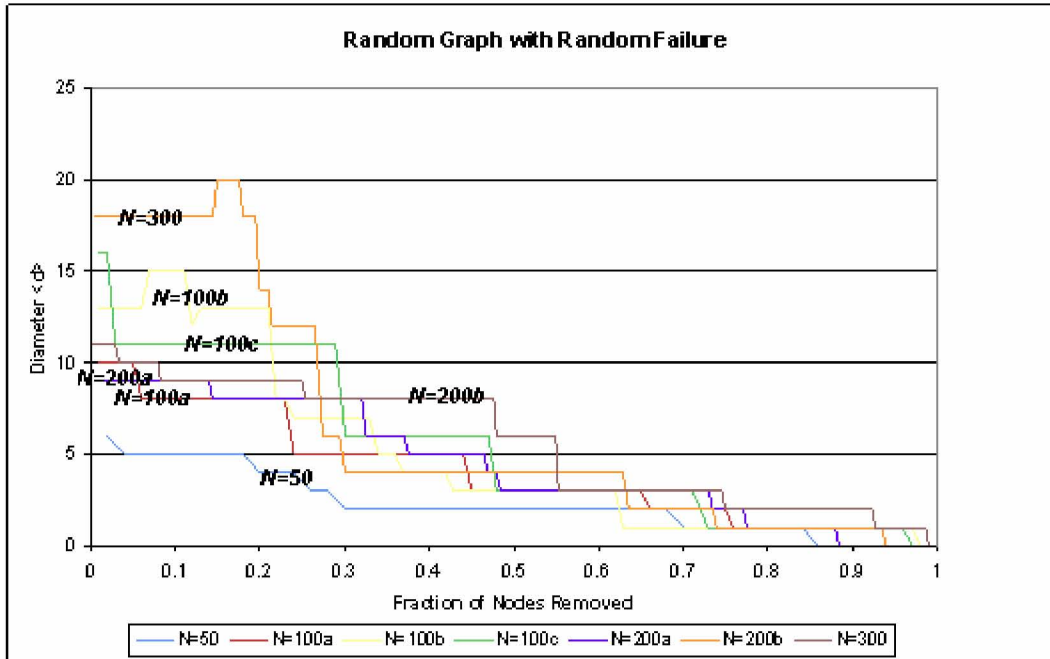


Figure 3-15: Diameter network decay (random attack on random topology).

At approximately 30% of the nodes removed, both \bar{T} and d decrease by 50% or more representing loss of connectivity. This point corresponds to the percolation threshold for the graph as it represents the largest percentage drop in diameter. As stated previously, as the fraction of nodes removed increases, the largest component for which diameter is measured, changes (i.e. the set of nodes comprising the largest component) until total fracture occurs). Similar to \bar{T} measured for a disconnected graph, if diameter were measured across all nodes in the graph irrespective of connectivity, the diameter could be said to be infinite, or undefined.

Figure 3-16 shows the results of simulations of random failure with an Exponential topology. Attack simulations were performed on Exponential topologies of $N = 50$, 100, and 200. Again accepting differences in magnitude for \bar{T} as a function of N , the overall (i.e., mean) effect is a 50% decrease in \bar{T} at 70% of the nodes removed

compared with the undamaged case. This is a substantial increase in resistance over the random topologies. Unusual behavior was observed for the $N = 50$ case where \bar{l} increased substantially at over 70% nodes removed. This is an artifact of the fracture process for small N and as with the random topology case, is considered anomalous.

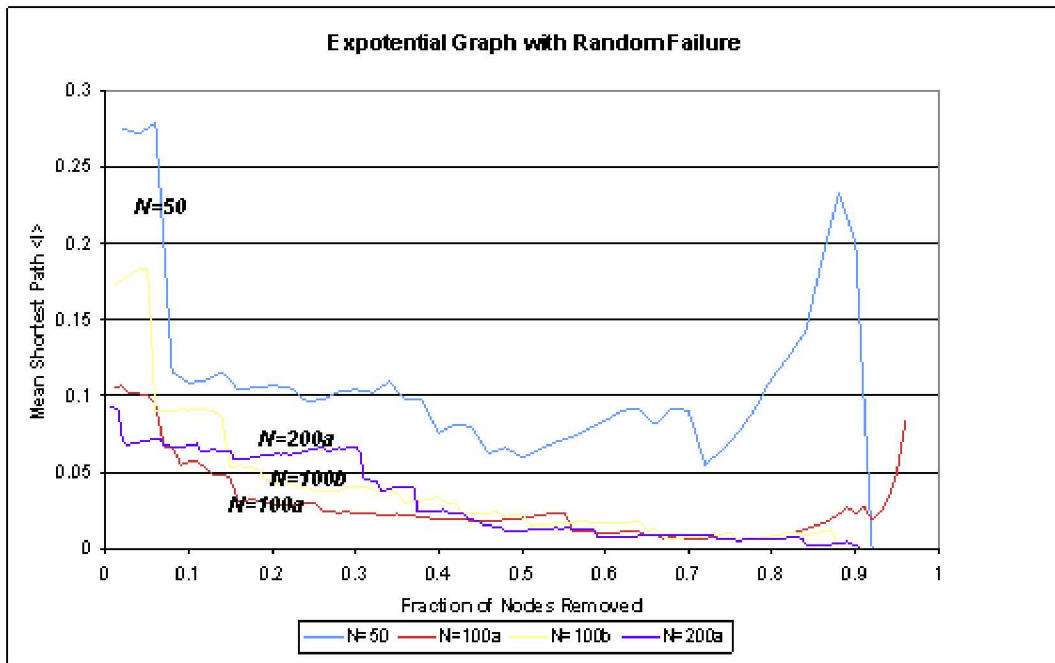


Figure 3-16: Simulation results from random attack on Exponential topologies.

Figure 3-17 shows the results of scale-free (Power-law) topologies subject to random failure. Attack simulations were performed on Power-law topologies of $N = 50, 100$, and 200. Compared with the undamaged case, these topologies show great resistance to failure, exhibiting only a 50% loss in connection efficiency (\bar{l}) at 80% of the nodes removed. This result corresponds well with results obtained by (Albert et al. 2000) and others. The percolation threshold for these graphs is near 90%.

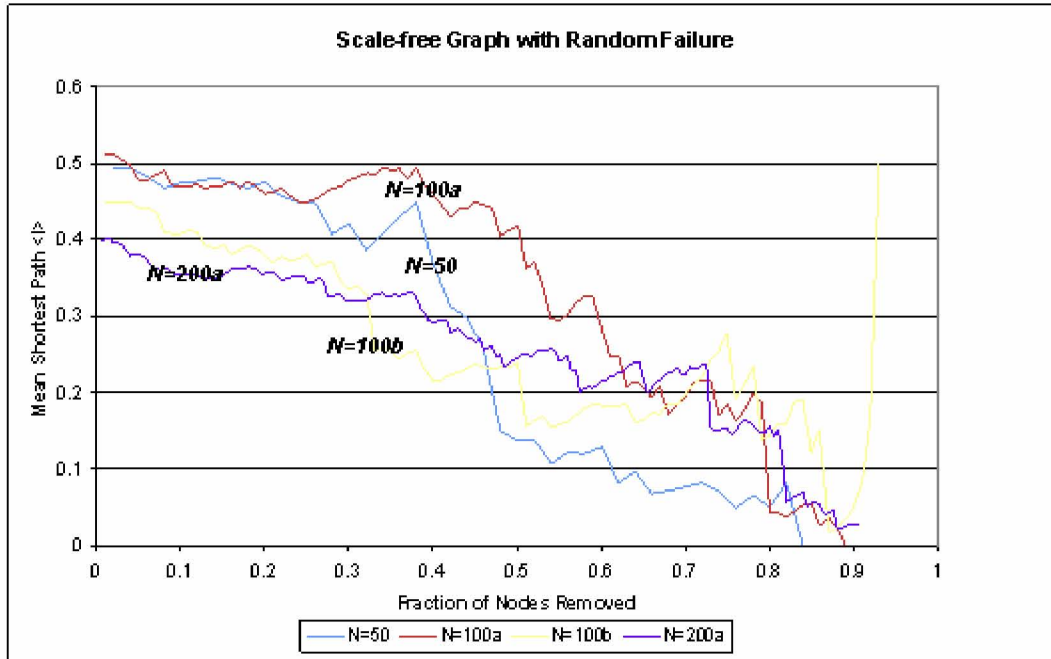


Figure 3-17: Simulation results from random attack on Power-law topologies.

Computational complexity was an issue in calculating graph statistics on Power-law topologies. Algorithms to compute \bar{l} typically operate in $O(N^2)$ time similar to Dijkstra's shortest path algorithm. For sparse graphs (i.e., graphs with much less than N^2 edges such as from the random topology generator), performance slightly better than $O(N^2)$ can be achieved through the use of more efficient data structures such as adjacency lists. However, for dense graphs such as those created by the Power-law generator, the performance can be much worse. Because Power-law topologies remain connected for so long during a random attack, the size of the largest component remains approximately constant until a very large fraction of nodes are removed. Whereas attack simulations on random graphs seem to accelerate as the graph becomes increasingly fractured, the average shortest path calculation times on a Power-law topology remain constant for each damage increment resulting in no

speed-up as the network becomes more damaged. The net effect was significant computational time requirements for random attack simulations of large Power-law graphs. Attack simulations on $N = 200$ networks exceeded 3 hours on a Pentium IV PC with 1.7 Ghz processor with 512 MB RAM. Interestingly, the same simulation was also run on a Pentium IV PC with 4.0 Ghz processor and 4 GB RAM and still required 2.5 hours to complete.

3.5.2 Sensitivity of networks to targeted failure or attack

Targeted failure (or attack) is defined as the systematic selection and deletion of specific nodes in the network and any edges attached to those nodes. Nodes are selected according to a nodal hierarchy where nodes are ranked in order of decreasing degree. For these simulations, the top 1% of nodes (ordered by decreasing degree) were simultaneously removed followed in 1% increments until all nodes had been removed.

Figure 3-18 shows the variation in average shortest path in random topologies subjected to targeted attack of the most connected (highest degree) nodes. Resistance to targeted failure is slightly lower than for random attacks. Loss in connection efficiency is exhibited by decreases of 50% in \bar{l} after 30% of nodes are removed, however, complete loss of connectivity occurs at $f = 0.72$. Although hubs are not present in Random topologies, the targeting of slightly higher degree nodes had a greater effect on loss of connectivity for random topologies.

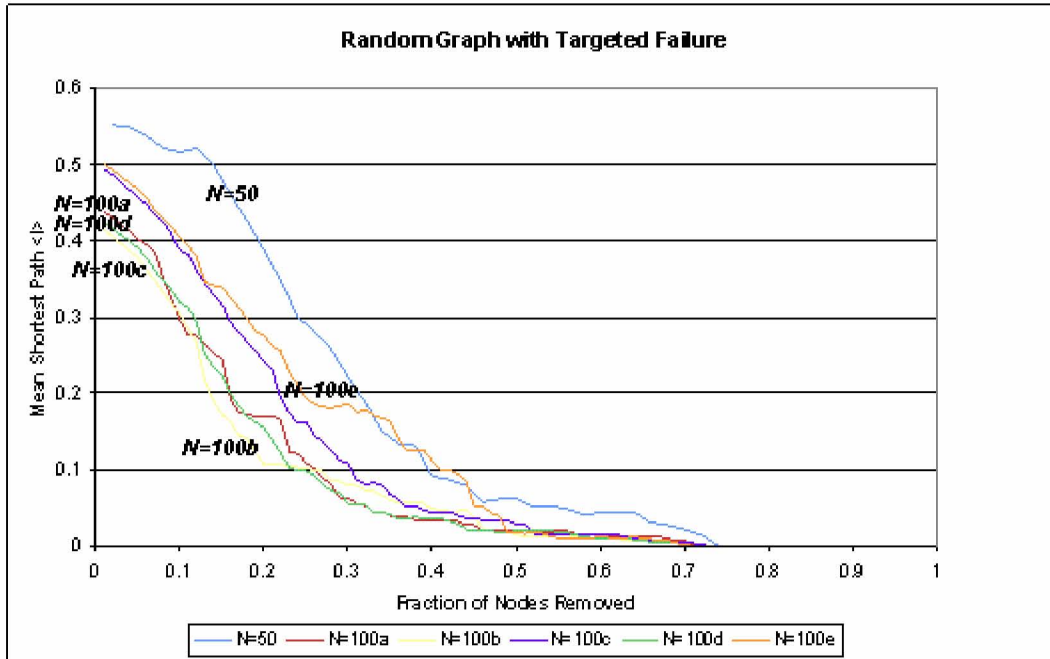


Figure 3-18: Simulation results of Targeted attack on Random topologies.

Figure 3-19 shows the results of targeted attack simulations performed on Exponential topologies. A lower resistance to failure is shown with 50% decrease in \bar{L} after 5% of the nodes are removed. It is interesting to note that with the increased susceptibility to failure, the magnitudes of \bar{L} are smaller when compared to random topologies in Figure 3-18. This indicates that the Exponential topology is more efficient. That is, even though the network has approximately the same number of nodes and edges, the shortest distance between nodes in the largest connected component are, on average, smaller.

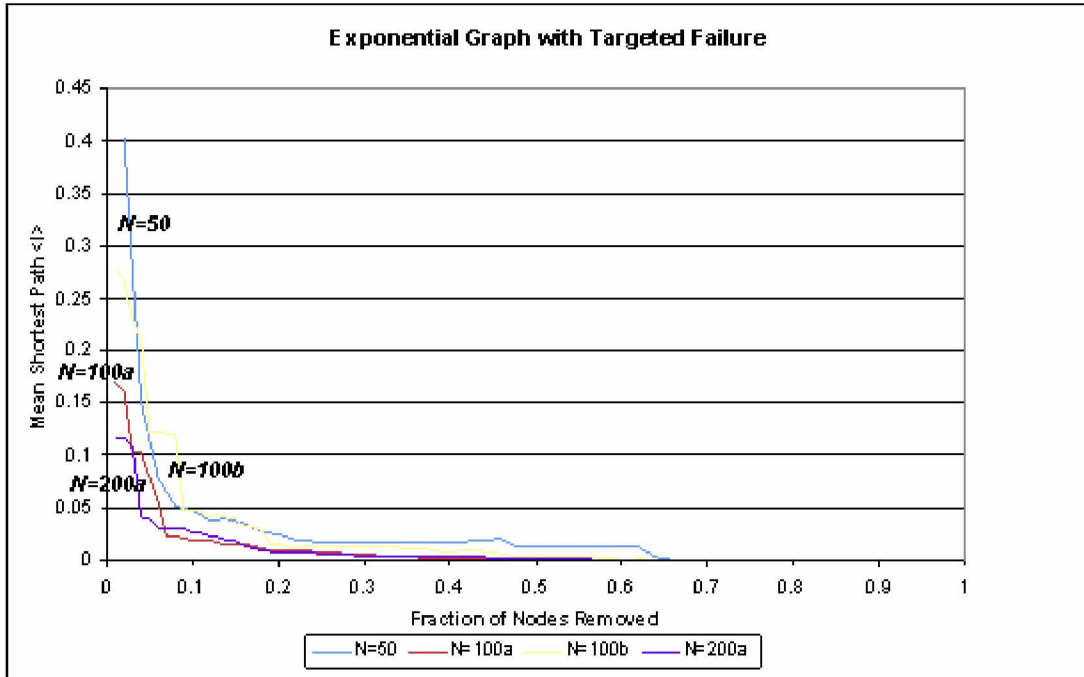


Figure 3-19: Simulation results of Targeted attack on Exponential topologies.

Figure 3-20 shows the results of targeted attack simulations performed on Power-law topologies. Here, the appreciable loss of connectivity occurs even sooner than in the Exponential case, at about 1% of the nodes removed. At $N = 100$, this means that simply removing the most connected hub destroys the connectivity and efficiency of the topologic structure. As seen in the move from Random to Exponential topology, the magnitudes of \bar{l} are still smaller indicating that the Power-law topologies are even more efficient when connectivity is maintained.

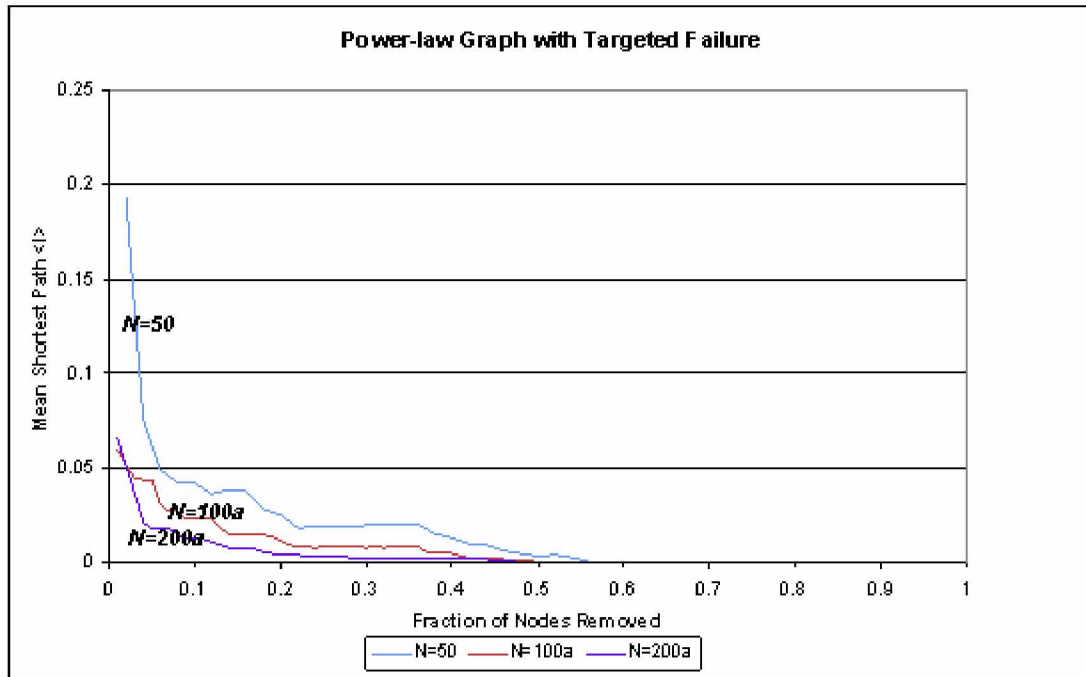


Figure 3-20: Simulation results of Targeted attack on Power-law topologies.

These results verify the work of others in demonstrating the efficiency of Exponential and Power-law topologies, their relative resistance to random failure, and susceptibility, especially Power-law, to targeted attack.

3.5.3 Sensitivity of networks to spatial attack

Spatial failure (or attack) is defined as the systematic selection and deletion of specific nodes in the network based on their spatial or geographic location. An attack location point is chosen at random from which a radial buffer is extended in equal outward increments. As shown in Figure 3-21, nodes that intersect the concentric rings of the buffer are simultaneously deleted until all the nodes in the field have been removed. At each increment of nodes removed, the average shortest path in the remaining largest connected component is measured.

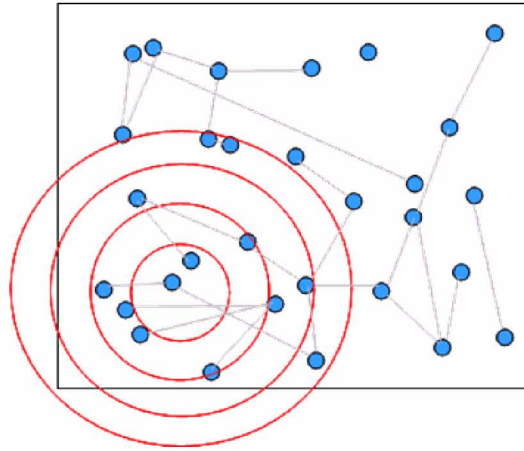


Figure 3-21: Conceptual spatial network topology subject to spatial attack.

The spatial attack case assumes that the attack location and spatial distribution of the nodes are uniform. That is, although the topologies may be Random, Exponential, or Power-law, the placement of the nodes in space is strictly random as is the selection of an attack point. Figure 3-22 shows the results of spatial attack simulations on random graph topologies.

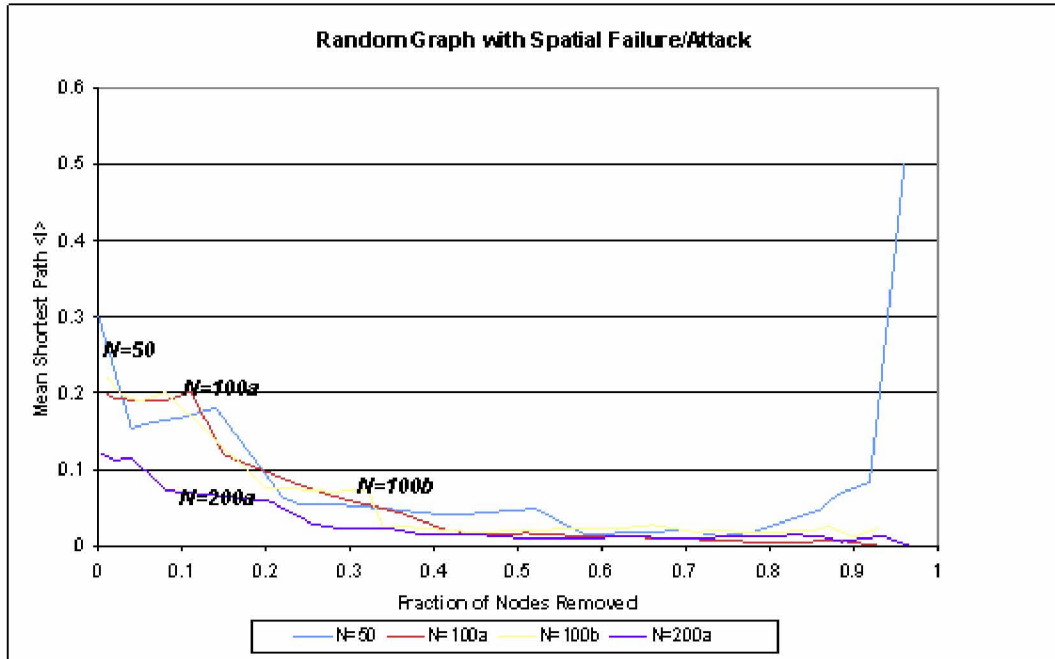


Figure 3-22: Simulation results for Spatial Attack on Random topologies.

Compared with Figure 3-14, the random attack on Random topology case, the decay curve in Figure 3-22 is more gradual and lacking an abrupt percolation threshold for the cases studied. The magnitudes of \bar{l} are similar to the random topology with random attack case, however. The small- N effects for the $N = 50$ case show a marked increase in \bar{l} at the point of total fracture, but, again, this is considered anomalous.

Figure 3-23 shows the results of spatial attack on Exponential topologies. Again, a more gradual decay is observed compared to the random attack on an Exponential topology case. Like the Exponential topology however, an increased resistance with percolation occurring near 40% of nodes removed is observed. The probability of the outwardly increasing area for each concentric ring of the spatial attack intersecting a higher-degree node is smaller.

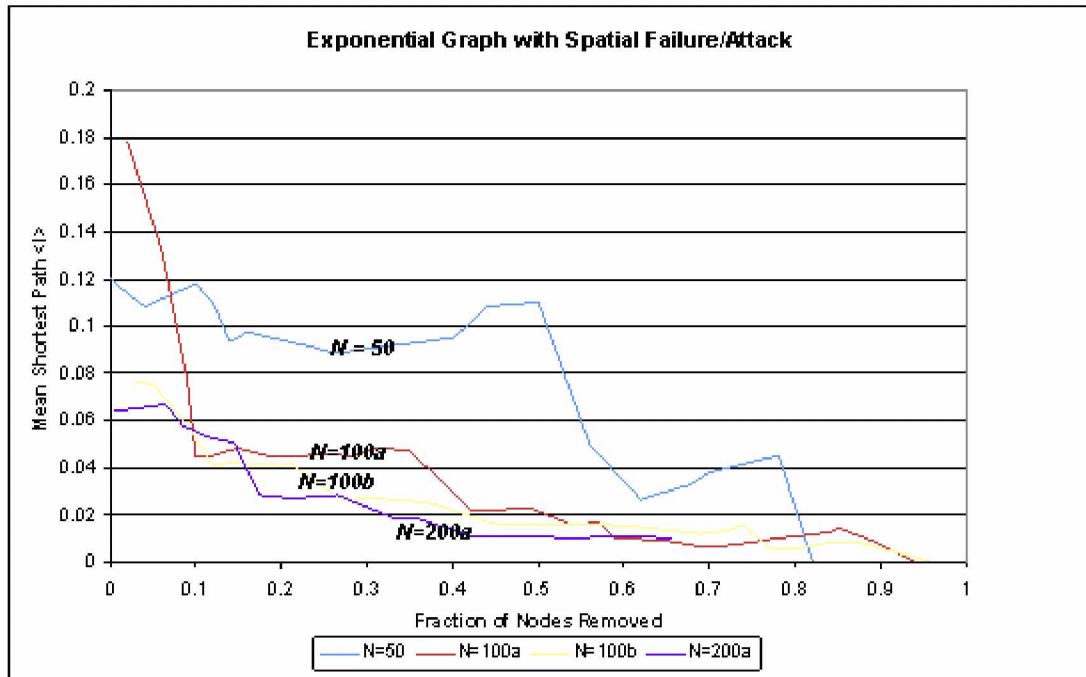


Figure 3-23: Simulation Results for Spatial Attack on Exponential topologies.

Figure 3-24 shows the results of spatial attack on Power-law (Scale-free) topologies.

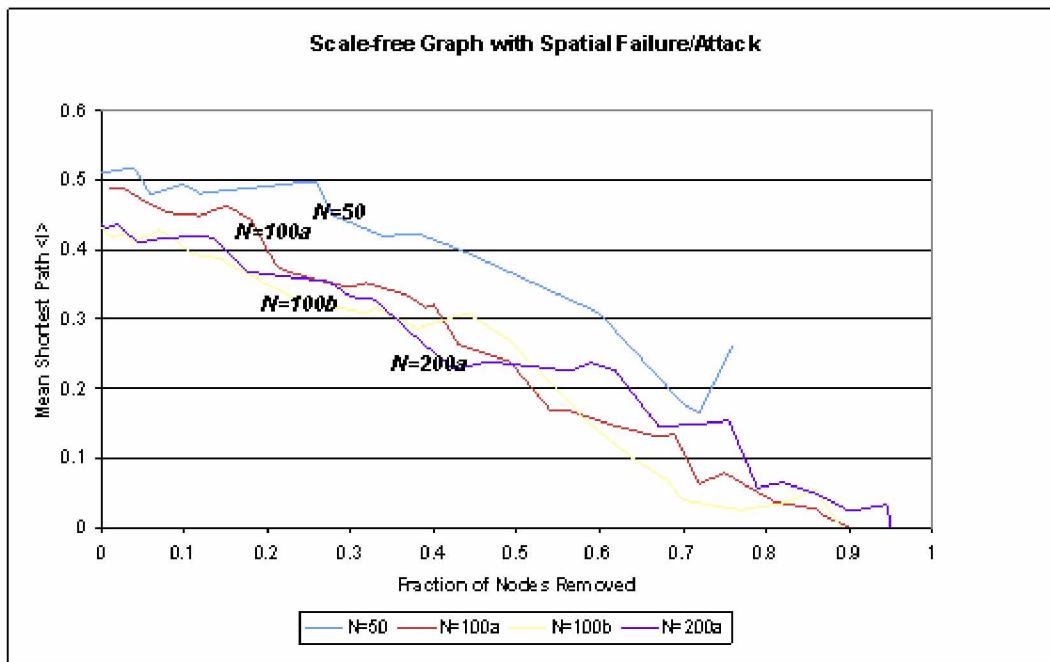


Figure 3-24: Simulation results for Spatial Attack on Power-law topologies.

The resistance of the Power-law topologies to spatial attack is similar to the Power-law topologies subjected to random attack in Figure 3-17. Percolation does not occur until over 70% of the nodes are removed. The magnitudes of \bar{l} are much higher than in the Power-law topology with random attack case, however. This might be explained by the spatial distribution of hubs within the network. Since spatial location is assigned with uniform probability, there is an equal chance of high-degree hubs being placed far from the attack point making them resistant (i.e., lower probability of intersection by concentric rings) and spatially more distant from nodes in the largest connected component.

This analysis was repeated using topologies produced by the Proximal topology generator. Recall that the Proximal generator uses a nearest neighbor assignment scheme which, unlike the previous attack scenario, uses location of the nodes as an explicit criteria in generating the topologies. Figure 3-25 shows the variation in the average shortest path for the largest component of the Proximal generated graph subjected to spatial attack. The resistance to failure is similar to that of the non-spatial scale-free topology, but shows slightly less resistance. 50% loss of the connection efficiency occurs at 50% of the nodes removed. As the network continues to fracture because of the buffered attack, the magnitude of \bar{l} , increases slightly, then decreases as the membership of the largest component changes.

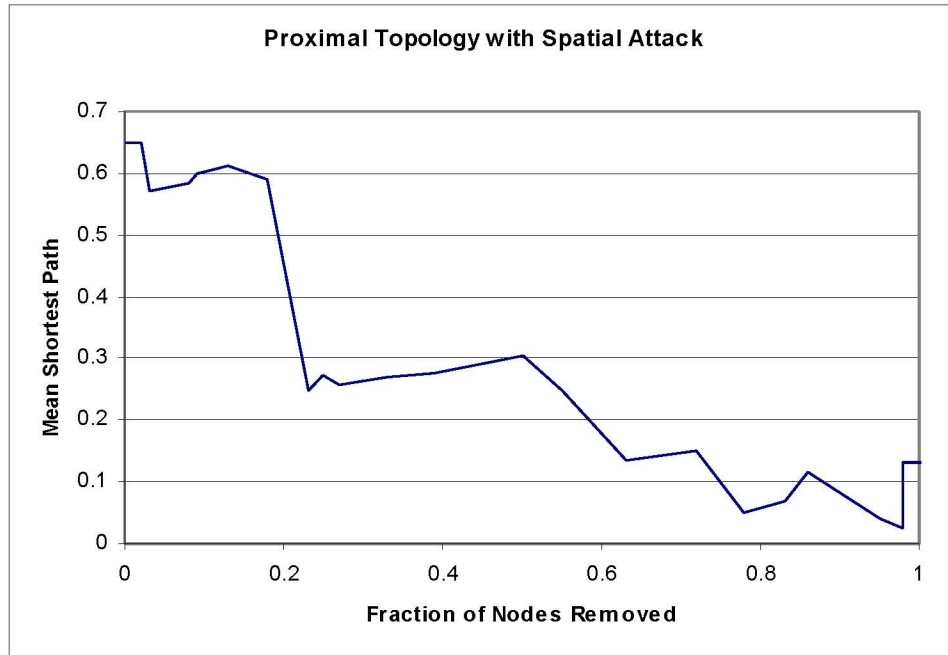


Figure 3-25: Proximal topology subjected to spatial attack ($N = 1000$).

The percolation threshold for the spatial case occurs at approximately 19% of the nodes removed. This improved survivability over the Power-law topology subjected to random attack case is interesting since the magnitudes of the average shortest path are similar. \bar{l} is in the range $0.5 - 0.1$ (before total collapse) for the Power-law topology subject to random attack and $\sim 0.6 - 0.1$ for the Proximal topology with Spatial Attack.

3.5.4 Independent Risk Curve Determination

These analyses have all considered the generation and attack of independent topologies. Whether these topologies represent independent sensor networks or physical infrastructure, their sensitivity to random failure or deliberate attack can be used to generate risk curves (i.e., CCDFs) for representing the independent topology as described in Section 3.1.

To calculate a CCDF for an independent topology, the percolation fractions for 100 realizations of the Proximal topology subject to spatial attack were measured for $N = 100$. The choice of N was arbitrary, although higher values would have increased computation time for \bar{f} calculations substantially. The mean fracture (\bar{f}) was 0.24 (24%) with a standard deviation of 0.09. The distribution (pdf) of the fracture percentages was approximately Normal, although goodness-of-fit statistics were not calculated.

A risk curve was generated for the results and is shown in Figure 3-26.

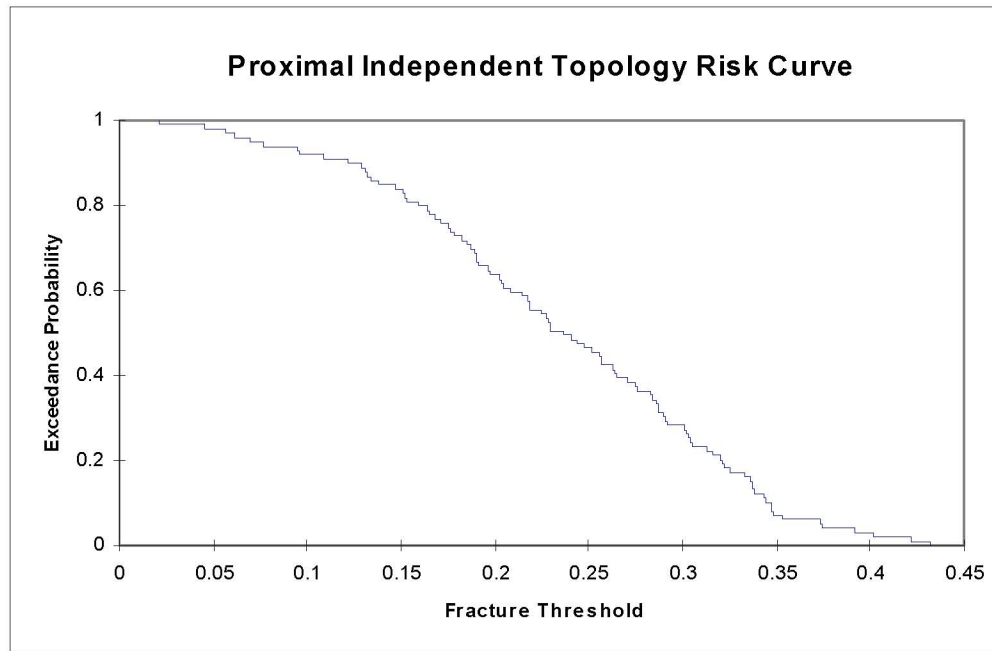


Figure 3-26: CCDF of simulation results from spatial attack on proximal topology.

By itself, the CCDF presents the exceedance probability that a fraction of nodes removed is greater than some threshold fraction (i.e., $P(F \geq f)$). In this case, the exceedance probability that in a spatial attack of a Proximal topology, the percolation

threshold would exceed the mean, $\bar{f} = 0.24$ is approximately 50%. When compared with dependent topology risk curves, this CCDF allows us to classify dominance and non-dominance cases.

As was discussed in Section 3.1, the condition of dominance for risk curves allows for differentiation of networks subject to similar failure conditions. If the dependent curve appears to the right of the independent curve, we can conclude that at all times the risk of the dependent curve is greater. At a fixed consequence, in this case fraction of nodes removed, the exceedance probability is higher and the dependent topology exhibits a risk premium over the independent case. The overriding goal with these comparisons is to identify and quantify derived vulnerability. It is hypothesized that derived vulnerability (i.e., risk inherited from the independent infrastructure network) is significant and dominates any risk or vulnerability that may be inherent in the sensor network itself. Upon determination of a corresponding dependent risk curve or CCDF, the dominance or non-dominance classification can be made and the derived vulnerability estimated.

3.6 Dependent Topology Vulnerability Analysis

The previous analyses have followed the progression from non-spatial topologies subject to random or targeted attack to spatial topologies subject to spatial attack. These analyses both confirm the vulnerability behavior identified by others and introduce new spatial parameters on which topology and vulnerability are based. This section moves beyond these analyses by considering the specific case of dependent topologies of sensor networks and derived vulnerability from the underlying infrastructure network. Of interest is the identification of vulnerability in the dependent network that is separable from the vulnerability of the independent network. In order to perform this separation, it is necessary to test the dependence assumption by, for example, targeting spatial or topologic criteria of the infrastructure network to determine response in the dependent sensor network.

3.6.1 Lifeline-Dependent Sensor Topologies

When sensors are distributed either randomly or around infrastructure, what is the difference in their resistance to loss of topologic connectivity and loss of spatial coverage when the underlying lifeline is attacked? An attack that occurs close to a lifeline network (e.g., pipeline, wire grid, or fiber backbone) will have variable effects depending on the structure of the network(s) in the vicinity of the attack. A practical example of such an attack is a road-side bomb or IED (improvised explosive device) targeting transportation lifelines in the US campaign in Iraq. Such attacks have cost hundreds of lives and caused substantial property destruction. This research quantifies the vulnerability to such attacks and may aid in developing appropriate defense mechanisms.

Figure 3-27 shows a conceptual representation of a lifeline network surrounded by surveillance sensors. In the event of a point-source attack, the impact on the independent and dependent topologies will be a function of *both* the proximity to the attack and the topologic separation (i.e., path distance).

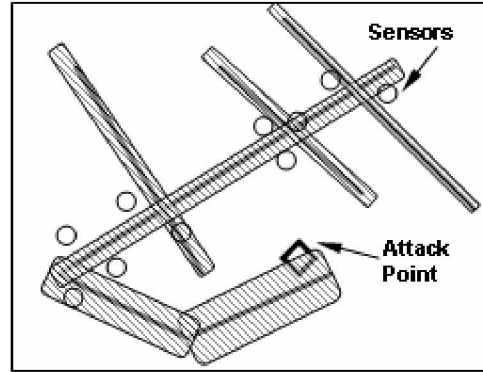


Figure 3-27: Conceptual infrastructure lifelines and impact buffers.

Impact buffers can be created to demarcate the zones affected around lifelines. These are regions drawn around each logical infrastructure lifeline element scaled to represent the spatial extent of an attack targeting that lifeline element. The widths of the buffers are determined based on integrated measures of path and Euclidean separation from the attack point. In Section 2.3.1, *route factor* (q) was introduced as the ratio of path distance to Euclidean separation distance between all points in the graph and some root vertex:

$$q = \frac{1}{n} \sum_{i=1}^n \frac{l_{i0}}{d_{i0}} \quad (3-9)$$

This measure is a proxy for efficiency in the network. High values of q (i.e., $q \gg 1$) indicate that the network is inefficient topologically while low values ($q \ll 1$)

indicate inefficiency in space. This measure can be adapted to model the integrated spatial and topologic impact of a point-source attack such as a bomb blast. As can be seen in Figure 3-27, an attack occurring in close proximity to a lifeline will obviously have a high impact or consequence on the nearest infrastructure as the width of the impact buffer suggests. However, the impact buffer widths of the connected lifeline elements should take into account not only region of influence, which might fall off as the inverse radius squared ($1/r^2$), say, but also the path separation distance. Inverse q (i.e., $1/q$) is an appropriate measure for scaling impact buffer widths as it captures the relative damage of connected infrastructure. By this measure, a long path separation distance may yield a proportionally small impact buffer width even given close proximity to the attack point.

This relationship is used in this section first for generating topologies to surround critical lifeline infrastructure. Second, the relationship is used for a lifeline attack mode where sensors located within impact buffers are targeted and disabled.

3.6.2 Lifeline Topology Generator

Using the arrangement of infrastructure lifelines as a base, the generator distributes nodes and edges to achieve coverage surrounding infrastructure assets. The generator attempts to generate clusters around lifelines to meet requirements of spatial coverage, connectivity between nodes constrained by maximum degree and to minimize the number of long distance connections.

Nodes are placed around infrastructure lifelines and are assumed static (i.e., not mobile), but reconfigurable in their edge attachments. Topologies are created by

nearest neighbor assignment as in the Proximal topology generator discussed previously.

Results of the lifeline topology generator are shown in Figure 3-28. The infrastructure layout is arbitrary; however it does respect the difference between the logical and geometric alignments of a given network. For example, logically the element in the upper-right of the figure is a single lifeline. Geometrically however, it is composed by three different edges connected by node numbers 12, 6, 5, and 11.

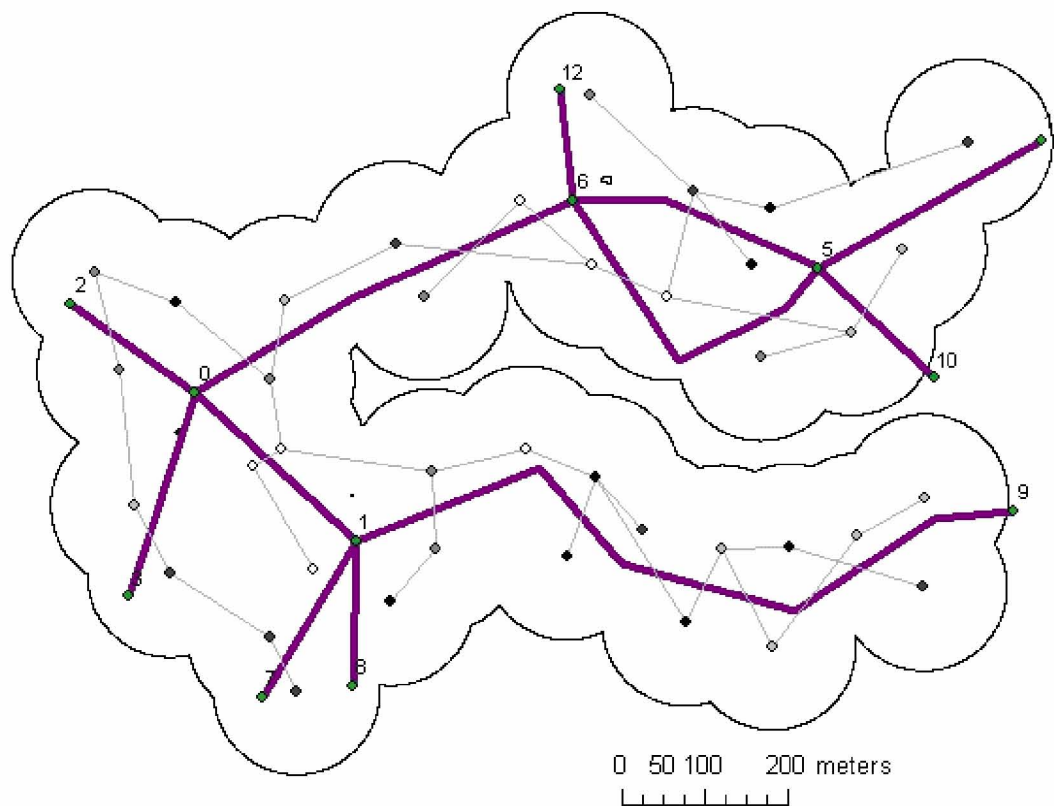


Figure 3-28: Infrastructure sensor network from lifeline generator.

A parameter of the generating algorithm is the spatial surveillance coverage associated with each sensor, set for this example at 100 meters. Upon sufficient

intersection of the respective sensor buffers (i.e., coverage of the independent lifeline), new edges and nodes are no longer added. Sensor degree is constrained to be less than four. The lifeline spatial network evolution achieves 80% coverage of the lifeline network at the point that only 50% of the eventual connectivity is established. As in Figure 3-11, the relative age of sensor nodes added is based on a white to black color ramp where the white colored nodes are the oldest.

This sensor network is relatively small (i.e., $N = 38$) and covers an area of 0.75 km^2 . The total length of the infrastructure lifeline network under surveillance is 3.98 km. The mean degree of the dependent sensor network topology is 2.0 with the resulting degree distribution shown in Figure 3-29. The minimum degree is 1 because of the connectivity constraint and the maximum degree is 4 because of the node-degree constraint of the generator. Note that, unlike the random, Exponential, or power law generators, the degree distribution, which is Poisson, is an artifact of the results and not by design.

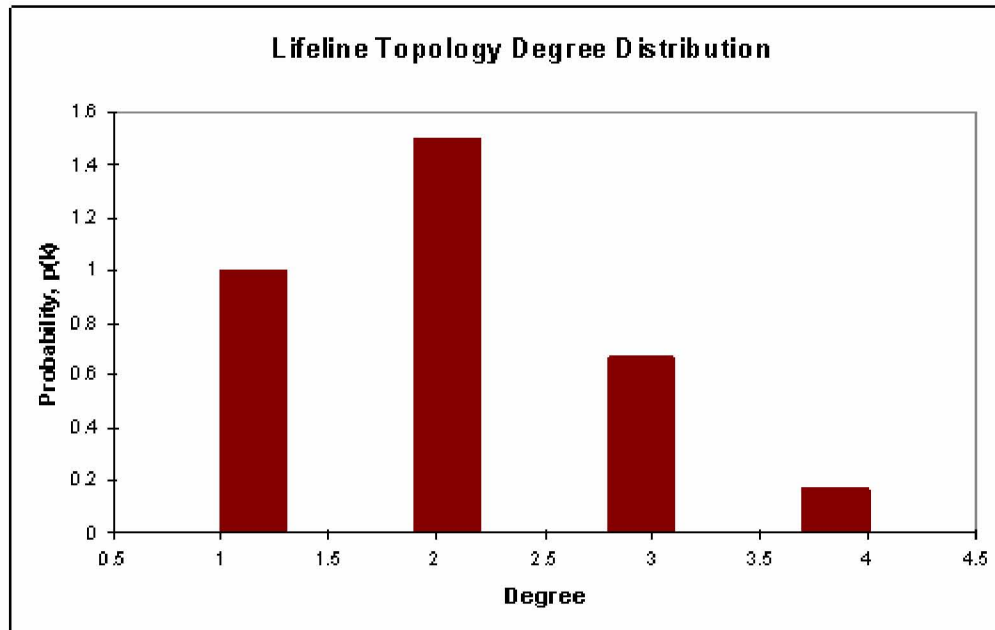


Figure 3-29: Typical lifeline topology degree distribution.

The constraint on limiting long-distance connections is suspected to make the distribution similar to a random topology. Otherwise, behavior similar to the Proximal generator (i.e., closer to Power-law behavior) would be seen.

3.6.3 Lifeline Spatial Attack

The lifeline attack is accomplished by selecting an attack point at random and identifying the nearest lifeline element from a GIS database. The length, capacity, and spatial density of other infrastructure around the selected feature are all a function of the dataset and consequently the built environment and could also be used as attack/selection criteria. For this analysis, attack points were not selected based on criteria of the independent infrastructure. They were chosen randomly.

The selected lifeline is chosen as the epicenter (network centroid) of the attack. The closest infrastructure node to that location is selected as the network root for purposes

of the attack simulation. For each lifeline network element, the Euclidean and path distances are computed from Equation (3-9) and used to compute inverse route factor ($1/q$). Buffer widths are computed by $1/q^2$ and used to create impact regions around each logical infrastructure element.

Figure 3-30 shows the buffer regions (i.e., impact regions) generated by the inverse route factor method for a typical simulation. Note the placement of the attack point in the upper left.

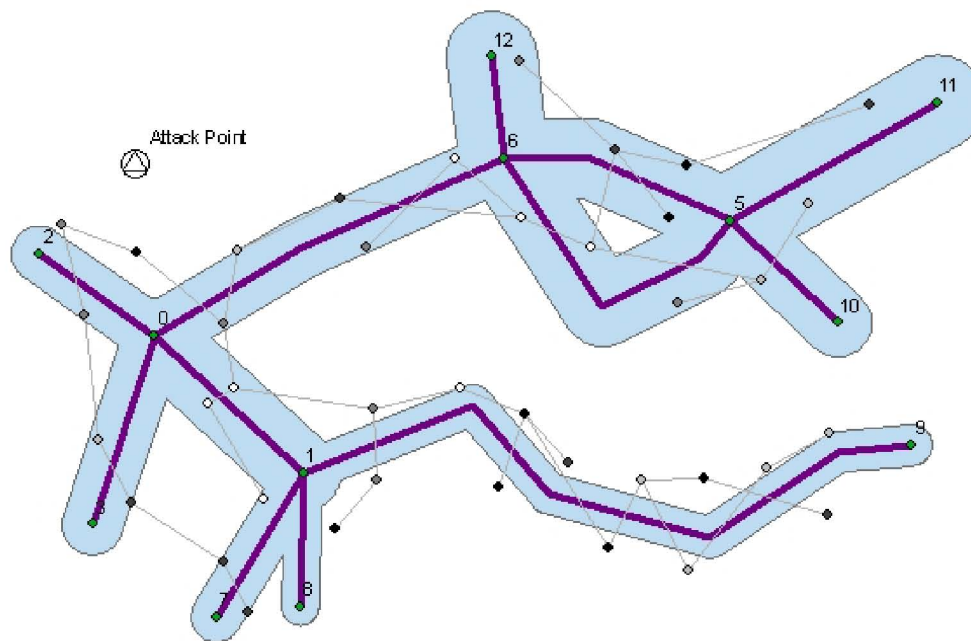


Figure 3-30: Infrastructure lifeline layout with route factor impact buffers.

Because of the location of the attack point, some portions of the independent network are more susceptible than others. The elements closest to the attack point spatially are also close in terms of path separation distance. Note that depending on how the

buffer impact regions are developed, some sensors and their attached edges fall *outside* the effected areas, thereby remaining survivable.

Figure 3-31 shows the results of \bar{I} measurements made when nodes within each buffer impact region are incrementally deleted in order of decreasing buffer width. This is similar to the nodal hierarchy used in the targeted attack mode, except the hierarchy is based on the width of the buffer region, not the degree of the node. Small clusters of nodes, not within the impact regions, remain connected and become the largest connected components in the former network once the affected nodes are removed. Note that topology is not reconfigured after the nodes in each impact buffer region are deleted. In general, the network exhibits extended resistance over the Proximal topology generator. A two-stage percolation occurs with a 50% decrease in the magnitude of \bar{I} occurring at 20% of the nodes removed, and a further reduction of 65% in \bar{I} at 70% of the nodes removed.

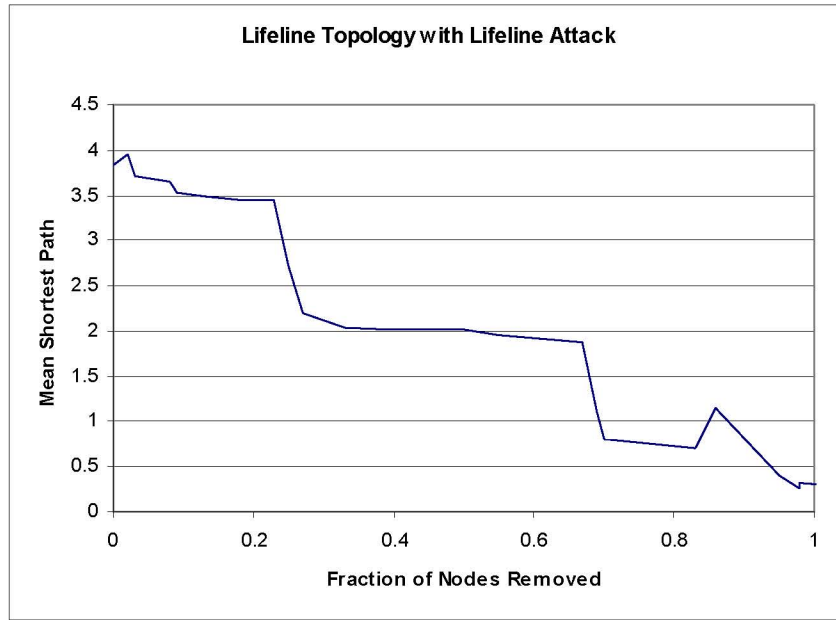


Figure 3-31: Network decay curve for lifeline attack (dependent topology).

In the simulations performed, the nodes that survive the lifeline attack mode do so only marginally. That is, the surviving topologies, generated by the lifeline-dependent attachment scheme, reside just outside the impact buffer regions determined by the inverse q method. This was a surprising, repeatable result despite the changing location of the attack point between simulations.

From this analysis, we have results representing a dependent topology. That is, a sensor network whose topology is dependent on the placement of its nodes around an independent lifeline topology. For the next section, we will use this as a basis for generating risk curves and estimating derived vulnerability by comparing the dependent and independent cases.

3.7 Estimating Derived Vulnerability

As was done for the Independent Topology case in Section 3.5.4, the lifeline attack simulation was run for 100 iterations to determine the percolation thresholds for the dependent sensor network. Recall that the dependent sensor network (i.e., dependent topology) was generated as a function of the lifeline infrastructure based on coverage objectives and degree and maximum edge length constraints. The effects of the attack on the lifeline network (i.e., independent topology) are measured in the sensor network so that the derived vulnerability can be estimated.

For the simulated results, the mean fracture point ($\bar{f} = 0.45$) for the lifeline topology subject to lifeline attack was higher than for the independent case, $\bar{f} = 0.24$ (Proximal topology subject to spatial attack). The standard deviation was much higher as well, 0.31 compared with 0.09. The significantly higher variance in the distribution of fracture thresholds of the dependent topologies has important risk implications for estimating derived vulnerability. Recall from previous discussions that an objective of this research is to estimate and quantify derived vulnerability. Derived vulnerability is calculated from the relative risk dominance or non-dominance relationships of the CCDF curves. The dependent risk (CCDF) curve is generated based on the distribution of the dependent percolation thresholds shown in Figure 3-32.

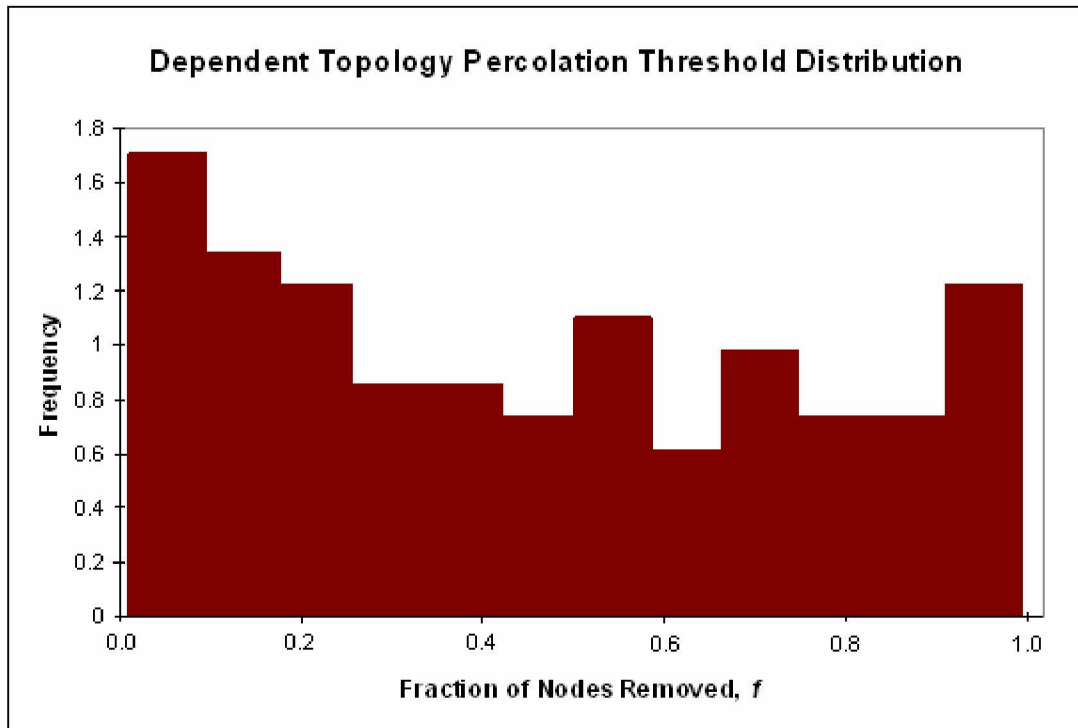


Figure 3-32: Distribution of dependent topology percolation thresholds.

The distribution of dependent percolation (fracture) thresholds is surprisingly bimodal. A high percentage of cases showed percolation at less than 20% of the nodes removed. Another high percentage of cases showed very high resistance to the lifeline attack with percolation not occurring until over 80% of the nodes were removed. The dual fragility and survivability of the dependent topology is very interesting. This could perhaps be explained by the incidence of nodes appearing either just inside or just outside the buffer impact regions of the lifeline infrastructure when subjected to lifeline attack.

The results from the dependent topology simulations were used to generate a dependent topology risk curve or CCDF. Figure 3-33 shows a comparison between

the independent CCDF shown previously in Figure 3-26 with the dependent topology CCDF. Exceedance probability is shown on a log scale for comparison.

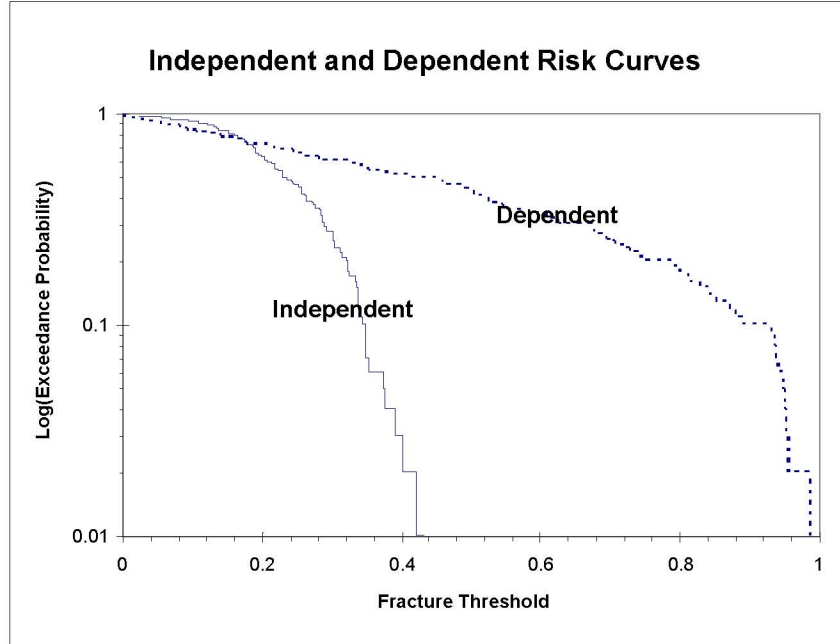


Figure 3-33: Comparison of Dependent and Independent CCDFs.

For the simulation experiments performed, the risk of the dependent topology significantly dominates the risk of the independent topology. For these similar sized networks (i.e., $N = 100$), the risk associated with a fixed consequence (i.e., $f = 0.4$) is greater than 50% ($P(f \geq 0.55) - P(f \geq .05)$). Despite the larger mean percolation threshold in the dependent sensor network which could be interpreted as higher resistance or survivability, the derived vulnerability (risk) is much higher than in the dependent case. This suggests that infrastructure sensor networks experience wide variability and subsequently risk to disruption as a result of their dependence on physical infrastructure networks. The mitigating effects of network reconfigurability using topology control and its applicability will be addressed in Chapter 4.

3.8 Summary

This chapter has presented a basis for quantifying the vulnerability associated with infrastructure sensor networks. New approaches for representing the dependence and independence relationships of topologies were developed and significant results from modeling the derived vulnerability of sensor networks were obtained. The results contribute an increased understanding of the survivability of sensor networks deployed to monitor critical infrastructure.

This chapter defined *dependent topologies* using as an example the CCTV sensor network in London, England used for public safety video surveillance. When vital infrastructure is attacked as it was in that city in July 2005, what impact is there on the sensor network? Can the sensor network survive disruption to maintain monitoring capability during and after an attack? This chapter developed a risk-based framework for representing the *derived vulnerability* of the sensor network when the independent infrastructure network is perturbed. It was shown that the risk associated with dependent sensor network topologies dominates that of the infrastructure network itself with a 50% risk premium of half the nodes being disrupted as a result of the infrastructure being targeted.

A series of simulation analyses were performed to model the percolation behavior of various spatial-topologic graph structures representing both dependent and independent topologies. New, spatial- and lifeline-based topology generators were developed in conjunction with new spatially-based attack modes. Table 3-2 summarizes the results of the simulation analyses performed in this chapter. The

columns represent the respective attack modes and the rows represent the different topologies studied. Whereas the survivability to random and targeted attack on Random, Exponential, and Power-law topologies has been studied previously, the survivability of the spatial and lifeline networks, especially dependent ones, represents a new and unique contribution to risk modeling of infrastructure sensor networks.

Table 3-2: Summary of simulation analyses and survivability results.

| TOPOLOGIES | ATTACK MODES | | | |
|--------------------|----------------------|------------------------|-----------------------|-----------------------------|
| | <i>Random Attack</i> | <i>Targeted Attack</i> | <i>Spatial Attack</i> | <i>Lifeline Attack</i> |
| <i>Random</i> | low resistance | low resistance | N/A [*] | N/A [*] |
| <i>Exponential</i> | med resistance | low resistance | N/A [*] | N/A [*] |
| <i>Power-law</i> | high resistance | very low resistance | N/A [*] | N/A [*] |
| <i>Proximal</i> | N/A [†] | N/A [†] | low resistance | med resistance |
| <i>Lifeline</i> | low resistance | med resistance | low resistance | low resistance [‡] |

^{*} These topology generators do not create spatial properties; therefore spatial attack modes are not possible.

[†] These attack modes were not studied in lieu of the spatial-based modes.

[‡] The mean resistance appears high for this case, but the bimodal percolation distribution suggests high risk and derived vulnerability.

The case has been made in this and in the previous chapter that spatially-based networks are constrained by their physical environment (e.g., planarity) and cannot achieve the efficiency of Exponential and Power-law topologies that feature hubs. These constraints should serve to decrease the vulnerability of these networks when considering the trade-offs of efficiency and risk. The analyses of this chapter have shown that the dependent topologies of infrastructure sensor networks can be even more vulnerable than their Power-law based counterparts.

Given this vulnerability, the need for considering the reconfigurability of infrastructure sensor networks is apparent. The next Chapter presents a framework for implementing topology control in infrastructure sensor networks that can mitigate their derived vulnerability and exhibit decentralized self-organization behavior.

4 Chapter Four – Self-Organization and Topology Control

The analyses of the previous chapter demonstrated the particular susceptibility of dependent sensor network topologies to attacks on infrastructure. The lifeline attack mode, which targeted the sensors surrounding lifeline network elements, yielded high variation of percolation threshold and a high risk premium on dependent topologies. The capabilities of sensor networking technology to detect disruption or degradation, dynamically compute new topologies based on coverage or performance requirements, and physically reform the network by reestablishing connectivity are a new approach for mitigating this risk. *Topology control* reactively resists percolation in the network and preserves both connectivity and efficiency, but its application can be limited.

It will be shown in this chapter that, despite the mitigating effects of topology control, there are performance boundaries that limit its application particularly across large spatial scales and when optimal or near-optimal topologies (with respect to physical layer cost, network layer congestion, or both) must be computed for large homogeneous networks in near real-time. Further, the reliance of centralized control (i.e., topology calculation and dissemination through a designated topology control node) will be discussed with an alternative *self-organization* framework proposed.

The motivations for this chapter are:

1. to demonstrate the applicability of topology control for mitigating the inherent risk in lifeline dependent sensor networks;
2. to investigate the performance bounds of topology control when applied across large spatial scales and for large homogenous networks;
3. to present a use case for self-organization behavior applied for scalable, survivable, topology control.

Section 4.1 investigates the first motivation above. The lifeline attack simulations in the previous chapter are repeated but with topology control applied. The degree of percolation resistance under topology control is discussed as well as the effect of spatial coverage loss.

Section 4.2 examines the critical spatial density of nodes necessary for the application of topology control and its implications on survivability.

Finally, Section 4.3 addresses the third motivation by introducing a framework for the self-organization behavior of lifeline dependent sensor networks.

Three research outcomes, summarized in Table 1-1 are developed in this chapter: lifeline attack resistance with and without topology control, the critical percolation density for sensor networks, and the balance of self-organization and topology control.

4.1 Survivability of Infrastructure Sensor Networks with Topology Control

The analysis of dependent sensor network vulnerability in Chapter 3 highlighted the increased risk of topologies which are dependent on underlying infrastructure versus independent topologies generated by spatial criteria. The lifeline topologies, generated based on coverage and maximum link length constraints, demonstrate wide variation in survivability as was shown in Figure 3-32. The application of topology control is presented in this section to evaluate its mitigating effects in response to lifeline-based attack.

4.1.1 Lifeline Topology Control Algorithm

The lifeline topology generator discussed in Section 3.6.2 operates by placing nodes around lifeline infrastructure according to coverage, degree, and maximum edge length constraints. Node placements and edge attachments are the outputs of the generator. In this sense, the generator is performing topology planning/design.

In response to network perturbation, the process of topology control has a much different function. It responds to disruption in real time and forms a new topology based on the prior objectives and constraints, but with node location fixed. In this sense, topology control has much less freedom to achieve its objectives.

The lifeline topology control algorithm (LTCA) is based on the physical layer topology control heuristics described in Section 2.5.1. Equation (4-1) is the formulation of the minimum lifeline cost ($cost_{ll}$) objective:

$$\begin{aligned}
cost_{ll} = \min \sum_{(i,j)} b_{ij} d_{ij} \\
s.t. \begin{cases} \sum_j b_{ij} = 1, \forall i \\ b_{ij} = b_{ji}, \forall i, j \end{cases}
\end{aligned} \tag{4-1}$$

where d_{ij} is the effective edge length between nodes and b_{ij} is the minimum connectivity constraint.

Figure 4-1 depicts the application of the lifeline topology control process. In Figure 4-1(a), a segment of the unperturbed infrastructure network is shown with a five node sensor network surrounding it. The respective service areas of each sensor node blanket the extent of the infrastructure network. The topology of the sensor network, one 4-degree node and four 1-degree nodes, was generated by the lifeline topology generator. Bi-connectivity was not required.

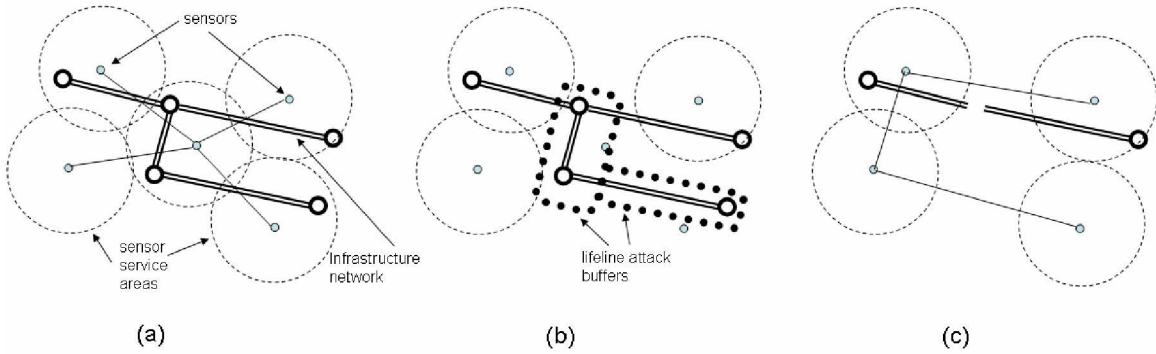


Figure 4-1: Illustration of Lifeline Topology Control.

In Figure 4-1(b), lifeline attack occurs destroying two of the infrastructure network segments. The central node in the sensor network is intersected by the buffer impact region and is thus destroyed. The sensor in the lower-right is just outside the buffer region and it survives. At this point, topology control is applied to re-establish

connectivity in the sensor network. In Figure 4-1(c), the infrastructure and sensor networks are shown after topology control is applied. New links are established connecting the four remaining nodes. Note that connections are chosen so as to go around the area affected by the lifeline attack. It is presumed that disruptions occurring along linear infrastructure elements will obscure line-of-sight connections across the disruption. The constraint is imposed that new sensor network links cannot be established crossing over disrupted infrastructure elements.

4.1.2 Lifeline Attack with Topology Control

The lifeline attack simulations in Section 3.6.3 were repeated and augmented to allow topology reconfiguration. Topology control was implemented to form minimum-cost (i.e., with respect to effective edge length) topologies after the deletion of nodes intersecting each buffer region. Average shortest path for the largest connected component was measured after each perturbation and again after topology control was applied. Unlike the previous analyses, the addition of topology control in response to lifeline attack attempts to preserve the largest connected component in the network. Therefore, the set of nodes that comprise the largest component are expected to remain stable, the effects of the lifeline attack notwithstanding.

Figure 4-2 shows the results of the lifeline attack on the lifeline topology with topology control. As the nodes intersecting each lifeline buffer region are deleted, topology control is applied to reestablish connectivity in the network. The mean shortest path of the largest component in the network is measured before the application of topology

control and after. As a result, the size of the largest connected component, to the extent possible given the loss of nodes, is restored to near its original size.

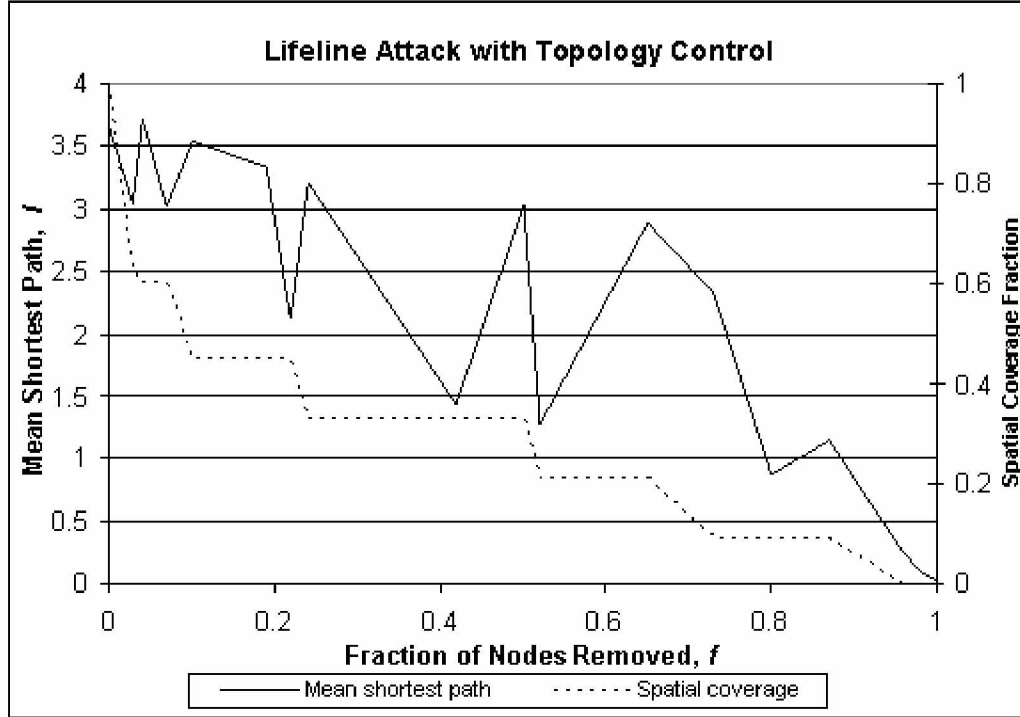


Figure 4-2: Network decay of lifeline topology subject to lifeline attack with topology control.

The mean shortest path oscillates as a result of the LTCA. Each drop in \bar{l} corresponds with the selection and deletion of an impact buffer region and each increase is the topology control response. Note that with the application of topology control, no abrupt percolation occurs. In fact, a 50% decrease in \bar{l} from the unperturbed condition does not occur until 80% of the nodes have been removed. This demonstrates the effectiveness of topology control in recovering connectivity after disruption occurs.

Also shown in Figure 4-2 is the change in spatial coverage (secondary vertical axis) as a result of the lifeline attack. Spatial coverage is a function of the placement of nodes. At

75% of the nodes removed from the network, the lifeline network has only 10% coverage, although a portion of the sensor network remains connected and the mean shortest path is 85% of the unperturbed state. This is due to the survival of nodes at the fringe of the lifeline dependent network. As was discussed in Section 3.6.3, these fringe nodes play a large role in determining the percolation threshold of lifeline topologies subject to lifeline attack. The application of topology control increases this role by resisting percolation until a very large fraction of nodes are deleted from the network. It does not, however, preserve the spatial coverage of the deleted nodes. Topology control cannot directly address the restoration of coverage area unless nodes are mobile and able to re-position themselves in response to failure or attack.

To compare the performance of the LTCA across simulations and against the no-topology control lifeline attack case, the distribution of f was evaluated. The application of topology control causes the network decay to occur gradually, without abrupt changes in connectivity of the largest component as was seen in other cases. Percolation threshold was taken as that f where a 50% drop in \bar{l} occurs. 100 iterations of the lifeline attack scenario were repeated for the lifeline network used previously. Sensor network topologies with $N = 30$ were simulated. The mean percolation threshold for these simulations was $\bar{f} = 0.68$ with standard deviation equal to 0.11. The distribution of percolation thresholds is shown in Figure 4-3.

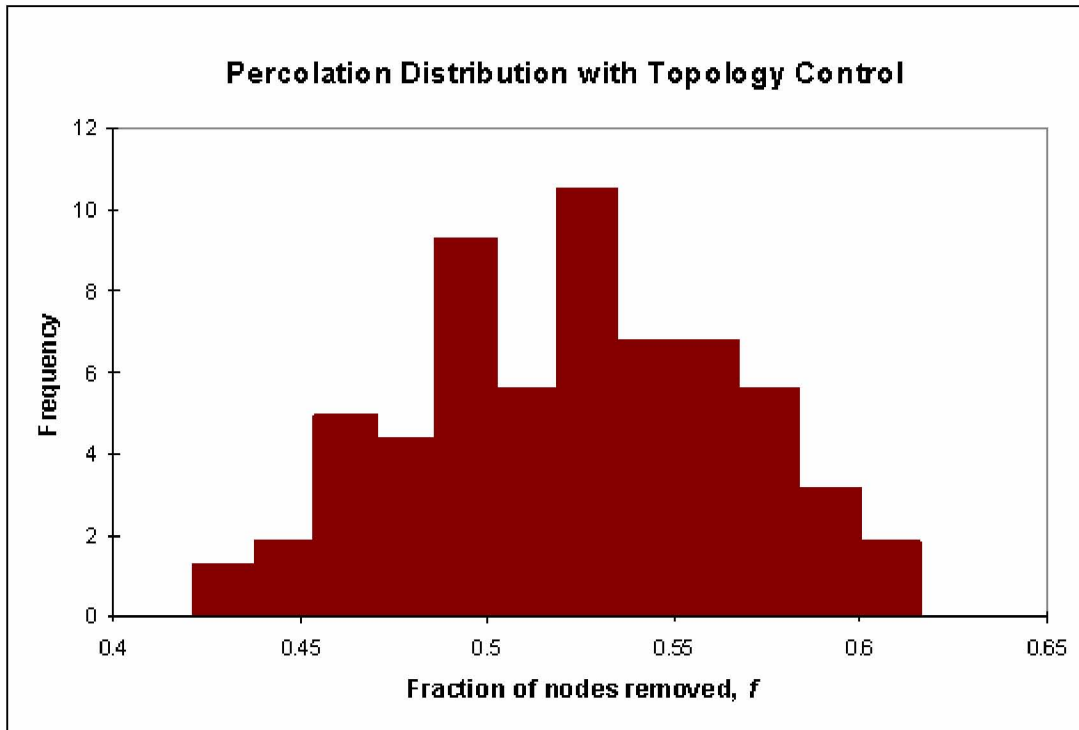


Figure 4-3: Percolation threshold distribution for lifeline attack with topology control.

The distribution is approximately Normal. Recall the mean percolation threshold $\bar{f} = 0.45$ and bimodal distribution of percolation thresholds for the no-topology control case in Figure 3-32. Percolation occurred with high probability for both low ($< 10\%$) and high ($> 90\%$) thresholds in that case. The topology control case results in both higher mean resistance and lower variance.

Although spatial coverage is not retained to the same degree, topology control is successful at preserving a connected component such that activity observed from the remaining sensors can be communicated across the network. The next section investigates some limitations of topology control when applied to infrastructure sensor networks

4.2 Limitations on Topology Control Scalability

Topology control is very effective in mitigating the effects of percolation and maintaining connectivity through significant fracture in the network. The ability to reconfigure the network is based on potential connectivity. The LTCA operates on a potential connectivity graph determined from nodes within the observable service area of each node. For the lifeline attack simulations of Chapter 3 and Chapter 4, the nominal radius (r) for each sensor was approximated as 1 km. This corresponds with the current capabilities of Free Space Optical (FSO) and hybrid RF/FSO point-to-point sensor networks discussed in Section 2.5.4.

There are diminishing returns on the application of topology control across scales. Topology control stops being effective as the scale of the network grows. The topology control algorithm developed is spatially constrained (i.e., it is incapable of making long haul connections). Without long-haul connections, we lack the edge length diversity and consequently the resistance observed from the Proximal generator. As the locations of the sensors remains fixed, the applicability of topology control is limited by the spatial range of each sensor.

Kumar et. al (2005) provides a theoretical basis for the scalability limit of both coverage and throughput (θ). Placement of nodes becomes the controlling parameter in the spatial scalability of topology control algorithms. The application to lifeline-based topologies has not been studied and is the basis for this section.

4.2.1 Critical Density

Given the effectiveness of topology control in recovering the connectivity of lifeline dependent sensors, and the apparent inability for topology control to mitigate loss in spatial coverage due to lifeline-based attack, an estimate of the critical density below which topology control is completely ineffective is needed. Density of sensors is measured by the number of sensors per area, per length of the lifeline network.

Simulations were performed to generate 100 realizations of a lifeline topology subject to lifeline attack with the application of topology control. Beginning with a sensor density of 0.005 sensors per square meter per meter of lifeline, the density was incrementally decreased and the mean shortest path measured.

Figure 4-4 presents the results of the simulations. The horizontal axis shows the sensor density and the vertical axis the exceedance probability of mean shortest path. Reading from right to left, topology control remains effective at maintaining 70% of the unperturbed dependent sensor network connectivity until the density drops to 0.003 sensors / m^2 / m. At that point, the probability drops precipitously until a density of 0.0014, where exceedance probability drops to zero. This means that in the 100 simulations performed, none resulted in the recovery of connectivity by the action of topology control below a density of 0.0014 sensors / m^2 / m.

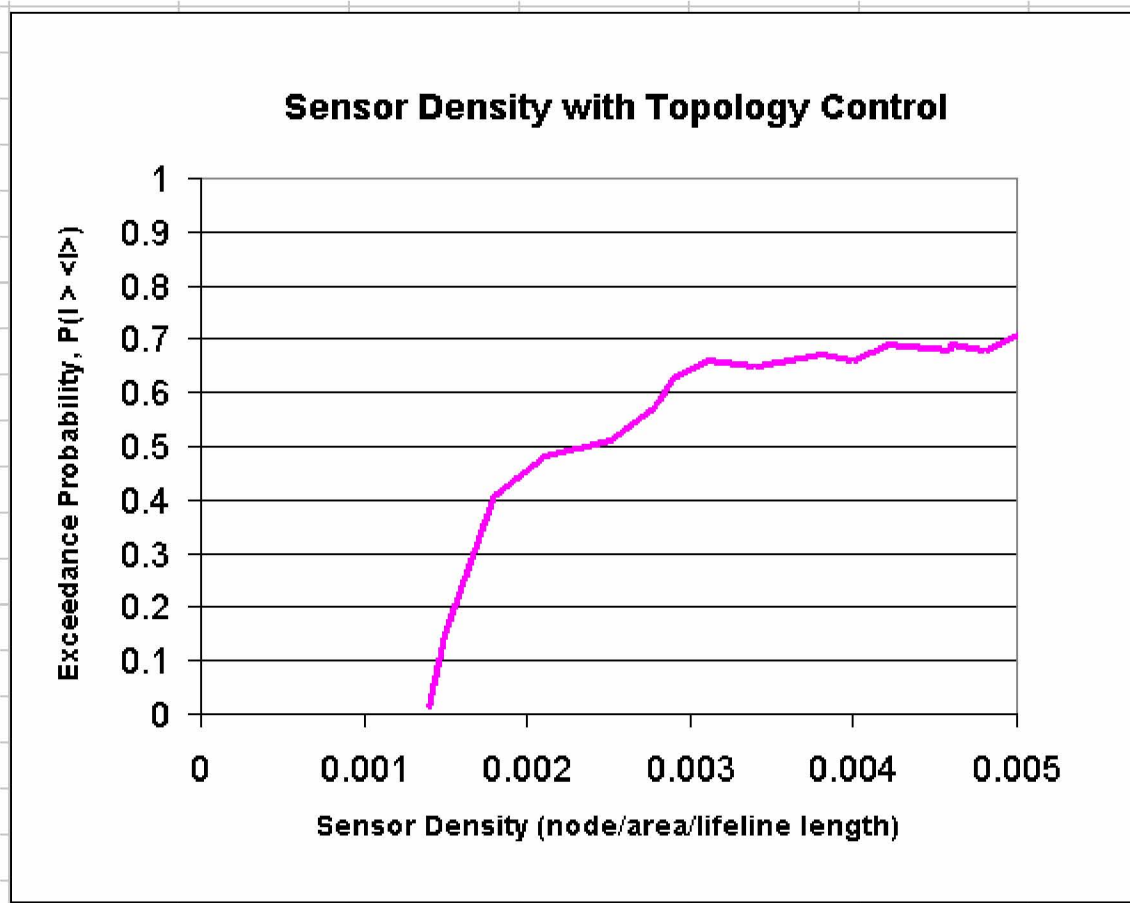


Figure 4-4: Experimentally derived critical density determination for lifeline dependent topologies.

This analysis has provided an experimental estimation of the critical density of lifeline sensor networks subject to lifeline-based attack. Although analytical methods exist to estimate the theoretical critical density of nodes distributed on a two dimensional lattice (see discussion in Section 2.2.5), none such methods exist for linearly-dependent features (i.e., random lattices with arbitrary, topologically connected linear gaps or voids). This experimental approach provides a practical limit which may be applied by placement algorithms or node-mobility processes to insure that the density of lifeline dependent sensor networks doesn't drop below critical levels.

4.3 Self-organization of Infrastructure Sensor Networks

Infrastructure is generally not self-organized. In fact, physical infrastructure is carefully planned to meet coverage, capacity, and service life requirements. More recently, effort has been devoted to infrastructure design that includes survivability (e.g. blast resistance) and redundant (i.e., backup) systems. As previously stated, this research focuses on decoupling the sensor network from the infrastructure it monitors to allow for self-organization behavior.

Research in *self-organizing* systems is centered on observed system behavior not designed or predicted by underlying properties or components. Such “emergent” properties can be seen in system initialization (i.e., connections between components), to evolution (growth or decay of the system) to healing (restoration of connectivity or transport capacity after disruption). Sensor networks embody all of these emergent properties.

A system is *self-organized* if it is structured without any external or dedicated control entity. Interaction between the constituent parts of the system is localized. That is, there is no one entity that is responsible for the coordination of the individual entities. The effects of self-organization include *adaptability*, *scalability*, *robustness*, and *survivability*. Adaptability is the simultaneous response of the entire system initiated by the action of one or a small set of constituent parts. Scalability is the replication of self-organizing behavior across small or large numbers of system components distributed spatially, temporally, or both. Robustness is the ability of the overall system to maintain expected performance given the loss of some system parts. And, survivability, as defined in

Section 2.2.6, is the ability of the system to remain connected while a significant fraction of its parts are removed or destroyed.

These behaviors represent the ideal characteristics of a dynamic wireless sensor network deployed for the monitoring of critical infrastructure. Topology control processes, although effective at mitigating the risks of lifeline-based attacks down to the limits of critical sensor density, are burdened with computational and communication overhead in the reconfiguration of the network after a disruption occurs. Optimal topologies with respect to physical layer cost, network layer congestion, or both approach NP-Hard complexity. Even given efficient heuristics capable of calculation of near-optimal topologies in near-real time, the communication overhead in acquiring current link state information for the entire network is limiting. A framework for the distributed, decentralized, and *in situ* application of topology control is needed.

The development of this framework is extensive and beyond the scope of this dissertation. However, the functional requirements of such a framework are discussed in addition to applications for critical infrastructure protection. The three sections that follow highlight the principal requirements of a self-organization framework for the distributed application of topology control.

4.3.1 Heterogeneous architecture

The assumption of homogeneity among sensor nodes is prefaced on the requirement that any other node can assume the centralized DTCN role should the current DTCN be compromised. This constraint results in a lack of diversity in node capabilities. Each node shares the same range (surveillance and communication capability), connection

capacity (number of interfaces), and handling capacity (throughput). This lack of diversity sacrifices the efficiencies that are possible from graph structures such as Power-law topologies.

Figure 4-5 depicts a conceptual representation of a hierarchical network.

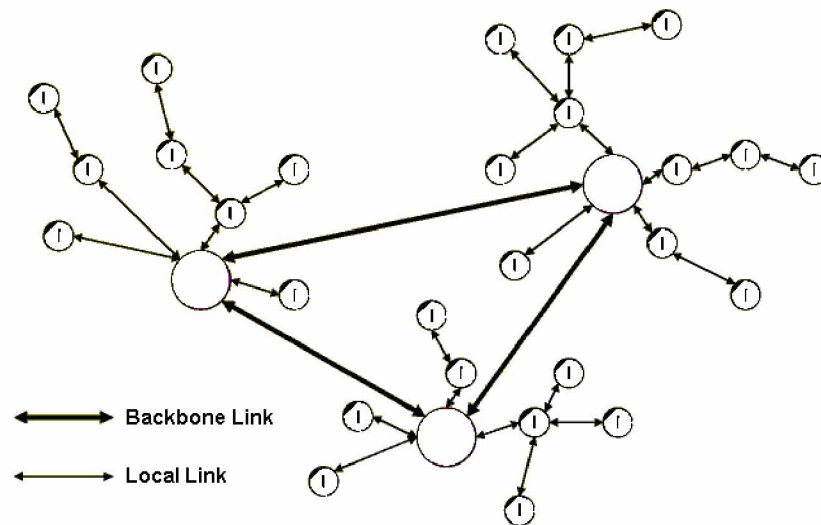


Figure 4-5: Conceptual heterogeneous (hierarchical) network architecture.

A hierarchical self-organization framework would allow for the application of topology control locally-only. Given small clusters of nodes, optimal or near-optimal topologies could be computed and implemented without regard to the other clusters in the network. Similarly, base-station sensor nodes or cluster heads could establish topologies between similar nodes. The application of topology control at multiple network tiers would alleviate computational complexity and improve survivability without sacrificing efficiency.

4.3.2 Evolutionary design

Evolutionary design is the assignment of locally applied rules to individual system components. The interaction of individual components affect global performance of the system, whose behavior is said to be emergent. Emergent behavior is a requirement of a self-organization framework for infrastructure sensor networks because of the need for large scale coverage and connectivity, but without centralized control. Evolutionary design algorithms can establish fitness parameters in the network that estimate global state (node location, throughput capability, etc.) given only local parameters. Although the translation of cellular automata-type models to a sensor network platform have been suggested, the specific constraints of survivability and application of topology control have not been formulated as yet.

4.3.3 In-situ processing

In-situ processing is the capability of the sensor network to manipulate both surveillance data being collected from a particular node at that node location, and to analyze traffic from neighboring nodes for relevance to the overall network state. The same computational capability that would otherwise be necessary for topology calculation and formation could be applied to in-situ processing to alleviate some of the surveillance and communication overhead in the network. This is a requirement of a self-organization framework for infrastructure sensor networks because of the need to not just reactive but proactive topology control. The capacity for the network to maintain or recover spatial coverage and network connectivity can be enhanced by a distributed method for each node to determine global network state based on data sampled and processed in-situ.

4.4 Summary

The focus of this chapter was the application of topology control for mitigating the derived vulnerability and inherent risks in dependent sensor networks. Topology control was shown to be effective in recovering a large fraction of the unperturbed network connectivity as measured by mean shortest path when a lifeline topology was subjected to lifeline-based attack. Topology control was not, however, effective at recovering the spatial coverage of the network.

The critical density of lifeline-dependent sensor networks was estimated using simulation experiments. Below a density of $0.0014 \text{ sensors} / \text{m}^2 / \text{m}$, topology control was in effective at maintaining connectivity of the dependent network.

This chapter attempts to reconcile two competing forces of network organization. Self-organization is a bottom-up process where nodes are given simple rules applicable for communicating with neighboring nodes only, and through emergence, achieve globally desirable performance characteristics. *Topology control*, as described in Chapter 2, is largely a top-down process where network-wide control is centralized in a DTCN (Designated topology control node) which is responsible for determining a desirable, ideally optimal, topology as a function of physical layer costs or network layer congestion. The requirements of a self-organization framework for infrastructure sensor networks where the balance of the bottom-up and top-down network control processes is a function of the independent topology (i.e., physical infrastructure network) as well as conditions in the physical and network layers was presented.

5 Chapter Five – Summary and Conclusions

The infrastructure that supports our quality of life is increasingly fragile. In our efforts to engineer inexpensive and efficient energy, transportation, communication, and utility networks, the normal trade-offs between cost and level of service have been complicated by security concerns. It is no longer enough to design efficient, cost-effective systems – they must be survivable to both natural and man-made (e.g., terrorist) disruptions and take into account emergent properties of interconnected, inter-dependent infrastructure to prevent catastrophic and cascading failures.

Sensor networks provide new capabilities to monitor the health, performance, and security of our dense interconnected infrastructure. But these networks too, if coupled or co-located with infrastructure networks, are vulnerable. This research has investigated the vulnerability and survivability of sensor networks deployed to monitor critical infrastructure and presented sensor network survivability in an infrastructure risk context.

In Section 1.1, the focus of this research was codified by Mendes et al. (2004): to “address in a systematic fashion the robustness and vulnerability of large technological and infrastructural networks...Complex networks react in different ways to different perturbations. In general they are robust to random damages but weak to attacks targeting some key elements of the system. A systematic theory of network resilience and robustness needs to address both local (individual failures) and global vulnerabilities (cascading failures).”

This research has responded to this problem definition by directly investigating the vulnerability of dependent infrastructure sensor networks. The variable vulnerability of different spatial and topologic structures was simulated to generate a risk profile of dependent sensor networks. Topology control was introduced as a mitigating technology for preventing fracture in networks. Lastly, self-organization behavior of sensor nodes was presented as a framework for overcoming the spatial-scalability limitations of sensor networks at critical percolation density.

Although a contribution, this research is only a step in the direction of full understanding of vulnerability and survivability of infrastructure sensor networks.

Figure 5-1 is a conceptual representation of the research areas that will contribute to the creation of survivable *yet dependent* sensor networks.

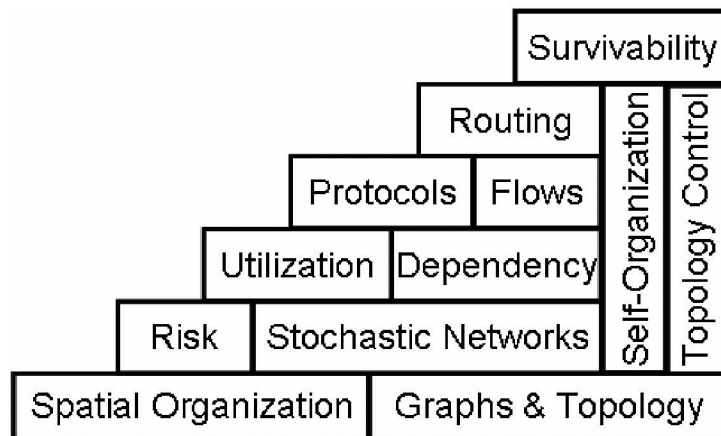


Figure 5-1: Sensor network survivability "layer cake"

This work has addressed research needs in the bottom layers, however significantly more work is necessary to develop a complete platform that includes robust survivability in the engineering trade-offs of cost and efficiency.

5.1 Assessment of Goals and Objectives

In Section 0, the goals and objectives for this research were presented. The overriding goal has been to make a fundamental contribution of knowledge in the modeling of sensor networks deployed for critical infrastructure protection. The vast majority of research in sensor networks is conducted in the realm of electrical and communications engineering. This research has presented a unique and interdisciplinary approach for considering the fundamental spatial and survivability requirements of infrastructure sensor networks.

The first objective of this research was to quantitatively assess the vulnerability and survivability of different spatial/topologic structures to random, targeted, and spatially-based perturbations. While the attack tolerance of large aspatial networks has been studied by Albert et. al. (2000), and the vulnerability of fixed information infrastructure networks has been studied by Gorman (2004; Gorman et al. 2004), no study of random, spatially-generated topologies, especially infrastructure dependent lifelines, has been performed to date. The simulation analyses of Chapter 3 demonstrated the increased survivability of spatial networks (i.e., higher mean percolation threshold than Power-law topologies) and the high variability in the percolation behavior (i.e., bimodal distribution of mean percolation threshold) of dependent sensor networks.

The second objective was to investigate the dependency relationships between sensor and infrastructure networks with respect to risk and re-configurability. The concepts of independent and dependent topology were presented in addition to derived

vulnerability. Risk curves, or complimentary cumulative distribution functions (CCDFs) were used to summarize the risk (i.e., consequence multiplied by likelihood of occurrence) associated with different topologies. The wide variation in mean percolation threshold for the lifeline dependent sensor network topology, and the corresponding CCDF, contributed to the dependent topology risk dominating the risk of the independent infrastructure network. With the application of topology control for re-configuration of the topology after lifeline-based disruption occurred, the net percolation threshold rose, effectively to 1, within the limits of the critical density of nodes in the network. Thus, topology control was shown to create an iso-risk relationship where the dependent sensor network was no more vulnerable than the infrastructure network itself.

The third objective was to demonstrate the application of topology control and self-organization behavior in infrastructure sensor networks and fundamental limits on their use. In addressing the second objective, topology control was successful in recovering from instantaneous percolation. The limit of this response capability is quickly reached as the spatial density of nodes decreased below a critical threshold. Using a percolation-theory based approach; a technique for applying self-organization behavior of sensor nodes to form sub-critical hierarchies of sensor network clusters was developed.

5.2 Summary of Findings

In this section, the ten principal and unique findings of this research are summarized as outlined in Section 1.4:

5.2.1 Infrastructure graph context

The problem of infrastructure organization and performance was framed as a graph-model class decomposition in Figure 2-1. The selection of appropriate graph models depends on the physics of the infrastructure network. Transportation networks are generally undirected while flow networks are usually always directed. Spatial properties and physical constraints also contribute to the suitability of particular graph models used to represent infrastructure. Graph models and their corresponding topologies have implications on efficiency and survivability. Power-law and dependent sensor network topologies are “robust yet fragile. That is, they are resistant to random failure but susceptible to intentional attack.

5.2.2 Spatial-Topologic context for infrastructure

The unique “robust yet fragile” nature of aspatial networks was used to show how the spatial structure of networks is constrained, less efficient, yet more survivable. The scales of efficiency (e.g., very high degree hubs) are not possible in spatial networks because of planarity and physical space constraints, but the structural trade-offs between spatial and topological organization provide additional degrees of freedom in quantifying risk. Spatial attack can be more damaging than targeted attack alone based on inter-dependency and co-location of networked infrastructure.

5.2.3 Infrastructure Risk

A framework was presented for describing the hazards, vulnerability, and risk criteria associated with infrastructure and infrastructure sensor networks. Physical infrastructure networks are generally vulnerable because of their inter-connected, interdependent, co-located and coupling properties. Infrastructure Sensor networks needed for monitoring and surveillance of infrastructure. A combined risk context allows for estimation of vulnerability and prediction of survivability.

5.2.4 Independent and Dependent Topologies

The concept of independent and dependent topologies was presented. An independent topology is one on which no other topology relies for its structure. Infrastructure networks (e.g., roads, pipes, communication backbones) were treated as independent topologies in this research. A dependent topology is one in which the structure (i.e., spatial arrangement of nodes and topology of edge-vertex connections) relies on another topology. Infrastructure sensor networks were treated as dependent topologies in this research.

The novel implication with these two concepts is that the dependent topology, in addition to its structure, can assume both the efficiency in performance and the vulnerability of the independent topology

5.2.5 Derived Vulnerability

Derived vulnerability was introduced as the vulnerability inherited from the independent infrastructure network. Put in the context of risk curves which show the consequence-weighted likelihood of occurrence of network percolation, for example,

derived vulnerability can be used to quantify the degree to which a dependent topology is more or less risky than an independent one.

It was demonstrated how the derived vulnerability from dependent topologies can be dominated by the topology of the underlying infrastructure, but in most cases the infrastructure dominates the independent case. The vulnerability of independent and dependent topologies was compared using the concept of risk dominance and non-dominance. CCDF curves (i.e., risk curves) generated for each case were compared to show that the lifeline based attack mode in general is less survivable than the spatial (i.e., Proximal) based attack.

Although not directly investigated, alternate properties of networks were discussed with respect to their role in vulnerability particularly flows and utilization in communication, electrical power, and transportation networks. Here, the structural vulnerability of networks was discussed and the effects of cascading failures which can dominate any vulnerability inferred from the topologies structure of the network alone.

5.2.6 Topology Generators

Two topology generators were developed that use spatial criteria as opposed to degree-based preferential attachment to create stochastic topologies. The first, a Proximal generator (Section 3.3.4), uses nearest-neighbor attachment during a network evolution process. The degree distributions of these topologies resembled Power-law topologies, but were more resistant to targeted (i.e., spatial) attack. The

diversity of edge lengths in the network, which are responsible for this resistance, makes the Proximal topologies a fundamentally different type of graph.

The second generator, a Lifeline Topology Generator (Section 3.6.2), uses the spatial organization of an infrastructure lifeline network as a growth function such that each sensor placed in the network provides incremental spatial coverage of the infrastructure and is within minimum (i.e., 1) and maximum (i.e., 4) degree constraints. The degree distribution of these topologies were Poisson, although the network size was small (i.e., $N < 50$) for the topologies generated. Vulnerability of lifeline-generated topologies appeared lower based on a higher mean percolation threshold compared to the Proximal topologies. However, a high variance and bimodal distribution of percolation threshold indicated substantially more vulnerability.

5.2.7 Spatial and Lifeline-based Attack Modes

Directed attack modes based on spatial rather than degree criteria were created. The spatial attack mode involves the random selection of an attack point within a sensor field. A radius around the attack point is extended incrementally until all nodes in the network are intersected and subsequently deleted. The lifeline attack mode uses the inverse route factor ($1/q$) to generate spatially- (i.e., Euclidean) and topologically-integrated measures of separation distance from an attack point. Buffer impact regions are scaled around each lifeline infrastructure element using inverse route factor as a width function. Elements close in proximity to an attack point, but far-removed in terms of path or network distance have a proportionately smaller impact

region. Elements close in both Euclidean distance and path distance have a high buffer width.

5.2.8 Lifeline Attack Resistance with and without Topology Control

When compared with Proximal topologies, the lifeline-based attacks showed average performance which appeared more resistant than similar attacks on Proximal topologies. Investigation of f variation across simulations, however, showed high variability in the lifeline attack mode with high frequencies of both low and high percolation thresholds. This behavior was attributed to the fringe nodes which exist at the points most distant from each lifeline element. These nodes were located either just inside or just outside the buffer impact regions. These nodes create a “robust yet fragile” condition where they are responsible for both low and high resistance to percolation.

Topology control was applied to reactively resist percolation and mitigate the high variation. It was shown that topology control can effectively maintain network connectivity and despite the loss of nodes in the network, maintain relative magnitudes of graph-theoretic measures such as mean shortest path near unperturbed levels. Topology control does not recover loss of coverage area as nodes are deleted, however. Further, it is spatially dependent on the critical density of nodes deployed. Following from percolation theory, at the point critical density drops below a certain level, the probability of topology control maintaining a contiguous connected graph is low.

5.2.9 Critical Percolation Density for Sensor Networks

Other frameworks that demonstrate Power-law and “robust yet fragile” behavior were discussed, in particular Highly Optimized Tolerance (HOT). Based in percolation modeling on 2d-lattices, HOT explains robust resistance to failure for events in which systems were designed to handle, but poor performance for extreme perturbations.

To explain the theoretical basis for the critical density condition and the investigation of redundant, non-participating sensor network elements as a strategy for insuring critical density and predicting network survivability was discussed..

5.2.10 Balance of Self-Organization and Topology Control

We defined the competing problem of self-organization and topology control for sensor networks and offered modes of Geographic Automata (GA) to provide spatial emergent behavior – allowing vulnerability and risk to be managed as a spatial quantity and allowing (near optimal) topologies to be formed based on considerations of only their local neighborhood.

5.3 Principal Conclusions

Three principal conclusions are made as a result of this research.

The creation of spatially-derived topologies, from the Proximal topology generator and Lifeline-based topology generator, exhibited unique properties characteristic of their respective spatial network evolution processes. Aspatial topologies that achieve smallworld efficiency (i.e., low separation distance) and resistance to random attack through the presence of high-degree hubs are also susceptible to targeted attack.

Spatial topologies, constrained by planarity or dependency requirements exhibit similar “robust yet fragile” behavior, but because of their spatial rather than topological organization. Proximal topologies achieved survivability from a diversity of long and short Euclidean distance connections, while lifeline topologies lack such survivability because of their co-location and dependency relationship with the independent infrastructure network.

Sensor networks deployed around infrastructure are particularly vulnerable to disruption caused in the independent sensor network. The independent infrastructure topology constrains both the placement of nodes and the connections possible between sensors. Without active network topology control, these dependent networks are not survivable and their risk dominates any derived vulnerability inherited from the independent infrastructure network.

Topology control is surprisingly effective at maintaining connectivity, providing the critical density of sensors is high-enough and that sufficient consideration is paid to service area limiting factors such as line-of-sight, obscuration, etc.

5.4 Recommendations for Future Work

This research has contributed to the understanding vulnerability of dependent sensor networks, but many extensions to this work and new opportunities remain.

The discrete modeling of network flows, both in the sensor network (e.g., packets) and in the infrastructure network (e.g., water, gas flow), either through continuous time approximation or through discrete-event simulation, would provide a more holistic view of vulnerability. The research of Albert et. al (2004) on the structural vulnerability of the North American power grid considered the electrical loads and utilization of nodes in addition to topologic structure. Flows were modeled using simple application of Kirchoff's laws. Although their analyses were telling in demonstrating the effects of cascading failures on non-redundant, transmission infrastructure, new research has revealed that power engineering considerations (e.g., transformer load cycles and switch controllers) must be considered to realistically model cascading electrical failures (Holmgren 2005).

Engineering considerations of sensor network hardware (e.g., communications interfaces) contributes to the topologic forms and consequently the survivability behavior of the network (Li et al. 2004). Network simulation packages such as OPNET (OPNET 2005) can explicitly model the interplay of topology, routing, and network performance. From this standpoint, network survivability can be extended from coverage or graph-theoretic measures used in this research to actual measures of throughput, availability and QoS (Desai et al. 2005). The realistic modeling of infrastructure network flows combined with protocol-based network simulation in the

sensor network represents a difficult challenge but a necessary one for integrated modeling infrastructure and dependent sensor network topologies.

Wider application of spatial analysis would significantly extend this research. Just as packages such as OPNET would provide for explicit modeling of network communications, high-level geometric and network models available in ESRI ArcGIS would allow for route modeling, tracing, and explicit service area analysis of infrastructure sensor networks. Because the topology generators and attack modes developed in this research were created from within a GIS environment, this extension is straightforward.

The spatial distribution of impacted areas from the lifeline attack mode presented in Sections 3.6.1 and 3.6.3 require some form of calibration from actual natural and man-made disaster events. O'Rourke has developed infrastructure damage estimation techniques based on point-source disruptions (O'Rourke et al. 1999). For the 1994 Los Angeles Northridge Earthquake, point damage locations were correlated with peak ground acceleration measurements to create a lifeline damage profile with which the extent of disruption could be estimated. These techniques could be adapted and expanded for infrastructure sensor network models to create more calibrated spatial distributions.

6 Appendix A: Properties of the Pareto distribution

The moments of order ν about the origin of the Pareto pdf are:

$$m_\nu = \int_0^\infty x^\nu f_X(x) dx = \int_0^\infty x^\nu ab^a x^{-(a+1)} dx \quad (\text{A-1})$$

For $\nu = 1$, the mean is,

$$E[x] = \int_0^\infty x f_X(x) dx = \frac{ab}{a-1} \quad (\text{A-2})$$

The central moments of order ν of the Pareto pdf are,

$$m'_\nu = \int_0^\infty (x - E[x])^\nu f_X(x) dx \quad (\text{A-3})$$

For $\nu = 2$, the variance is,

$$Var[x] = \int_0^\infty (x - E[x])^2 f_X(x) dx = \frac{ab^2}{(a-1)^2(a-2)} \quad (\text{A-4})$$

Low-order moments about the origin and central moments are shown in Table A-1.

Table A-1: Low-order moments of the Pareto distribution.⁴

| ORDER | MOMENT ABOUT ORIGIN | CENTRAL MOMENT |
|-------|---------------------|--|
| 1 | $\frac{ab}{a-1}$ | – |
| 2 | $\frac{ab^2}{a-2}$ | $\frac{ab^2}{(a-1)^2(a-2)}$ |
| 3 | $\frac{ab^3}{a-3}$ | $\frac{2a(a+1)b^3}{(a-1)^3(a-2)(a-3)}$ |
| 4 | $\frac{ab^4}{a-4}$ | $\frac{3a(3a^3+a+2)b^4}{(a-1)^4(a-2)(a-3)(a-4)}$ |
| n | $\frac{ab^n}{a-n}$ | |

The moments are only defined for $b > n$; this means that the Moment generating Function is not defined. From the moments of Table A-1, the skewness is,

$$\gamma_1 = \sqrt{\frac{a-2}{a}} \left(\frac{2(a+1)}{(a-3)} \right) \quad (\text{A-5})$$

and the kurtosis is,

$$\gamma_2 = \left(\frac{6(a^3 + a^2 - 6a - 2)}{a(a-3)(a-4)} \right) \quad (\text{A-6})$$

⁴ von Seggern, D. CRC Standard Curves and Surfaces. Boca Raton, FL: CRC Press, p. 252, 1993; Eric W. Weisstein. "Pareto Distribution." From MathWorld--A Wolfram Web Resource. <http://mathworld.wolfram.com/ParetoDistribution.html>; and Johnson, N.I. and S. Kotz, *Continuous Univariate Distributions*, v.1, Houghton Mifflin, 1970

The median of the Pareto distribution is

$$x_{0.5} = b^{\frac{1}{a}}\sqrt{2} \quad (\text{A-7})$$

and the mode is,

$$\hat{x} = b \quad (\text{A-8})$$

The entropy of the distribution is,

$$H = \ln\left(\frac{a}{b}\right) - \frac{1}{a} - 1 \quad (\text{A-9})$$

7 Bibliography

- Albert, I. (2005, February 2005). "PyGraphlib." Retrieved February 2005, from <http://pygraphlib.sourceforge.org>.
- Albert, R., I. Albert, et al. (2004). "Structural Vulnerability of the North American Power Grid."
- Albert, R., I. Albert, et al. (2004). "Structural Vulnerability of the North American Power Grid." Phys. Rev. E **69**.
- Albert, R. and A.-L. Barabasi (2000). "Topology of Evolving Networks: Local Events and Universality." Physical Review Letters **85**: 5234-5237.
- Albert, R., H. Jeong, et al. (2000). "Attack and error tolerance of complex networks." Nature **406**: 378.
- Baecher, G. B. and J. T. Christian (2003). Reliability and statistics in geotechnical engineering. Chichester, West Sussex, England; Hoboken, NJ, J. Wiley.
- Barabási, A.-L. (2002). Linked: the new science of networks. Cambridge, Mass., Perseus Pub.
- Barabási, A.-L. and R. Albert (1999). "Emergence of scaling in random networks." Science **286**: 509-512.
- Baran, P. (1964). Introduction to Distributed Communications Networks, RAND Corporation.

- Bhandari, R. (1999). Survivable networks: algorithms for diverse routing. Boston, Kluwer Academic Publishers.
- Black, W. R. (2003). Transportation: a geographical analysis. New York, Guilford Press.
- Bollobas, B. and O. Riordan (2005). "A short proof of the Harris-Kesten Theorem." Bulletin of the London Mathematical Society.
- Bornholdt, S. and H. G. Schuster, Eds. (2003). Handbook of graphs and networks: from the genome to the internet. Weinheim, Wiley-VCH.
- Bu, T. and D. Towsley (2002). On Distinguishing between Internet Power Law Topology Generators. IEEE INFOCOM 2002, IEEE.
- Bush, B. W., C. R. Files, et al. (2001). Empirical Characterization of Infrastructure Networks, Los Alamos National Laboratory.
- Carlson, J. and J. Doyle (2000). "Highly Optimized Tolerance: Robustness and Design of Complex Systems." Physical Review Letters **84**(11): 2529-2532.
- Chung, F., P. Erdos, et al. (1998). Erdos on graphs: his legacy of unsolved problems. Wellesley, Mass, AK Peters.
- CIAO (1997). Critical Foundations: Protecting America's Infrastructures. Washington, DC, US Department of Commerce.
- Dantzig, G., R. Fulkerson, et al. (1954). "Solution of a large-scale traveling salesman problem." Operations Research **2**: 393-410.

- Davis, C., I. Smolyaninov, et al. (2003). "Flexible optical high data rate wireless links and networks." IEEE Communications Magazine(3).
- Desai, A. (2003). Dynamic Topology Control of Free Space Optical Networks.
Department of Electrical and Computer Engineering. College Park, MD,
University of Maryland. **Master of Science Thesis**.
- Desai, A., E. Baskaran, et al. (2005). Modeling and Simulation of Point-to-point Broadband Wireless Networks. OPNETWORK 2005, Washington, D.C., OPNET, Inc.
- Dorogovtisev, S. N. and J. F. F. Mendes (2003). Evolution of networks: from biological nets to the Internet and WWW. Oxford; New York, Oxford University Press.
- ESRI (2005). ArcGIS 9 Geoprocessing Framework. Redlands, CA.
- Faloutsos, M., P. Faloutsos, et al. (1999). "On power-law relationships of the Internet topology." Computer Communications Review **29**: 251.
- Gastner, M. and M. Newman (2004). "Shape and efficiency in spatial distribution networks." Phys. Rev. Lett.
- Gastner, M. and M. Newman (2004). "The Spatial Structure of Networks." Phys. Rev. E.
- Gorman, S. and R. Kulkarni (2004). "Spatial small worlds: new geographic patterns for an information economy." Environment and Planning B: Planning and Design **vol. 31**: pp. 273-296.

- Gorman, S., L. Schintler, et al. (2004). "The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure." Journal of Contingencies and Crisis Management **Vol. 12(2)**: pp. 48-63.
- Gupta, P. and P. R. Kumar (1999). Capacity of wireless networks., University of Illinois, Urbana-Champaign.
- Gurumohan, G. and J. Hui (2003). Topology Design for Free Space Optical Networks. Computer Communications and Networks 2003, Chicago, IL, IEEE.
- Holmgren, Å. (2005). Risk Analysis of Infrastructure Systems: Electrical Case. CREATE Homeland Security Center. Los Angeles, CA, University of Southern California: 21.
- Holmgren, Å. and T. Thedéen (2003). Riskanalys (Risk Analysis). Riskier i tekniska system (Risk in Technical Systems). G. Grimvall, P. Jacobsson and T. Thedéen. Studentlitteratur, Stockholm.
- Kansky, K. J. (1963). Structure of Transportation Networks: Relationships Between Network Geometry and Regional Characteristics. Department of Geography Research Paper #84, University of Chicago.
- Li, L., D. Alderson, et al. (2004). A First-Principles Approach to Understanding the Internet's Router-level Topology. SIGCOMM '04, Portland, OR, ACM.
- Liu, F., U. Vishkin, et al. (2005). Bootstrapping Free-Space Optical Networks. 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05).

- Mendes, J. F. F., R. Pastor-Satorras, et al. (2004). "Virtual Round Table on ten leading questions for network research." European Physics Journal B **38**: 143-145.
- Milgram, S. (1967). "The Small World Problem." Psychology Today(5): pp 60 - 67.
- Milner, S., C. Davis, et al. (2003). SENSORS: Optical Wireless Sensor Networks for Critical Infrastructre Surveillance (0330225). Arlington, VA, National Science Foundation.
- Milner, S., A. Desai, et al. (2005). "Self-organizing broadband hybrid wireless networks." J. Optical Networking **4**: 446-459.
- Newman, M. (2005). "Power laws, Paerto distributions and Zipfs law." Contemporary Physics(46): 323-351.
- Newman, M. E. J. (2003). "The structure and function of complex networks." SIAM Review **45**: 167-256.
- O'Rourke, T. (1993). Prospectus for Lifelines and Infrastructure Research. The Art and Science of Structural Engineering: Proceedings of the Symposium Honoring William J. Hall, University of Illinois, Urbana-Champaign, Prentice Hall.
- O'Rourke, T., S. Toprak, et al. (1999). GIS Characterization of the Los Angeles Water Supply, Earthquake Effects, and Pipeline Damage. Research Progress and Accomplishments 1997-1999: Multidisciplinary Center for Earthquake Engineering Research. Buffalo, New York: 44-53.

- OPNET. (2005). "Communication network modeling and simulation software." June 2005, from <http://www.opnet.com>.
- Python. (2005). "Python is an interpreted, interactive, object-oriented programming language." Retrieved May 2005, from <http://www.python.org>.
- Renno, J., M. Tunncliffe, et al. (2001). Simulation of a Video Surveillance Network Using Remote Intelligent Security Cameras. ICN 2001: First International Conference on Networking, Part II, Colmar, France., Springer-Verlag.
- Stauffer, D. and A. Aharony (1994). Introduction to percolation theory. London; Bristol, PA, Taylor & Francis.
- Watts, D. J. and S. H. Strogatz (1998). "Collective dynamics of small-world networks." Nature **393**: 440.
- West, D. B. (1996). Introduction to graph theory. Upper Saddle River, NJ, Prentice Hall.
- Wilson, R. J. (1985). Introduction to graph theory. Harlow, Essex, England, Longman.
- Yook, S.-H., H. Jeong, et al. (2002). "Modeling the Internet's large-scale topology." Proceedings of the National Academy of Sciences: 13382-13386.
- Zeiler, M. (1999). Modeling Our World: The ESRI Guide to Geodatabase Design. Redlands, CA USA, Environmental Systems Research Institute Press.

Zhuang, J., M. Casey, et al. (2004). Multi-Objective Optimization Techniques in Topology Control of Free Space Optical Networks. Proceedings of IEEE MILCOM 2004, Monterey, CA.