VULNERABILITY OF NETWORKS AGAINST RANK ORDERED INDEPENDENT LINK FAILURES

by

Serdar Çolak

B.S., Civil Engineering, Boğaziçi University, 2008

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Civil Engineering

Boğaziçi University

2010

ACKNOWLEDGEMENTS

I would like to thank my instructors Prof. Ali Rana Atılgan and Assoc. Prof. Hilmi Luş for helping me to this new area of research and being incredibly helpful, my friends for their presence at times of need, and particularly my family, who have always been there to support me.

ABSTRACT

VULNERABILITY OF NETWORKS AGAINST RANK ORDERED INDEPENDENT LINK FAILURES

In this study, various random and regular networks are investigated and compared in terms of their vulnerabilities against independent but ordered failures. Upon the mathematical basis of graph theory, methods of analysis of the structure and topology of networks are investigated, and parameters such as shortest paths, cuts, and degree distributions dealing with connectivity patterns are analyzed. Moreover, probabilities and correlations between the connected elements of networks are defined, measured and compared. Using these parameters, centrality and betweenness measures are discussed as primary methods of ranking and used to rank these elements in terms of specific functions such as network performance and reliability. Failure scenarios based on these ranking methods are applied on ring structures, Erdos Renyi, scale free and small world networks as well as Istanbul's highway and rapid transit networks and Turkish railway network. The responses of these networks against these failures are shown to be related to their structural properties and topologies.

ÖZET

AĞLARIN SIRALANMIŞ BAĞIMSIZ BAĞ KOPMALARINA KARŞI KIRILGANLIĞI

Bu çalışmada, çeşitli düzensiz ve düzenli ağların bağımsız ancak sıralı bağ kırılmalarına karşı kırılganlıkları incelenmiş ve karşılaştırılmıştır. Grafik teorisinin matematiksel temeli üzerinden ağ yapıları ve topolojilerini analiz metodları incelenmiş, en kısa yollar, kesikler, ve bağ dağılımları gibi bağlantı desenleri ile ilgili parametreler analiz edilmiştir. Bunun üzerine, elemanlar arasındaki bağ olasılıkları ve bağlılaşımları belirlenmiş, ölçülmüş ve karşılaştırılmıştır. Bu parametreler kullanılarak, merkezlilik ve aradalık ölçütleri öncelikli sıralama yöntemleri olarak ele alınmış, ve ağ elemanlarını ağ güvenilirliği ve performansı gibi belirli fonksiyonlara göre sıralamada kullanılmıştır. Bu sıralama metodlarına dayanarak oluşturulan kopma senaryoları dairesel ağ yapıları, Erdos Renyi, ölçeksiz ve küçük dünya ağları ile birlikte, İstanbul otoyol ve hızlı ulaşım ağı ile Türkiye demiryolları ağı üzerine uygulanmıştır. Ağların bu kopmalara karşı tepkilerinin yapısal özellikleri ve topolojileri ile ilişkili olduğu gösterilmiştir.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS/ABBREVIATIONS

A	Adjacency matrix
a_{ij}	Adjacency matrix element in row i and column j
B	Incidence matrix
b_{ij}	Incidence matrix element in row i and column j
C	Clustering coefficient of the network
C_i	Clustering coefficient of node i
C_B^{sp}	Shortest path betweenness
C_B^{rw}	Random walk betweenness
c	A cycle
D	Diagonal degree matrix
$d(i)$	Degree of node i
d_i	i^{th} element of the degree sequence
E	Set of edges (links)
$E_{kk'}$	Unnormalized degree correlation matrix
$e(i)$	Number of edges between the neighbors of node i
F	Minimum cut set cardinality matrix
G	A graph or a network
G'	Subgraph
$g_i^{(st)}$	Number of shortest paths between s and t that pass through i
$g^{(st)}$	Number of shortest paths between s and t
$I^{(st)_i}$	Current passing through node i for source s and target t
K_n	A complete graph of order n
$\bar{k}_{nn}$	Average nearest neighbor degree
$\bar{k}_{nn}(k)$	Average nearest neighbor degree of nodes with degree k
L	Shortest path matrix
l_{ij}	Shortest path length between nodes i and j
$\bar{l}$	Average shortest path length
M	Markovian transition matrix
m	Number of edges in the graph, size

n	Number of nodes in the graph, order
n^i	Number of nodes in component i
$n^{(z)}$	Number of nodes in the zth shell of a tree network
n_k	Number of nodes with degree k
P_k	The degree distribution
$P(k'\|k)$	Conditional degree distribution
$P(k\|k', k'')$	Joint conditional degree distribution
p	Probability
p_n	Node failure probability
p_e	Edge failure probability
$R(G, s, V)$	All terminal reliability
$R(G, s, \{s, t\})$	Two terminal reliability for source s and target t
$R(G, s, \{s, t\}, p)$	Two terminal reliability for source s and target t and probability p
S	State of a network
s	Source-target vector
T	Normalized trip matrix
V	Set of vertices (nodes)
V_i^{st}	Voltage at node i for source s and target t
z	Shell of a tree network
δ_{ij}	The Kronecker delta
γ	The exponent of the power law distribution
ι	Identity matrix
$\mathcal{L}$	The Laplacian
φ_S	Binary connectivity function for state S
ρ	Set of edges that form a path
ρ_k	A path of length k

1. INTRODUCTION

The objective of this study simply is to investigate the infrastructure networks that surround us. A lot has changed in the last decade in the world, increased population and demand caused vast investments on infrastructures: people wanted to travel faster, clean water delivered to their faucets, electricity at their mountain cabins. Huge bridges were built, power lines were drawn to every corner and most of these demands were met. However the whole picture could be seen only after these needs were met: in every developed country, or city, infrastructures formed huge webs that became very difficult to manage. Traffic problems today can no longer be solved by only fixing problematic intersections, it was seen that the problems were only delayed to pop up in some other junction. Power shortages occur in a city only because some cables were damaged in another city a thousand miles away. Causes that would seem very minor at first sight can lead to cascading failures and unforeseen damage, as these networks grew out of control. I believe we are at that time where these infrastructure networks are in need of detailed analysis and reconfiguration for better performance in terms of efficiency, safety, and fulfilling their purpose; because everything that makes the modern society civilized is based on these infrastructures. This problem obviously is not easy to solve, since there is no specific profession that could address it completely: a mathematical theory is of course helpful but is not enough by itself; a dynamics approach is also very insightful but does not constitute a comprehensive solution.

It is widely accepted that the interest in network science begins with Euler's proof of the Königsberg bridge problem using walks on a simple connected graph. From then on, the interest in the structure of networks that are abundant in life rapidly grew.

The mathematical analysis of graphs, or networks, is the root of graph theory [1, 2, 3, 5]. Very recently, along with the incredible growth of the world wide web, complex networks have been under investigation in terms of many aspects like scaling [6], epidemic spreading [9], dynamics [11, 10], statistical mechanics [26], navigation [27], evolution [25], and many others. The primary concern of this study however is about the vulnerability of complex networks against different failure scenarios. This problem has also been worked on heavily.

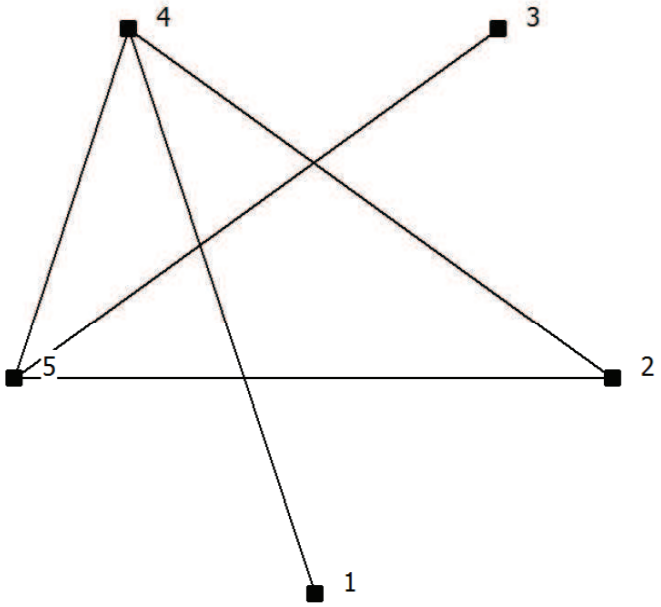

Figure 1.1. A graph G with 5 nodes and 5 edges, with $V = \{1, 2, 3, 4, 5\}$ and $E = \{(1, 4), (2, 4), (2, 5), (3, 5), (4, 5)\}$.

Some works directly address the theoretical networks or common models [45, 46, 47, 48], whereas some others directly investigate infrastruceture networks [49, 50, 51], like power grids [52, 53, 54, 55], gas networks [56] or even metabolic networks [57]. In this study, transportation networks are analyzed from a more general point of view, also an intriguing subject for vulnerability analysis [58, 59].

1.1. Graph Theory

A *graph* or *network* is a pair of disjoint sets $G = (V, E)$ where the elements of V are the *vertices* or *nodes* of the graph G, and the elements of E are its *edges* or *links*. The elements of E are unordered 2 element subsets of V. An edge joining the vertices x and y is denoted by (x, y). If $(x, y) \in E$, then x and y are *adjacent* or *neighboring* vertices of G and the vertices x and y are *incident* with the edge (x, y).

A graph can be either *directed* or *undirected*, and either *weighted* or *unweighted*. A directed graph constitutes directionality on its edges, that is, the edge (x, y) allows passage from x to y, but not from y to x. In an undirected graph, edges are bidirectional, passage is

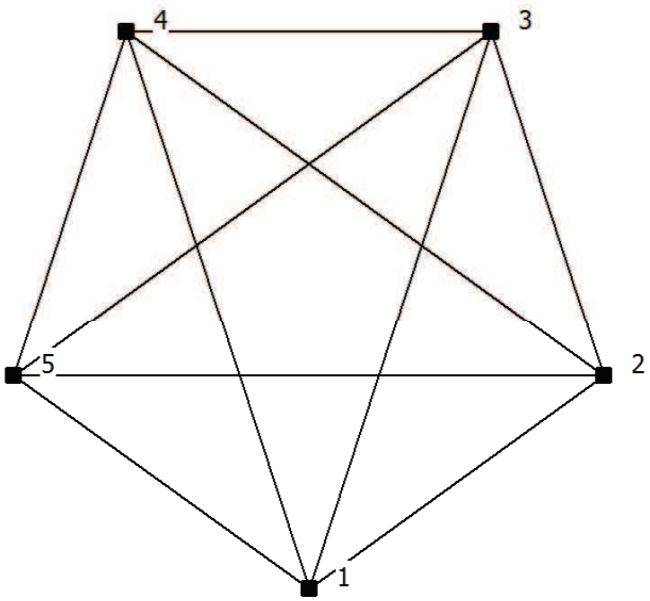

Figure 1.2. The complete network with 5 nodes, K_5. One path ρ on this network has $V_\rho = \{1, 2, 5, 4\}$ and $E_\rho = \{(1, 2), (2, 5), (5, 4)\}$. A cycle c would connect back to its origin, thus would be $c = \{V_c, E_c\}$ with $V_c = \{1, 2, 5, 4, 1\}$ and $E_c = \{(1, 2), (2, 5), (5, 4), (4, 1)\}$.

permitted along both directions. A *weighted* graph has a value that represents the cost, or the resistance associated with travelling along each edge.

The number of vertices of a graph G is its *order*, denoted by n; and the number of edges is its *size* denoted by m.

If all the vertices of G are pair-wise adjacent, then G is *complete*. A complete graph on n vertices is a K_n, for example a K_3 is a triangle. In K_n, every pair of vertices are adjacent. [1]

If $V' \subseteq V$ and $E' \subseteq E$, then G' is a subgraph of G, written as $G' \subseteq G$. A subgraph $G' \subseteq G$ is a spanning subgraph of G if V' spans all of G, or similarly, if $V' = V$.

A *path* is a non-empty graph $\rho = (V, E)$ of the form $V_\rho = \{x_0, x_1, \ldots, x_k\}$, $E_\rho = \{(x_0, x_1), (x_1, x_2), \ldots, (x_{k-1}, x_k)\}$ where the x_i are all distinct. The vertices x_0 and x_k are

called the *initial* and the *terminal* vertex, respectively. The initial and terminal vertices are linked by ρ and are called its *endvertices*. The number of edges of a path is its *length*, and a path of length k is denoted by ρ_k. In paths, k is allowed to be zero, thus $\rho_0 = K_1$. If $\rho = \{(x_0, x_1) \dots (x_{k-2}, x_{k-1})\}$ is a path and $k \geq 3$, then the graph $c = \rho \cup \{(x_{k-1}, x_0)\}$ is called a *cycle*.

Independence is a term often used in connection with vertices, edges and paths of a graph. A set of vertices (edges) is *independent* if no two elements of it are adjacent. A set of paths is independent if for any two paths each vertex belonging to both paths is an endvertex of both. Therefore ρ^i and ρ^j are independent if and only if $V(\rho^i) \cap V(\rho^j) = \{x, y\}$ whenever $i \neq j$.

A non-empty graph G is called *connected* if any two of its vertices are linked by a path in G. A maximal connected, non-empty subgraph of $G = (V, E)$ is called a *component* of G.

The incidence matrix $B = (b_{ij})_{n \times m}$ of a graph $G = (V, E)$ with $V = \{v_1, \cdots, v_n\}$ and $E = \{e_1, \cdots, e_m\}$ is defined by:

$$b_{ij} = \begin{cases} 1 & \text{if } v_i \text{ is the initial vertex of the unidirectional edge } e_j, \\ -1 & \text{if } v_i \text{ is the terminal vertex of the unidirectional edge } e_j, \\ 1 & \text{if } v_i \text{ is the endvertex of the bidirectional edge } e_j, \\ 0 & \text{otherwise.} \end{cases} \tag{1.1}$$

The incidence matrix B of the network in Figure 1.1 is

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

The adjacency matrix $A = (a_{ij})_{n\times n}$ of G, which constitutes its more fundamental mathematical representation, is defined by:

$$a_{ij} = \begin{cases} 1 & \text{if } v_i v_j \in E, \\ 0 & \text{otherwise.} \end{cases} \tag{1.2}$$

The adjacency matrix of the network in Figure 1.1 is

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

The number of edges incident on a vertex i in G is respresented by $d(i)$, namely the *degree* of a node. The nodes in the network in Figure 1.1 have degrees $1, 2, 1, 3, 3$ respectively. The degree vector of an undirected network can be obtained by summing the rows or the columns of the adjacency matrix:

$$\sum_j A_{ij} = d\,(i)\,. \tag{1.3}$$

The adjacency matrix A and the incidence matrix B are related by the simple formula $BB^T = D - A$, where D is a nxn diagonal matrix where $D_{ii} = d(v_i)$.

The distance l_{ij} in G of two vertices i and j is the length of a shortest $i - j$ path in G; if no such path exists, $l_{ij} = \infty$. The path with the shortest length between two vertices i and j is called the *shortest path*. [5]

For the network in Figure 1.1, the matrix consisting of the lengths of the shortest paths

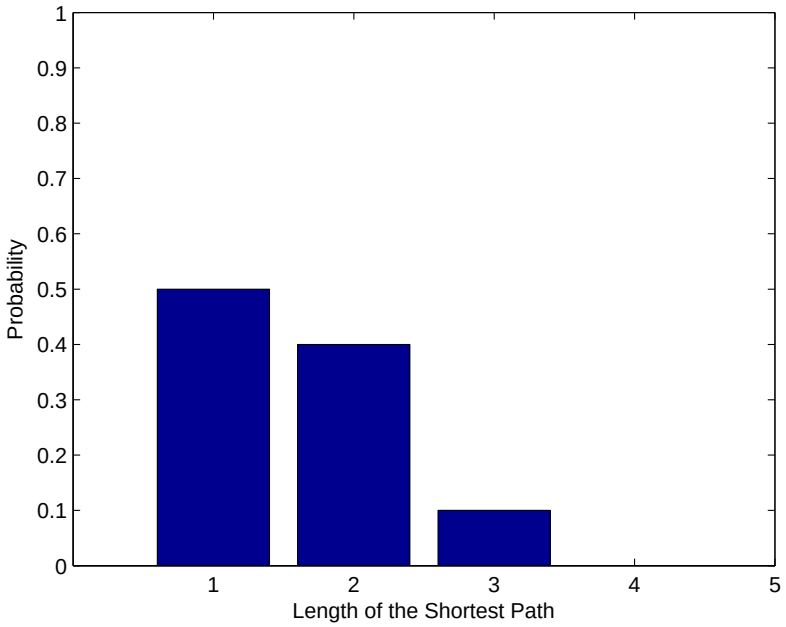

Figure 1.3. The probability distribution of the shortest path lengths of the network depicted in Figure 1.1.

between node pairs is:

$$L = \begin{pmatrix} 0 & 2 & 3 & 1 & 2 \\ 2 & 0 & 2 & 1 & 1 \\ 3 & 2 & 0 & 2 & 1 \\ 1 & 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 1 & 0 \end{pmatrix}$$

The distribution of the shortest paths can also be extracted for further information, as in Figure 1.3.

A set of edges whose removal disconnects nodes i and j is a *cut set*. A $minimal$ cut is the set with minimum cardinality, i.e. the minimum number of edges whose removal disconnects the nodes. A very important theorem in graph theory is developed by Menger[5], which states that the cardinality of the minimum cut set between two distinct nodes is equal to the maximum number of edge-independent paths between these nodes. The minimum cut

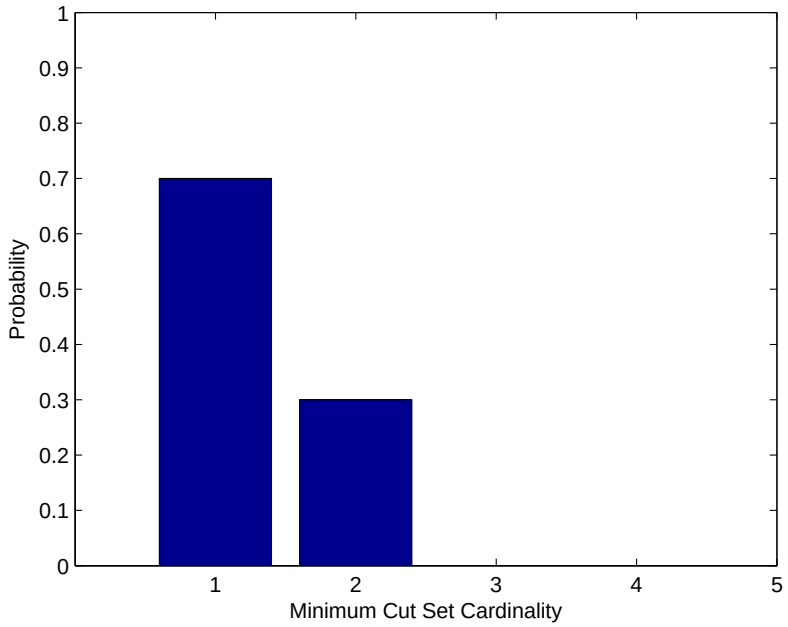

Figure 1.4. The probability distribution of the cardinalities of the minimum cut sets

matrix of the network in Figure 1.1 is,

$$F = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 2 & 1 & 0 & 2 \\ 1 & 2 & 1 & 2 & 0 \end{pmatrix}$$

The number of nodes with degree k is denoted as n_k. The degree distribution is the probability distribution of the degrees, and the probability function indicating the probability of encountering a node with degree k is denoted as $P(k)$ and can be found by

$$P(k) = \frac{n_k}{n}. \tag{1.4}$$

The degree distribution of the network in Figure 1.1 is shown in Figure 1.5.

The matrix $D - A$ is also referred to as the $Laplacian$ of a network. For a connected

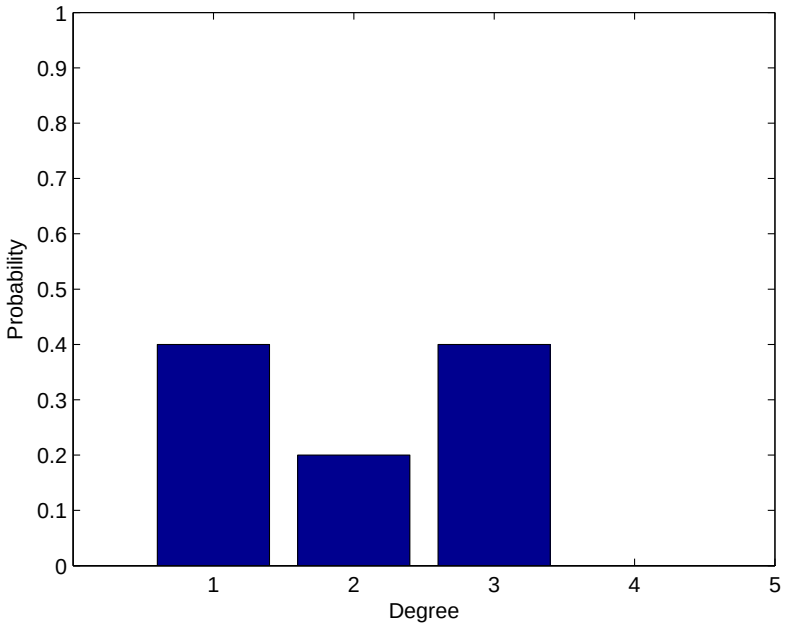

Figure 1.5. The degree distribution of the graph in Figure 2.1

network, the Laplacian has rank $n-1$, and therefore is not invertible. It can be noticed that all rows and columns of the Laplacian sum to zero, which also proves its singularity.

For the network in Figure 1.1, the Laplacian is as follows:

$$\mathcal{L} = \begin{pmatrix} 1 & 0 & 0 & -1 & 0 \\ 0 & 2 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 & -1 \\ -1 & -1 & 0 & 3 & -1 \\ 0 & -1 & -1 & -1 & 3 \end{pmatrix}.$$

2. CORRELATIONS IN NETWORKS

The connections in a network are prone to containing correlations, in the sense that certain nodes may tend to be connected, or stay disconnected. Most of the time these correlations are non-trivial, but they have a great impact on the behaviour of a network, since they define the conditions of the network's connectivity. These correlations can be categorized as *degree, two nodes* and *three nodes* correlations. [6]

2.1. Degree Correlations

Degree correlations look for connectivity relationships between degree values, using the degree distribution $P(k)$. Therefore they are primarily concerned with the conditional probabilities of a node of degree k being connected to a node of degree k', $P(k'|k)$.

The symmetric matrix $E_{kk'}$ can be constructed, to act as a basis upon which the conditional probabilities can be obtained. Off-diagonal elements of $E_{kk'}$ are the number of edges that connect a node of degree k to a node of degree k'. The diagonal elements are equal to twice the number of edges between two nodes of degree k. This matrix satisfies the following equations:

$$\sum_{k'} E_{kk'} = kn_k, \tag{2.1}$$

$$\sum_{k,k'} E_{kk'} = \bar{k}n. \tag{2.2}$$

Using these identities, the conditional probabilities can be written as,

$$P(k'|k) = \frac{E_{kk'}}{kn_k}. \tag{2.3}$$

The $E_{kk'}$ matrix of the network in Figure 1.1 is,

$$E_{kk'} = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 2 \\ 2 & 2 & 2 \end{pmatrix}.$$

When every row of $E_{kk'}$ is divided by the product of the corresponding degree and the number of nodes with that degree, $P\left(k'|k\right)$ is obtained:

$$P\left(k'|k\right) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1/3 & 1/3 & 1/3 \end{pmatrix}.$$

The result shows that for this network, there is a one third possibility of a node with degree three being connected to a node with degree one, two or three.

Degree correlations are useful in a theoretical sense, but are not very representative for the analysis of a single network, since they rely heavily on statistical data. Therefore other empirical correlation measures are more commonly used. [9]

2.2. Two Nodes Correlations

Also called the *average nearest neighbor degree*, $\bar{k}_{nn}\left(k\right)$, of nodes of degree k, two nodes correlations in a network [6] can be calculated by

$$\bar{k}_{nn}\left(k\right) = \sum_{k'} k' P\left(k'|k\right). \tag{2.4}$$

For the network in Figure 1.1, the average nearest neighbor degree is,

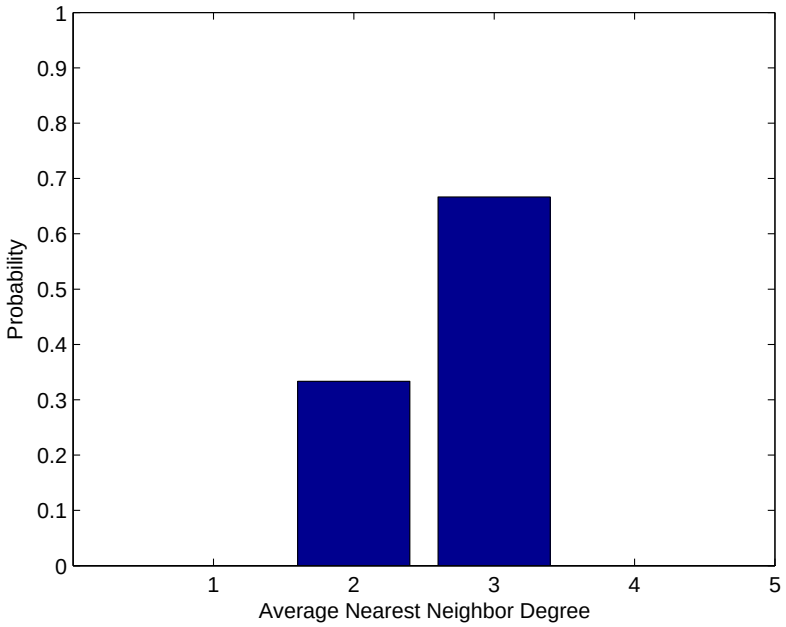

Figure 2.1. The probability distribution of the average nearest neighbor degree of the network in Figure 1.1

$$\bar{k}_{nn}(k) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1/3 & 1/3 & 1/3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \\ 2 \end{pmatrix}$$

Correlated networks exhibit two possible behaviours in terms of their average nearest neighbor degrees: $\bar{k}_{nn}(k)$ either increases or decreases with k. The increasing trend suggests that similar degree nodes are connected, networks with this behaviour are called *assortative* networks. The decreasing trend means that nodes tend to connect to other nodes that are not similar, as in the case where higher degree nodes are preferentially connected to low degree nodes, and vice versa. This sort of networks are called *disassortative* networks. If the average nearest neighbor degree is independent of k, then there is an absence of two nodes correlations. [7, 8, 10] Figure 2.2 depicts this relationship for the network in Figure 1.1.

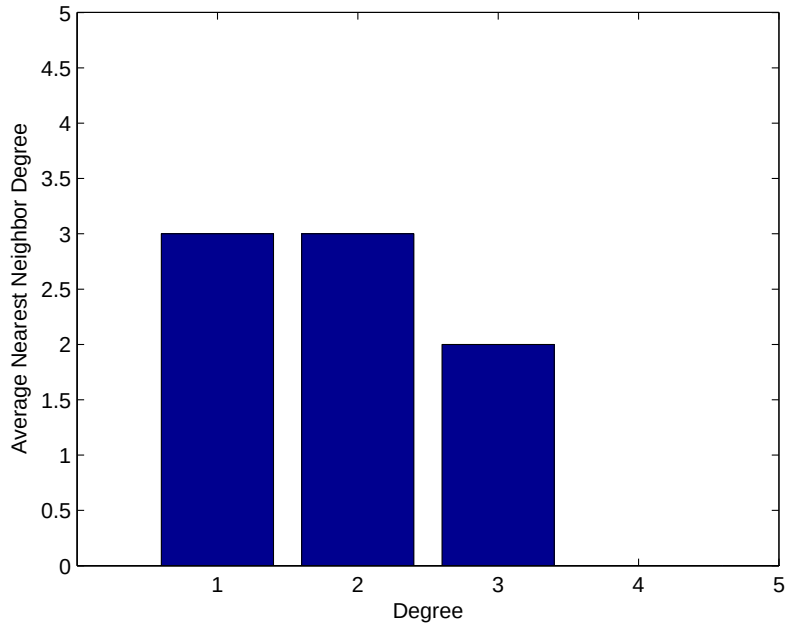

Figure 2.2. The graph of $\bar{k}_{nn}(k)$ versus k, a measure of the assortativitiy of the network in Figure 1.1

2.3. Three Nodes Correlations

As one might follow from two nodes correlations, the relationship between three nodes can be obtained by using the joint conditional probability $P(k|k', k'')$. However the statistical issues are only magnified in this method, hence other assessments are preferred.

$Clustering$ in a network is a measure of the probability of two adjacent nodes also sharing a neighbor. Under these circumstances the two nodes and their common neighbor form a triangle, the complete graph with three nodes, i.e. K_3.

Watts and Strogatz have proposed [11] a local measure for clustering, called the *clustering coefficient*, which is the ratio of the number of edges e_i between the k_i many neighbors of node i to the number of edges between these neighbors if they were to form a complete graph between them. The mathematical representation of the parameter is,

$$C_i = \frac{2e(i)}{d(i) \times (d(i) - 1)}. \tag{2.5}$$

Another way of calculating the clustering coefficient is by counting the number of triangles in the network [6]:

$$C = \frac{3 * \text{number of triangles}}{\text{number of triplets}}. \tag{2.6}$$

The clustering coefficient of node 4 in Figure 1.1 is pictured in Figure 2.3. The neighbors of node 4 are nodes 1, 2 and 5. In the subgraph consisting of these three nodes there is only one edge, whereas a complete network consisting of these three nodes would actually have 3.

The clustering coefficient of the nodes and in the network in Figure 1.1 are

$$C_i = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1/3 \\ 1/3 \end{pmatrix},$$

and Figure 2.4 shows the distribution of these values.

The clustering coefficient of the network C is the average of the clustering coefficients of all nodes in the network.

$$C = 1/3.$$

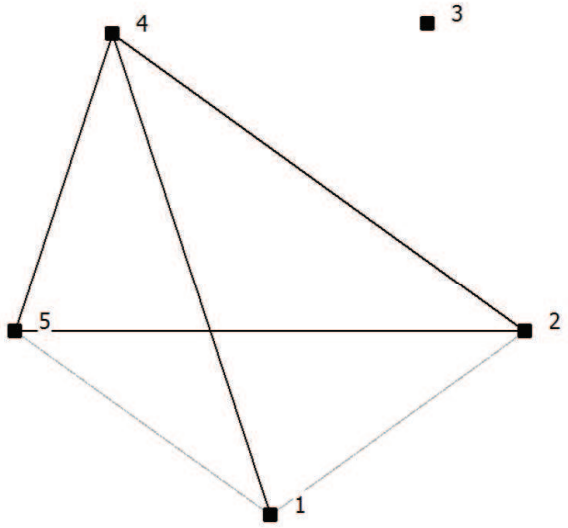

Figure 2.3. The neighborhood and the edges present (dark) and edges not present (light) for node 4 of the network depicted in Figure 1.1

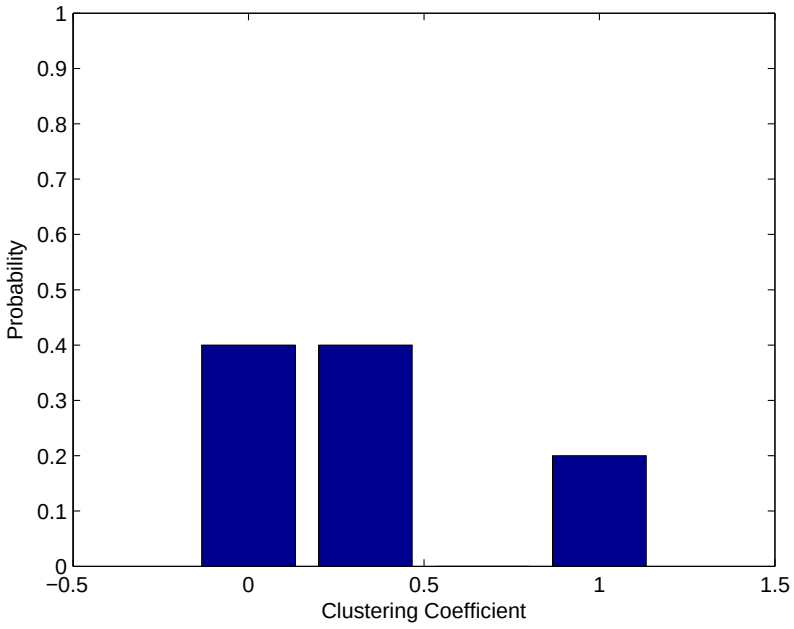

Figure 2.4. The probability distribution of the clustering coefficient of the network depicted in Figure 1.1

3. RANK ORDERING METHODS

Except for complete, or very uniformly designed ordered networks, two different elements of a network are often not equally important in terms of a desired criteria, such as performance or reliability. The difference is especially important in the case of the failure of these elements, since the expectation is that the network will react differently to the distinct failure of two different elements. Therefore it is obvious that in order to substantiate the network response against failures, the methods used in differentiating the elements of the network in terms of their importance, relevant to some function the network is required to fulfill, is a very important task. It is of course possible for both the attacker or the protector of the network to wish to use some other method by which the more critical elements can be found. These methods of ranking elements in terms of their importance for the network are generally referred to as *rank-ordering methods*.

It is important to note that not all ranking methods are based on the same network function. Some measure how critical an element is in terms of connectivity, some determine how crucial the element is in terms of the flow through the network. Therefore it is important to consider these rankings in their own context.

3.1. Degree

The simplest rank-ordering strategy for nodes is obviously the degree of that node, i.e. the number of links incident to a node for an undirected network. It is very straightforward to think that a node with the highest degree is of utmost importance to the network, and it sometimes is.

For specific network types, the differences in the distribution or the histogram of the node degrees shape the behavior of the network, and directly effect how reliable this ordering is. For a network where there is one node with a very high degree, and many other nodes with degrees about half as much, that node obviously is very important. In a larger network, there may be several nodes with degrees equal to that of the highest degree node

of the smaller network; however, they may not be as important since they are not unique. Moreover the other nodes may not have degrees half as much, but rather equal to 1. In other words, the statistical properties of the degree distribution is the key factor that determines how representative node degrees are in terms of their importance to the network. Therefore It is not very healthy to compare elements from different network contexts, therefore it is crucial to avoid directly comparing the degrees of nodes from networks with different sizes and degree distributions.

If the goal is to rank the nodes such that the failure of the first ranked element will cause the biggest damage on a network, one might tend to choose the node with the highest degree to attack. As a node fails, all edges incident to that node simultaneously fail, therefore all paths going into, out of, and through that node are no longer operational. Depending on the specific network, the results may be drastic, or the redundancies in the network may somehow cope with this failure. The idea behind the urge of attacking the node with the highest degree comes from the fact that, the failure of the node with the highest degree is actually the highest possible number of simultaneous link failures, since no other node is connected to as many edges. Therefore without any prior knowledge of the network topology, it is reasonable to expect that this method will cause the biggest damage, regardless of what we mean by damage. On the other hand, if we were to attack a number of low degree nodes, such that when the number of links that have failed is summed it is the same with that of the high degree node, how can we be sure that the damage caused is equal, or less, or more? Therefore it is important to identify the function of the network, and under what conditions the network at hand is no longer functional. Moreover, the network might still be functioning, but at an inadequate level.

Although very obvious for nodes, the degree measure is blurry for links. There isn't a similar measure for links, and complications arise if one devises a degree for a link using the degrees of the nodes at its both ends. Using the average of the degrees of the nodes is the first approach that comes to mind, and useful in terms of differentiating edges that lie between low degree nodes and those that connect high degree nodes. However by doing this one accepts that a link connecting nodes i and j with $d(i) = 1$ and $d(j) = 99$ and another link connecting nodes i' and j' with $d(i') = d(j') = 50$ have the same rank. From this point

on in this thesis, this method will be called *the average degree of a link*. Table 3.1 depicts these values for the links of the network in Figure 1.1.

Table 3.1. The average degrees of all edges of the network in Figure 1.1

Edge	Average Degree
(1,4)	2
(2,4)	2.5
(2,5)	2.5
(3,5)	2
(4,5)	3

3.2. Betweenness Centrality Measures

Over the years network researchers have introduced a large number of centrality indices, measures of the varying importance of the vertices in a network according to one criterion or another, with the goal of ranking the elements in terms of how *central* they are to the network. One centrality measure is *closeness*, which is the shortest-path distance between a vertex and all other vertices reachable from it. Closeness can be regarded as a measure of how long it will take information to spread from a given vertex to others in the network. The more complicated *betweenness centrality* measures aim to use specific paths between nodes and how frequently the network elements appear in these paths is the prime question. Betweenness, as one might guess, is a measure of the extent to which a vertex lies on the paths between others. [14, 15]

Many variations of the betweenness measurement exist, the difference being the properties of these paths that are taken into account. Some of these methods put an upper bound to the length of the paths, some only take the first k-many shortest paths, or all paths that are node or edge independent, that is, they do not share elements, into account. The two extremes of this choice would be only considering the optimal shortest paths, or conversely, totally overlooking the optimality criterion and considering all available paths. [16, 17]

If one was to think of types of paths lying on an axis, if the shortest path, symbolizing optimality, was to lie on one end of this axis; all available paths would probably lie on the other end, symbolizing redundancy. These two extremes are the two betweenness measures that will be considered in this work.

3.2.1. Shortest Path Betweenness Centrality

The shortest path betweenness of a vertex i is defined to be the fraction of shortest paths between pairs of vertices in a network that pass through i. If there is more than one shortest path between a given pair of vertices, then each such path is given equal weight such that the weights sum to one. $g_i^{(st)}$ denotes the number of shortest paths from vertex s to vertex t that pass through i and $g^{(st)}$ is the total number of shortest paths from s to t. Then the betweenness of vertex i is

$$C_B^{sp}(i) = \frac{\sum_{s<t} \left[g_i^{(st)} / g^{(st)} \right]}{\frac{1}{2} n(n-1)} \tag{3.1}$$

where n is the network size. [22]

The shortest path betweenness values are unnormalized in this sense, because every pair counts for one point. It can be normalized over the number of pairs in the network, which would be the case if an element were to lie on every shortest path on the network.

There are various methods of calculation of the shortest path betweenness, all share the same goal of finding $g_i^{(st)}$. One is by applying *Dijkstra's Algorithm* for all node pairs to obtain the shortest paths. For a given source and target node, Dijkstra's Algorithm works as follows:

1. Every node has a distance value assigned to it. The source node is assigned to 0 and all others to ∞. Mark the initial node as $current$, and all other nodes as $unvisited$.
2. Consider all unvisited neighbors of the current node, and calculate the distance to these nodes. For an unweighted network, all edges have weight 1. Therefore if a node i has

Table 3.2. The shortest paths between all node pairs for the network in Figure 1.1

Source - Target Pair	Shortest Path
$1, 2$	$(1, 4), (4, 2)$
$1, 3$	$(1, 4), (4, 5), (5, 3)$
$1, 4$	$(1, 4)$
$1, 5$	$(1, 4), (4, 5)$
$2, 3$	$(2, 5), (5, 3)$
$2, 4$	$(2, 4)$
$2, 5$	$(2, 5)$
$3, 4$	$(3, 5), (5, 4)$
$3, 5$	$(3, 5)$
$4, 5$	$(4, 5)$

distance 2, its neighbor j will have a distance value of 3. If the calculated distance value for a neighbor is smaller than the value previously assigned, then it replaces the older value. Otherwise the older and smaller value is kept. When all neighbors are considered, the node is marked as visited, not to be checked again.

3. Continue with the unvisited node with the smallest distance value, and repeat. Finish when all nodes are visited. The distance values are the shortest path distances to all nodes from the source node. [23]

By this process, every shortest path can be obtained, as in Table 3.2.1, and $g_i^{(st)}$ values can be calculated. The C_B values for all nodes and edges of the sample network in Figure 1.1 are below.

$$C_B^{sp}(i,j) = \begin{pmatrix} 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 4 \\ 4 & 2 & 0 & 0 & 4 \\ 0 & 2 & 4 & 4 & 0 \end{pmatrix}.$$

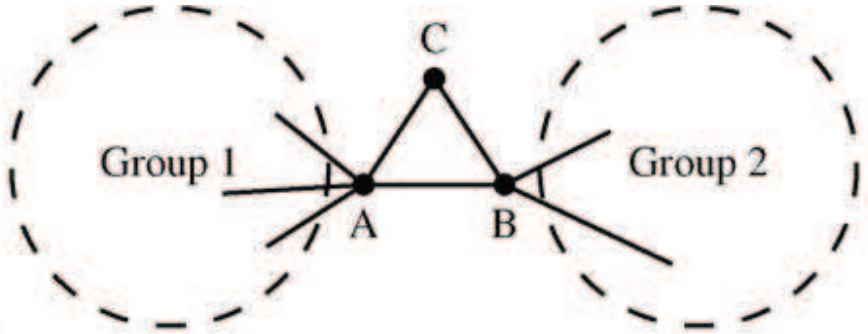

Figure 3.1. A sample network depicting the pitfalls of the shortest path betweenness. [22]

$$C_B^{sp}(i) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 3 \\ 3 \end{pmatrix}.$$

Shortest path betweenness can be thought of as a simulation in which there are $n-1$ agents at each node, each with the goal of reaching one of the remaining $n-1$ nodes using the shortest route possible. Suppose these agents move along the shortest path to their goal, and leave one dollar at each stop they make. The money gathered at that node after all agents reach their goal is the shortest path betweenness measure. It should be noted that this value is not normalized, as the shortest path betweenness is.

However, as this definition of betweenness emphasizes the shortest paths between vertices, there are some odd effects. For example if two relatively big components are only connected via two paths, one of length 1 and the other of length 2, all paths that start from one component and end in the other will use the shorter of these two paths. Therefore the longer path will have no shortest path running through it, thus a shortest path betweenness value of 0. However this longer path is obviously not as unimportant for the network as this measure suggests.

This issue can be seen from the network in Figure 3.1, where two large components are connected by two alternative paths. In this network, the shortest path betweenness values of node C and edges (A, C) and (B, C) are almost zero, since they do not get any contributions from the source target pairs that lie on opposite groups; all this emphasis is concentrated on edge (A, B) since it lies on every shortest path for such source target pairs.

3.2.2. Random Walk Betweenness

The random walk betweenness of a vertex i, by definition, is equal to the number of times that a random walk starting at s and ending at t passes through i along the way, averaged over all s and t.

A simple random walk means that a walker, at a specific site, chooses to move along on any one of the edges incident to that site with equal probability, without using any information about where this new site may lead to; and continues moving until it finds itself at the target. The simple random walk can be considered as a Markovian process, with a certain transition matrix: a probabilistic matrix whose element in row i and column j is the probability of moving to state i when at state j. [22]

Interestingly, when these walkers are electrons, this problem is very similar to a current flow problem in an electrical network where one unit of current is injected at a source node s and let run through the network where every edge has a unit resistance. This unit current is then collected at the target node t. The betweenness measure is concerned with the amount of current that passes every edge or node.

The length of the path chosen either by the walker or the electron has a positively linear relationship with the amount of resistance associated with that path, since more energy is required to walk a longer path. Therefore as the resistance increases, the amount of current along that path decreases in proportion.

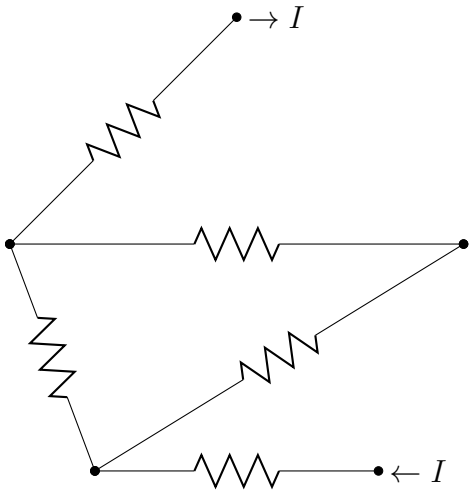

Figure 3.2. The electrical circuit analogy for the sample network of Figure 1.1, where the source node is 3 and target node is 1

In this analogy, Kirchoff's Law can be stated as,

$$\sum_j A_{ij} \left(V_i - V_j\right) = \delta_{is} - \delta_{it}, \tag{3.2}$$

for all i, where A_{ij} denote the elements of the adjacency matrix and δ_{ij} is the Kronecker delta:

$$\delta_{ij} = \begin{cases} 1 & \text{for } i = j, \\ 0 & \text{otherwise.} \end{cases} \tag{3.3}$$

In matrix form,

$$\begin{aligned} (D - A) \cdot V &= s, \\ V &= (D - A)^{-1} \cdot s. \end{aligned} \tag{3.4}$$

where the vector s is,

$$s_i = \begin{cases} +1 & \text{for } i = s, \\ -1 & \text{for } i = t, \\ 0 & \text{otherwise.} \end{cases} \tag{3.5}$$

In this context, the voltage matrix V can be calculated for every specific source-target pair. The voltage difference between two adjacent nodes would be equal to the current flowing along that edge, since every edge has unit resistance. [19]

Although easily stated, the greedy calculation of the random-walk betweenness measure is not very trivial, and it is an NP-complete problem. If one were to try to solve for the random walk betweenness values of a network by determining all paths between all node pairs, the process would take a considerable amount of time for even not-so-large networks, and it would not be feasible.

Many different types of walks can be created, based on various manipulations of the probabilities of choosing each of these options. A *simple random walk* is the most basic, and its transition matrix is

$$M_{ij} = \frac{A_{ij}}{k_j}, \tag{3.6}$$

where

$$k_j = \sum_i A_{ij}.$$

As a property, the powers of the transition matrix show the probability of starting at a specific site and ending up at that site after the number of steps as many as the power of the transition matrix. So for a walk starting at node s, the probability of being at node j after q steps is given by $\left[M^q\right]_{js}$. There are k_j many options ahead when the walker is at site y,

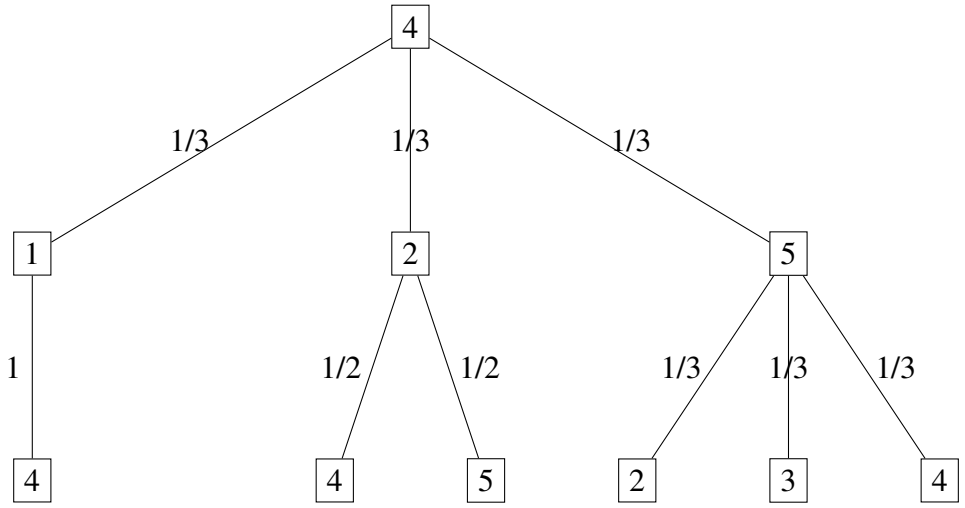

Figure 3.3. A decision tree showing the possible movement of a random walker starting at node 4 of the sample network in Figure 1.1. The numbers on the links show the probability of movement along that link.

therefore the probability of being at a node i adjacent to node j at the next step is $[M^q]_{js}/k_j$. In matrix form,

$$M = A \cdot D^{-1}. \tag{3.7}$$

The transition matrix M and its square for the simple network in Figure 1.1 is given below. The probabilities of reaching any node from node 4 in two steps, shown in the M^2 matrix, can directly be obtained from the decision tree in Figure 3.3.

$$M^2_{(2,4)} = 1/3 \times 1/3 = 1/9$$

$$M = \begin{pmatrix} 0 & 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & 1/3 & 1/3 \\ 0 & 0 & 0 & 0 & 1/3 \\ 1 & 1/2 & 0 & 0 & 1/3 \\ 0 & 1/2 & 1 & 1/3 & 0 \end{pmatrix}.$$

$$M^2 = \begin{pmatrix} 1/3 & 1/6 & 0 & 0 & 1/9 \\ 1/3 & 1/3 & 1/3 & 1/9 & 1/9 \\ 0 & 1/6 & 1/3 & 1/9 & 0 \\ 0 & 1/6 & 1/3 & 11/18 & 1/6 \\ 1/3 & 1/6 & 1/3 & 1/6 & 11/18 \end{pmatrix}.$$

It was previously stated that the random walk betweenness measure includes contributions from many paths that are not optimal (shortest) in any sense, contrary to the shortest path betweenness. However this does not mean that paths of any length contribute equally to the random walk betweenness value. It can be inferred from the powers of the transition matrix that as the length of a random walk grows, the probabilities associated with it quickly decrease. Therefore shorter paths still tend to count for more than longer ones since a random walk becoming very long without finding its target is relatively more unlikely.

For a Markovian transition matrix M, the following equation holds [21]:

$$\sum_{q=0}^{\infty} [M^q] = (\iota - M)^{-1}, \tag{3.8}$$

where ι is the identity matrix. Therefore the probabilities for all paths, ranging from length 0 to length ∞, can be summed with this equation. By summing all powers of this matrix, the unnormalized probabilities of moving from a vertex i to a vertex j can be obtained. The total

number of times the walker moves from j to i averaged over all possible walks, in matrix notation is,

$$\begin{aligned} V &= D^{-1}\left(\iota - M\right)^{-1} \cdot s \\ &= \left[\left(\iota - M\right) D\right]^{-1} \cdot s \\ &= \left[D - MD\right]^{-1} \cdot s \\ &= \left(D - A\right)^{-1} \cdot s \end{aligned} \tag{3.9}$$

The matrix $D-A$ is alternatively called the *graph Laplacian*, and for simply connected networks, it is singular with rank $(n-1)$. This suggests that one of the equations in the Laplacian is a combination of the others. For the Laplacian to become invertible, any row and its corresponding column must be removed. Actually, for every connected component, the Laplacian has rank $(n-1)$, therefore the removal of only one row and column is not enough to make the Laplacian of a fragmented graph invertible.

For the calculation of random walk betweenness, we need to calculate for all paths between all node pairs, symbolizing the starting and target nodes. Therefore in this context, a simple random walk starting at node s, and ending at node t can be characterized as an absorbing random walk, that is, the walker stops if it reaches t, much like a dead end for the walker. Therefore, $M_{it} = 0$, for all i. Column t of matrix M is hence set to zero.

It follows from this that the row t can also be removed, since the removal of the column suggests that its removal does not alter the transitions between other nodes. In order to overcome the invertibility problem, the target node is removed from the graph, so that it acts as a reference point.

On the other hand, we can consider choosing any node, regardless of it being a source or a target node, as the reference point, denoted by v. M_v denotes the transition matrix with these elements removed, similar to D_v and A_v. The inverse $(D_v - A_v)^{-1}$ is calculated, and a column and row of zeros are put in the place of node v. The resulting matrix is denoted as T. [22]

The voltage (energy spent to reach) at node i for source s and target t is,

$$V_i^{(st)} = T_{is} - T_{it}. \tag{3.10}$$

The currents passing through the source and target nodes, by definition, are equal to one:

$$I_s^{(st)} = 1, \qquad I_t^{(st)} = 1. \tag{3.11}$$

The current flowing along a node i is half the sum of the currents flowing along the incident edges;

$$I_i^{(st)} = \frac{1}{2}\sum_j A_{ij}\left|V_i^{(st)} - V_j^{(st)}\right| \qquad \text{for } i \neq s,t. \tag{3.12}$$

The random walk or current flowing from node j to node i is given by $|V_i - V_j|$ [22]. The final betweenness value of a node is,

$$C_B^{rw}(i) = \frac{\sum_{s<t} I_i^{(st)}}{\frac{1}{2}\times n\times(n-1)}. \tag{3.13}$$

An important point worth mentioning is that the choice of the reference node does not make any difference in the results. If $T_{(i)}^{(s,t)}$ were to denote the matrix T for the reference node i from which the observations are carried out and the source node s and target node t, and similarly for vectors V and I, from source 3 to target 1 and reference node 1 in the sample network of Figure 1.1,

$$T_{(2)}^{(3,1)} = \begin{pmatrix} 5/3 & 0 & 1/3 & 2/3 & 1/3 \\ 0 & 0 & 0 & 0 & 0 \\ 1/3 & 0 & 5/3 & 1/3 & 2/3 \\ 2/3 & 0 & 1/3 & 2/3 & 1/3 \\ 1/3 & 0 & 2/3 & 1/3 & 2/3 \end{pmatrix}, \qquad T_{(3)}^{(3,1)} = \begin{pmatrix} 8/3 & 4/3 & 0 & 5/3 & 1 \\ 4/3 & 5/3 & 0 & 4/3 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 5/3 & 4/3 & 0 & 5/3 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$V_{(2)}^{(3,1)} = \begin{pmatrix} -4/3 \\ 0 \\ +4/3 \\ -1/3 \\ +1/3 \end{pmatrix} \qquad V_{(3)}^{(3,1)} = \begin{pmatrix} -8/3 \\ -4/3 \\ 0 \\ -5/3 \\ -1 \end{pmatrix}$$

$$I_{(2)}^{(3,1)} = \begin{pmatrix} 1 \\ 1/3 \\ 1 \\ 1 \\ 1 \end{pmatrix} \qquad I_{(3)}^{(3,1)} = \begin{pmatrix} 1 \\ 1/3 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

The final random walk betweenness values for the nodes of this sample network are as follows:

$$C_B^{rw}(i) = \begin{pmatrix} 2/5 \\ 8/15 \\ 2/5 \\ 23/30 \\ 23/30 \end{pmatrix}.$$

For the edges, these values can be represented by a form similar to that of the adjacency matrix:

$$C_B^{rw}(i,j) = \begin{pmatrix} 0 & 0 & 0 & 0.4000 & 0 \\ 0 & 0 & 0 & 0.3333 & 0.3333 \\ 0 & 0 & 0 & 0 & 0.4000 \\ 0.4000 & 0.3333 & 0 & 0 & 0.4000 \\ 0 & 0.3333 & 0.4000 & 0.4000 & 0 \end{pmatrix}.$$

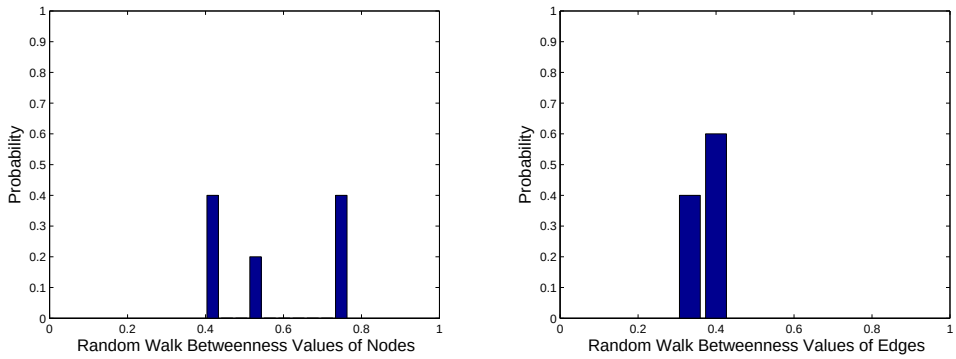

Figure 3.4. Random Walk Betweenness distribution for the nodes and the edges of the sample network in Figure 1.1

The distributions of these values are shown in Figure 3.4.

3.3. Comparison of Centrality Measures

Tables 3.3 and 3.3 show the centrality values of the elements of the sample network in Figure 1.1.

One interesting measure is how the shortest path betweenness fails to account for the importance of node 2. This problem is caused by the fact that no path connecting nodes 1 or 4 to 3 or 5 go through node 2, since it is not a shortest path. From the shortest path perspective, node 2 has no importance for the network.

However that may not actually be the case, when the implications of this result in real life are considered. If these nodes were to represent towns with huge populations, and the links the highways connecting them, it would be reasonable to expect most people to use the shortcut, the link that connects 4 to 5. The unreasonable part is to assume that no one would ever use the longer alternative 25 and 24. This issue is a drawback for the shortest path betweenness measure. The random walk betweenness measure does capture the importance of node 2, making it the third most important node in the network.

Table 3.3. The centrality values for the nodes of the sample network in Figure 1.1

Node	Degree	Shortest Path Betweenness	Random Walk Betweenness
1	1	0	2/5
2	2	0	8/15
3	1	0	2/5
4	3	3	23/30
5	3	3	23/30

Table 3.4. The centrality values for the edges of the sample network in Figure 1.1

Edge	Average Degree	Shortest Path Betweenness	Random Walk Betweenness
14	2	4	2/5
24	2.5	2	1/3
25	2.5	2	1/3
35	2	4	2/5
45	3	4	2/5

4. TYPES OF NETWORKS

The previous chapter dealt with formal definitions of networks. There are, however, a variety of network types, and therefore primary qualities that differentiate one network from another must also be analyzed. Most real life networks bear similarities, but also are very different in some aspects.

4.1. Regular Networks

Regular networks are those that exhibit the repetition of a certain pattern in their structure. There are various types of regular networks, of which some are $trees$, $lattices$ and *ring structures*.

4.1.1. Trees

Trees are networks that do not contain cycles. In other words, a tree is a network on which there is one and only one path connecting any two nodes.

In order to obtain a tree, k edges are emanated from one starting node, called the $origin$. Then, k edges are added to every new node, and the process is repeated until the desired network size is obtained. Every repetition of this procedure creates a new outer ring of nodes, called $shells$, denoted by z. The origin is the 0^{th} shell.

The number of nodes in each shell can be found using the following equation;

$$n^{(z)} = k\,(k-1)^{z-1}\,. \tag{4.1}$$

As the number of shells approaches infinity, the degree distribution of the tree structure converges to that of the ring structure. However for the purposes of this work, the networks under investigation have finite order, therefore there are nodes in the outermost shell. The

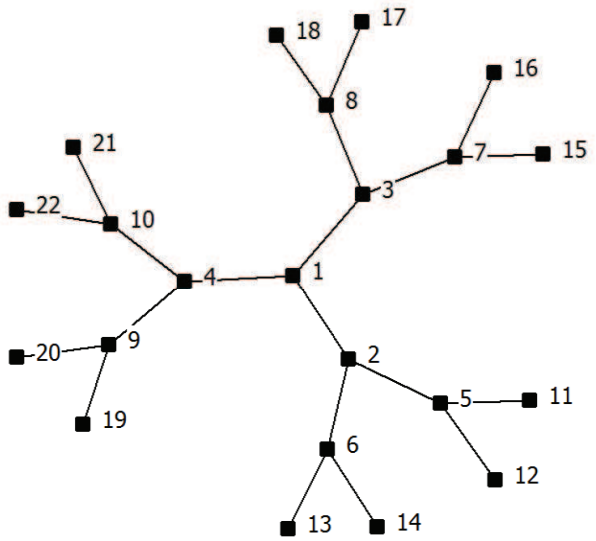

Figure 4.1. A finite tree network with $z = 3$ and $k = 3$

degree of the nodes in this shell is 1, unlike nodes in other shells that have degree k. Since these networks are called trees, these nodes are called $leaf$ nodes. Therefore for finite trees, the boundary effects created by the leaf nodes create a degree distribution that majorly differs from the Dirac$-\delta$ function, as in Figure 4.2.

4.1.2. Lattices

Lattices are regular structures where the nodes are placed on a geometric grid of desired size and dimension. This geometric shape can be a square, a cubes, a prism, a toroid, and many others.

Although some of these geometric slates on which the nodes are placed bear more continuity in their shapes than others, the boundary effect is always present in these network formations. For example, considering a two dimensional rectangular grid, the nodes on the outermost edges of the lattice will have less neighbors than those that are in the middle. Therefore the number of paths reaching these nodes is smaller when compared to that of a node that lies in the middle.

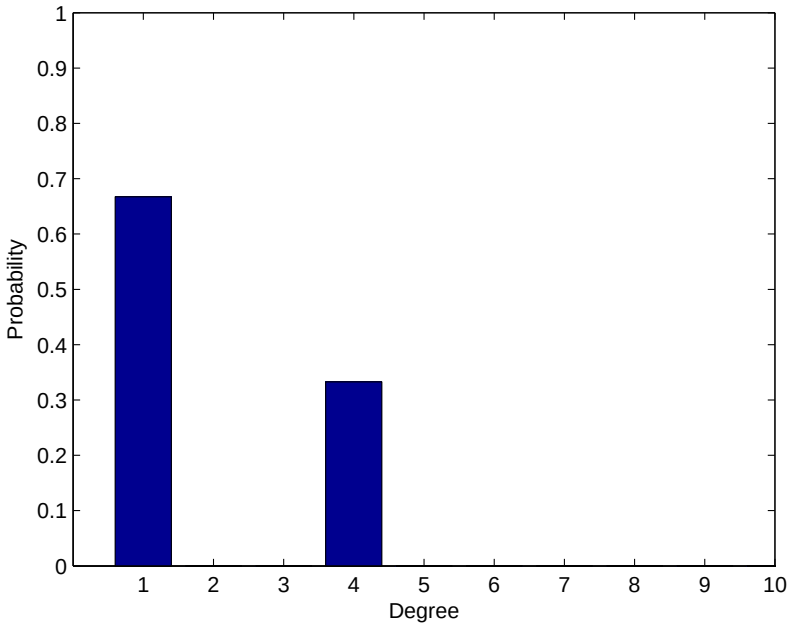

Figure 4.2. The degree distribution of a finite tree network with $z = 6$ and $\bar{k} = 3$, $n = 1457$.

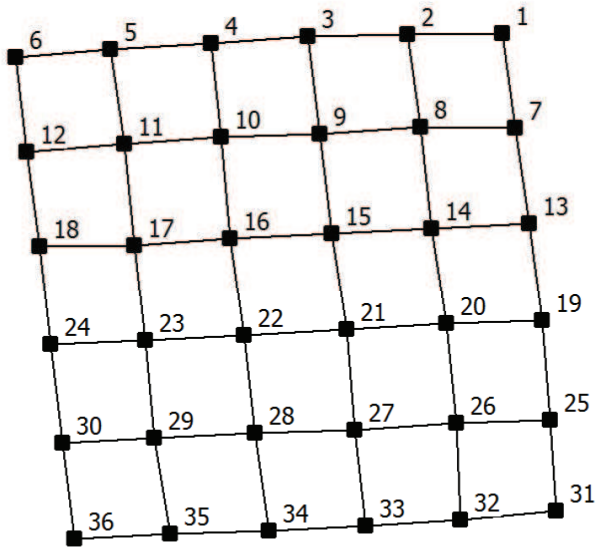

Figure 4.3. A rectangular lattice network with $n = 36$.

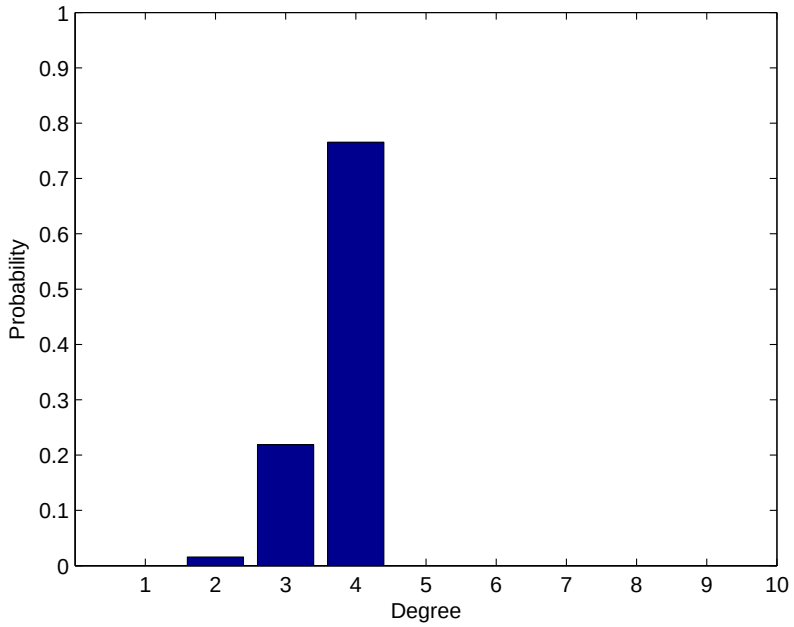

Figure 4.4. The degree distribution of a two dimensional rectangular lattice with $n = 256$.

4.1.3. Ring Structures

Rings are created by placing n nodes on a circle, and connecting every node with the k closest nodes, where n and k define the network order and size. It can be seen that k, which ends up being the average degree, cannot be an odd number.

In ring structures, such as the one in Figure 4.5, all nodes have the same degree. Therefore these types of networks have a degree distribution that resembles the Dirac-δ function, as in Figure 4.6. As a result, the network is also symmetric, which is why rings are often used as substrates from which other networks can be created. [24]

Obviously, the uniformity causes all minimum cuts to be of the same size, which is equal to the average degree of the ring structure, as in Figure 4.7.

Despite strong local connectivity, rings lack long range connections which cause relatively lengthy shortest paths between two opposite sides of a ring, leading to the shortest path distribution shown in Figure 4.8.

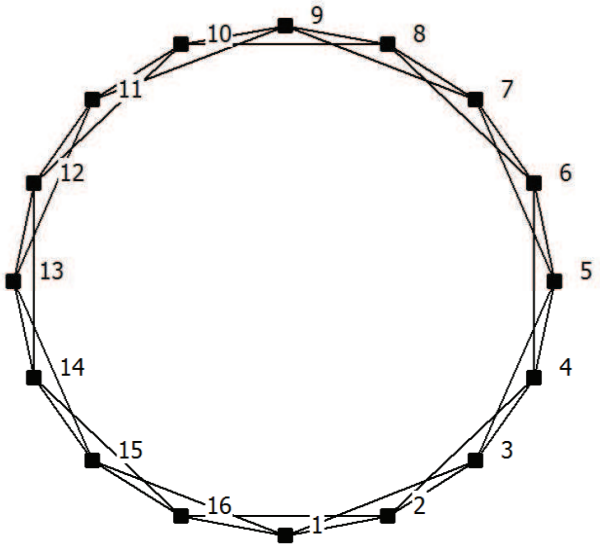

Figure 4.5. A ring network with $n = 16$ and $\bar{k} = 4$.

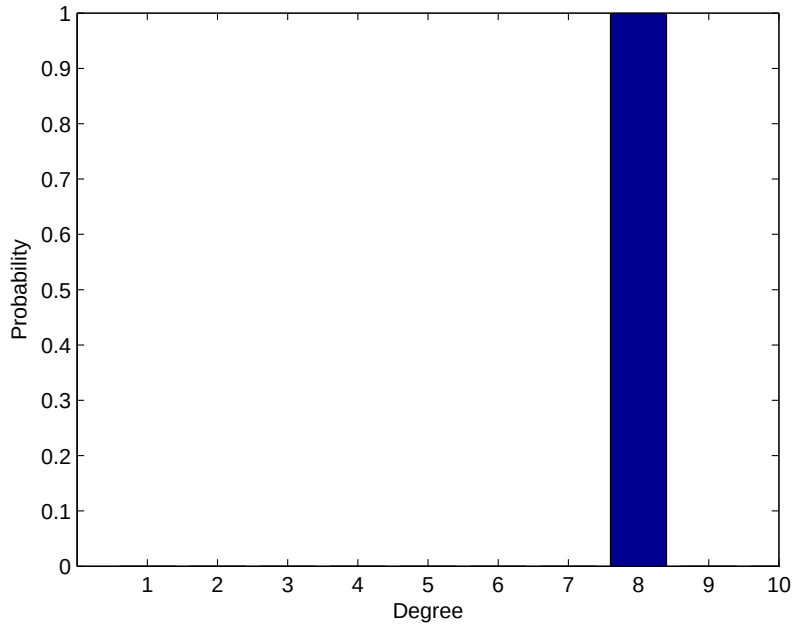

Figure 4.6. The degree distribution of a ring structure with $n = 256$ and $\bar{k} = 8$.

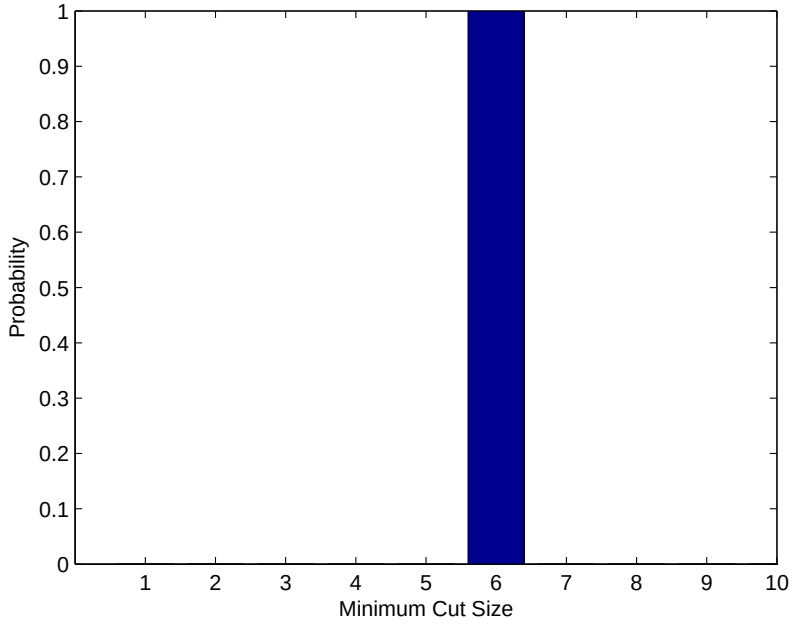

Figure 4.7. The minimum cut distribution of a ring structure with $n = 2048$ and $\bar{k} = 6$.

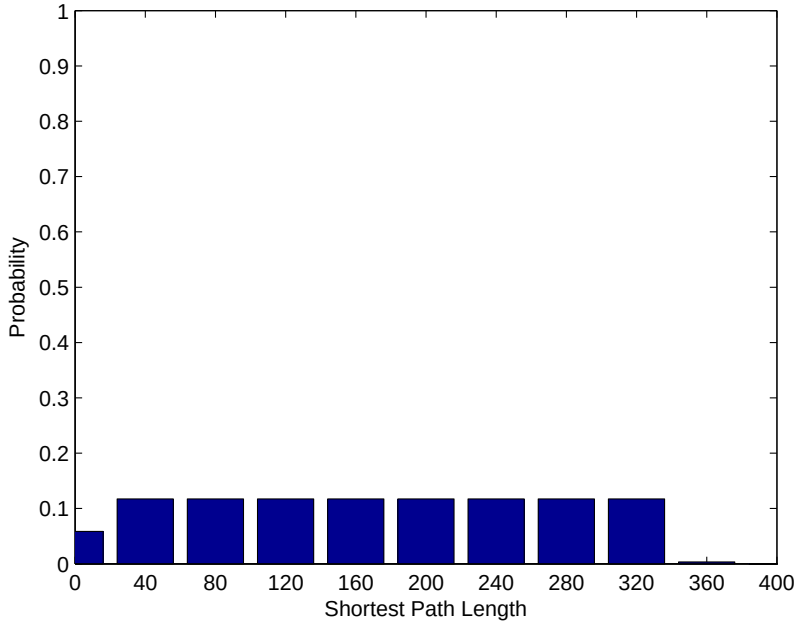

Figure 4.8. The shortest path length distribution of a ring structure with $n = 2048$ and $\bar{k} = 6$.

4.2. Erdos-Renyi Networks

Graph theory has its origins in the 18th century in the work of Leonhard Euler, the early work concentrating on small graphs with a high degree of regularity. In the 20th century graph theory has become more statistical and algorithmic. A particularly rich source of ideas has been the study of random graphs, graphs in which the edges are distributed randomly. Networks with a complex topology and unknown organizing principles often appear random, thus random graph theory is regularly used in the study of complex networks. [26]

For a graph with a fixed number of nodes n, an Erdos-Renyi network is a representation of the classical random graph. Each pair of nodes are connected by an edge with probability p. With probability $1 - p$, the edge is absent.

$$\bar{k} = p \times (n - 1). \tag{4.2}$$

There are details that need to be mentioned about this procedure. Unless forbidden, there is a good probability that the second procedure will create graphs in which a node is connected to itself, called $tadpoles$; or two nodes will be connected by more than one edge, called $melons$. Although it is possible to prove that for large enough networks the number of tadpoles and melons become statistically negligible, in this work these formations are forbidden. [6]

It can be seen from the first procedure that there are $2^{n(n-1)/2}$ distinct networks that can be created, each with number of edges smaller than or equal to $n\,(n-1)/\,2$.

A node in a $connected$ Erdos-Renyi Network with n nodes can have a maximum degree of $n - 1$, and a minimum degree of 1. If the node has degree k, there are k edges emanating from this node, each can connect to $n - 1$ different nodes. Therefore it can be seen from combinatorics that the probability of a given node having degree k is given by the

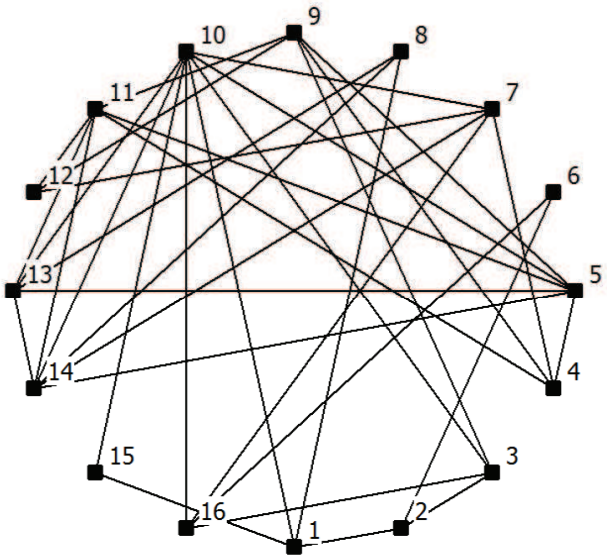

Figure 4.9. A sample Erdos-Renyi network with $n = 16$.

distribution

$$P(k) = \binom{n-1}{k} p^k (1-p)^{n-1-k}$$

It has been shown that for relatively large n and fixed p, the binomial distribution converges to the Poisson Distribution [25]:

$$P(k) = \frac{e^{-\bar{k}} \times \bar{k}^k}{k!} \tag{4.3}$$

The average shortest path of a large enough Erdos Renyi network [26] is approximated by,

$$\bar{l}_{ER} = \frac{\ln(n)}{\ln(pn)}. \tag{4.4}$$

The shortest paths, shortest path and random walk betweenness values in an Erdos

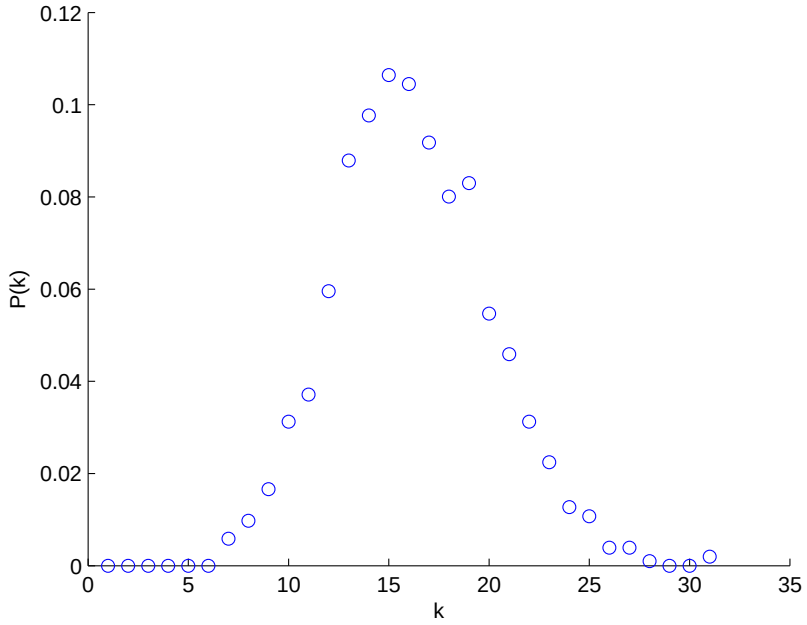

Figure 4.10. Degree Distribution of a generated Erdos Renyi Network in linear scale, with $n = 1024$ and $\bar{k} = 16$.

Renyi network are almost normally distributed, as seen in Figure 4.11 and Figure 4.12.

Erdos Renyi networks are uncorrelated, since they do not show an incline nor a decline in their $\bar{k}_{nn}$ versus k figures, as in Figure 4.13.

The clustering coefficients in an Erdos Renyi network are very small, and is approximated by [26],

$$\bar{C}_{ER} = p = \frac{\bar{k}}{n}. \tag{4.5}$$

. The whole creation process is totally random, hence it is not reasonable to expect the formation of a strong local structure. The average nearest neighbor clustering coefficient is shown to be uncorrelated with the node degree, as in Figure 4.14, which agrees with the uncorrelated nature of an Erdos Renyi network.

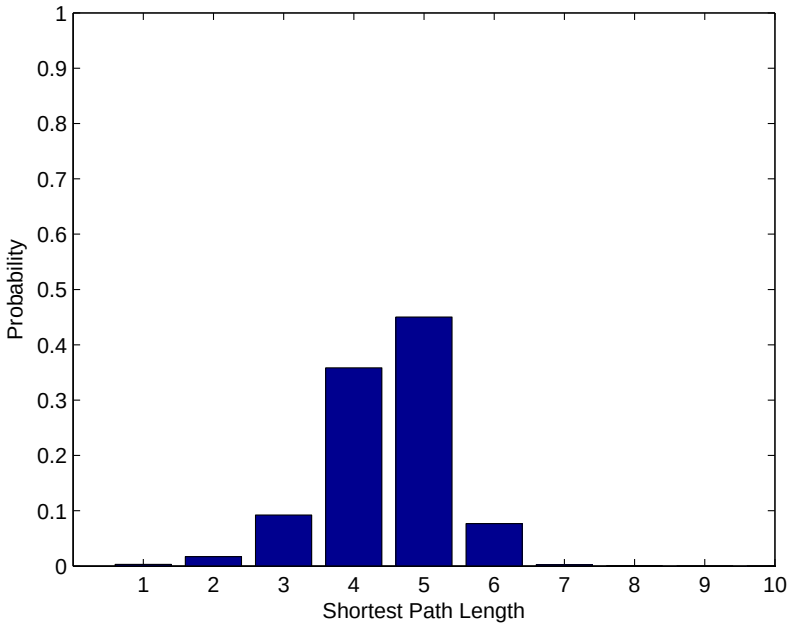

Figure 4.11. The distribution of the lengths of the shortest paths of a generated Erdos Renyi network with $n = 2048$ and $\bar{k} = 6$.

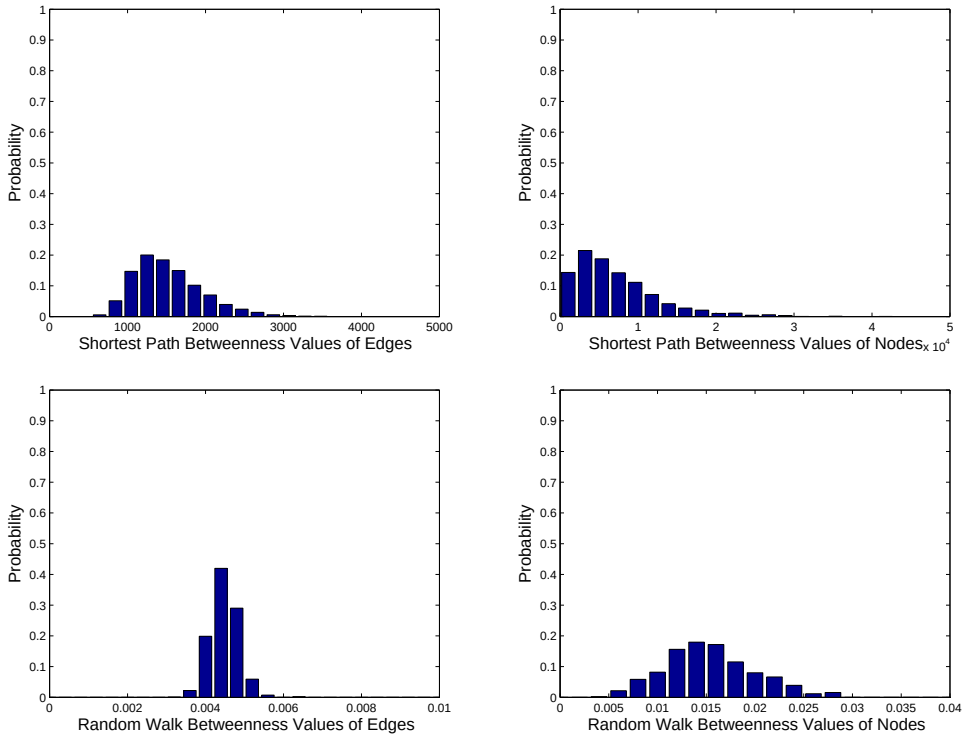

Figure 4.12. The shortest path and random walk betweenness distributions of two generated Erdos Renyi networks with $n = 2048$ and $\bar{k} = 6$ and $n = 512$ and $\bar{k} = 6$, respectively.

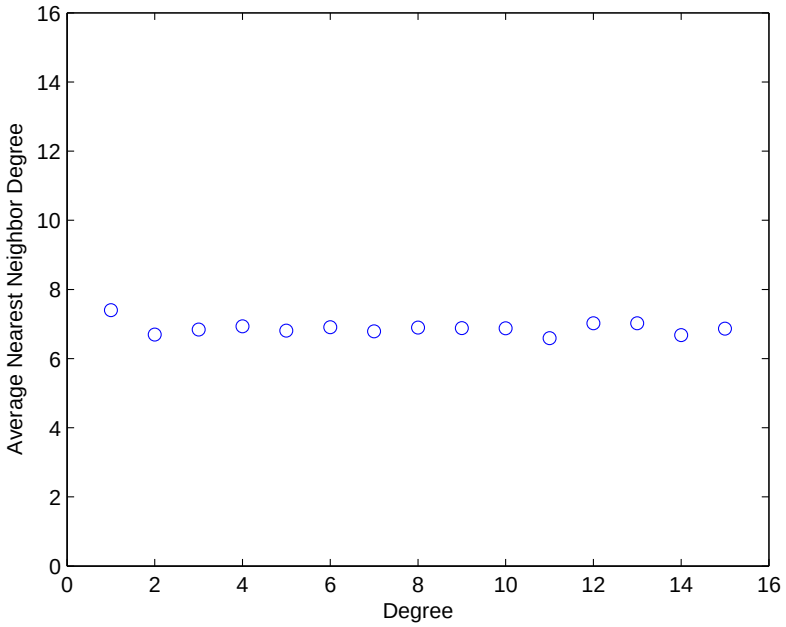

Figure 4.13. The average nearest neighbor degree versus degree for a generated Erdos Renyi network with $n = 2048$ and $\bar{k} = 6$.

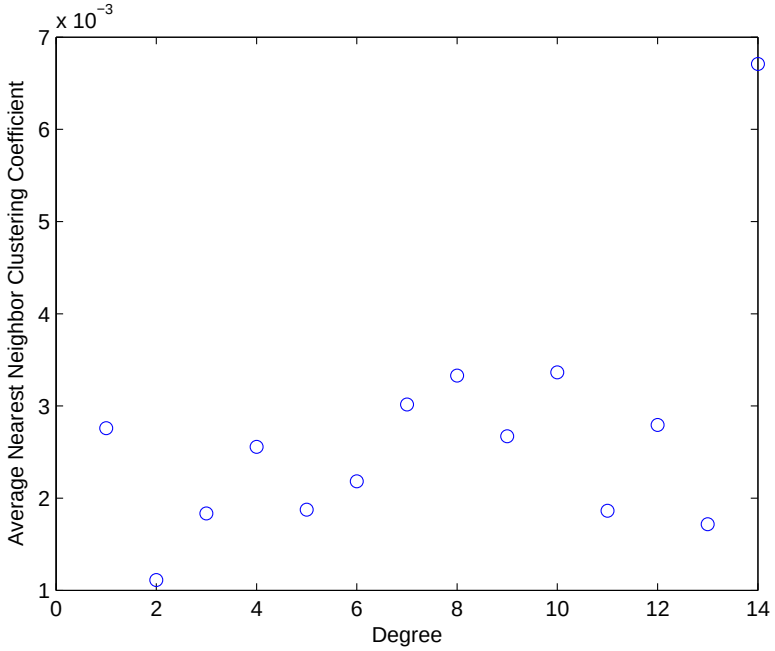

Figure 4.14. The average nearest neighbor clustering coefficient versus degree for a generated Erdos Renyi network with $n = 2048$ and $\bar{k} = 6$.

4.3. Scale-Free Networks

Scale-free networks have been encountered more recently, in the investigation of the map of the World Wide Web. This class of network is modelled by Barabasi and Albert [31]. Their model is actually a representation of a growing citation graph, a directed network in which an arc exists from one author to another for the existence of a citation; and a new author is added to the network if he publishes a paper. New vertices (authors) are added continuously, as new papers are published. It is more likely that the newer papers will cite the older papers in that field, where in the model each new node becomes attached to the old ones with a probability proportional to their degrees. This process is called *preferential attachment*.

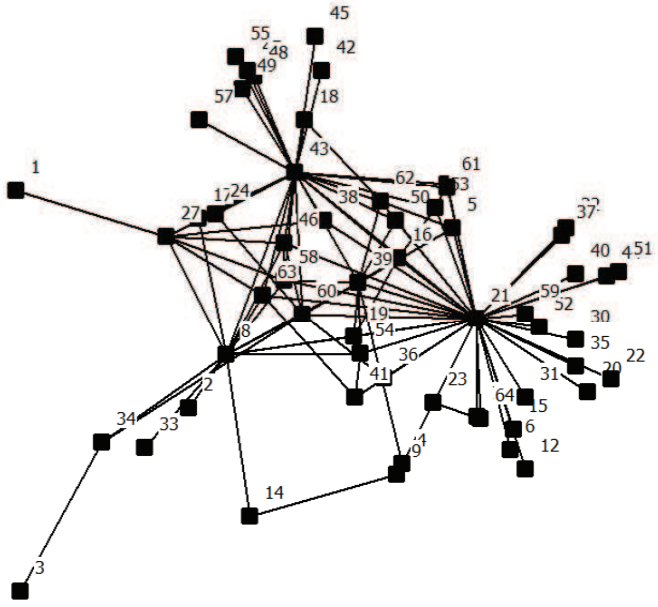

Figure 4.15. A sample scale-free network with $n = 64$.

It can be seen that nodes that start out early when the network is relatively small are going to turn out to be the ones that have the biggest degree in the end. Moreover, as the degree of a node grows, the probability of a new node being connected to it increases, which in turn increases its degree even further. Therefore preferential attachment creates a positive feedback loop, where nodes with bigger degrees go on to grow bigger. This sort of growth allows some nodes to have very big degrees, and many nodes to have smaller degrees. This phenomenon is also referred to as the *rich get richer*. The nodes with very big degrees are

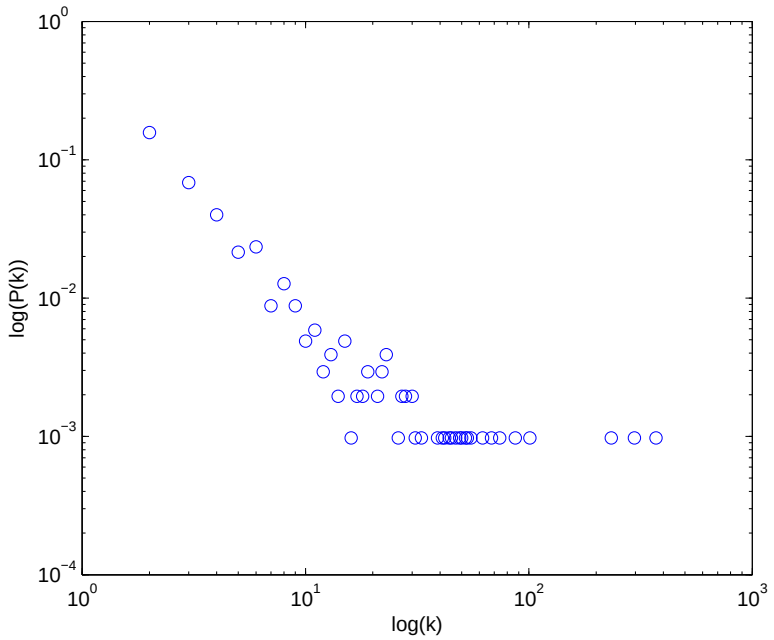

Figure 4.16. Degree distribution of a generated scale free network with $n = 1024$ and $\gamma = -2$.

called *hubs*. [31]

Scale-free networks typically follow a power-law distribution, where the probability of a node having degree k is given by

$$P(k) \approx k^{-\gamma}. \tag{4.6}$$

There are many things that can be said about the power law, the most important being its *fat tail*. Poisson and exponential distributions are rapidly decreasing funtions, such that as k increases, $P(k)$ decreases very rapidly. This means that there is very little probability that a node has relatively large degrees in these distributions. On the contrary, the power-law distribution has a fat tail, which allows for the existence of hubs.

The shortest path lengths are distributed more or less normally as in Figure 4.17, but the mean value of the shortest path length is slightly lower than that or the Erdos Renyi network. Figure 4.18 plots the relationship between the average nearest neighbor degree and

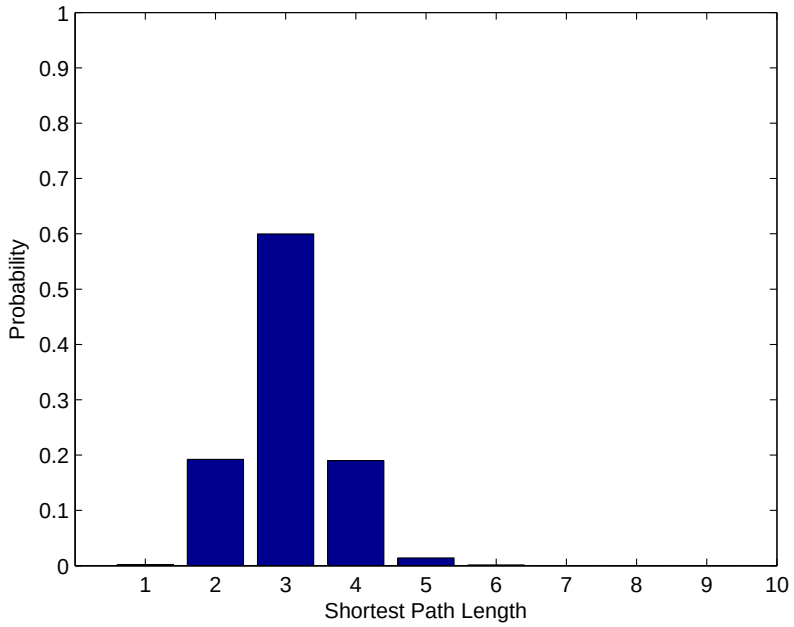

Figure 4.17. The distribution of the shortest path lengths of a generated scale-free network with $n = 2048$ and $\gamma = -2$.

the degree, which declines linearly in logarithmic scale, similar to the behavior of the degree distribution. This leads to the conclusion that scale free networks are disassortative, higher degree nodes are connected to lower degree nodes and vice versa, which can be interpreted as a trivial consequence of the power-law based degree distribution.

Another interesting property of scale free networks is that betweenness values on these networks are also exhibit a power law distribution. In other words, there are few nodes and edges that are exponentially more $inbetween$ than a big number of others which have low betweenness values. Figure 4.19 shows the distribution of these betweenness measures.

Scale free networks are not very strong in terms of local structure, hence they exhibit a low clustering coefficient value, which is still bigger than that of a similar Erdos Renyi network. The average nearest neighbor clustering coefficient increases as the degree increases, as shown in 4.20. This means the hubs have neighbors that have high clustering coefficient values.

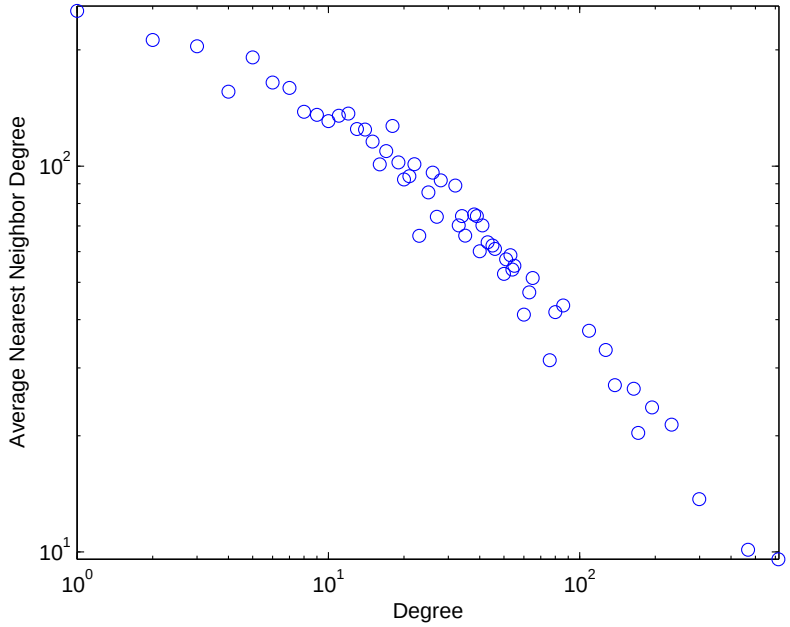

Figure 4.18. Average nearest neighbor degree k_{nn} versus node degree k for a generated scale free network with $n = 2048$ and $\gamma = -2$.

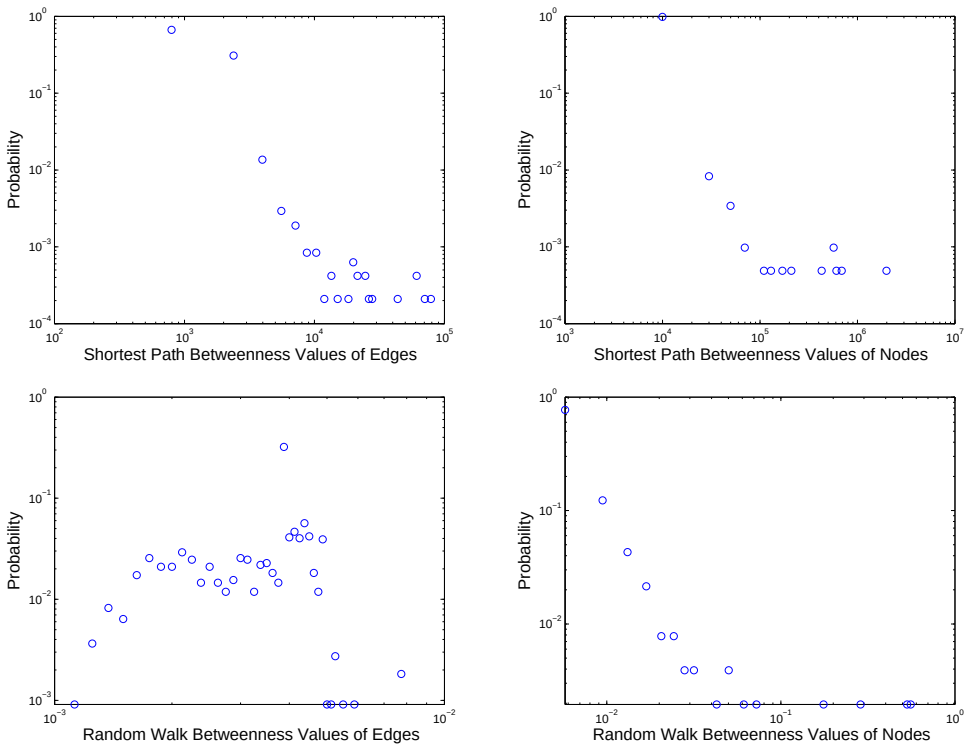

Figure 4.19. The shortest path and random walk betweenness distributions of the nodes and edges of a generated scale-free network with $n = 2048$ and $\gamma = -2$, and $n = 512$ and $\gamma = -2$, respectively.

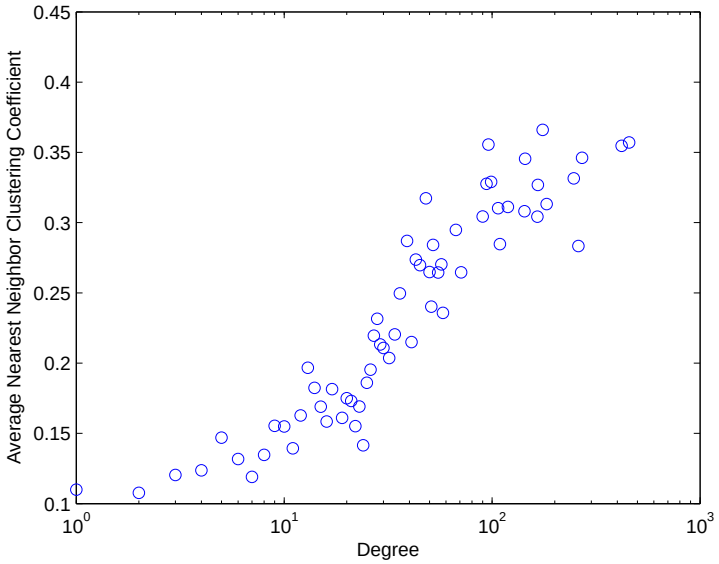

Figure 4.20. The average nearest neighbor clustering coefficient versus k graph, for a generated scale free network with $n = 2048$ and $\gamma = -2$.

4.4. Small World Networks

The title of these networks fit very well to their basic properties. Small world networks are highly clustered, like regular networks, yet have smaller average shortest path lengths, like random graphs. This interesting property makes small world networks easy to navigate.

Although many models of small worlds exist [28], the most common is the Watts Strogatz model. The process of building a small world network is by the random rewiring procedure for interpolating between a regular ring lattice and a random network, without altering the number of vertices or edges in the graph. Starting with a ring of n vertices, each connected to its k nearest neighbours by undirected edges. Then a node is chosen along with the edge that connects it to its nearest neighbour in a clockwise sense. With probability p, this edge is reconnected to a vertex chosen uniformly at random over the entire ring, with duplicate edges forbidden. This process is repeated by moving clockwise around the ring, considering each vertex in turn until one lap is completed. Next, the edges that connect vertices to their second-nearest neighbours clockwise are considered. This process, circulating around the ring and proceeding outward to more distant neighbours after each lap, is continued until each edge in the original lattice has been considered once. Three

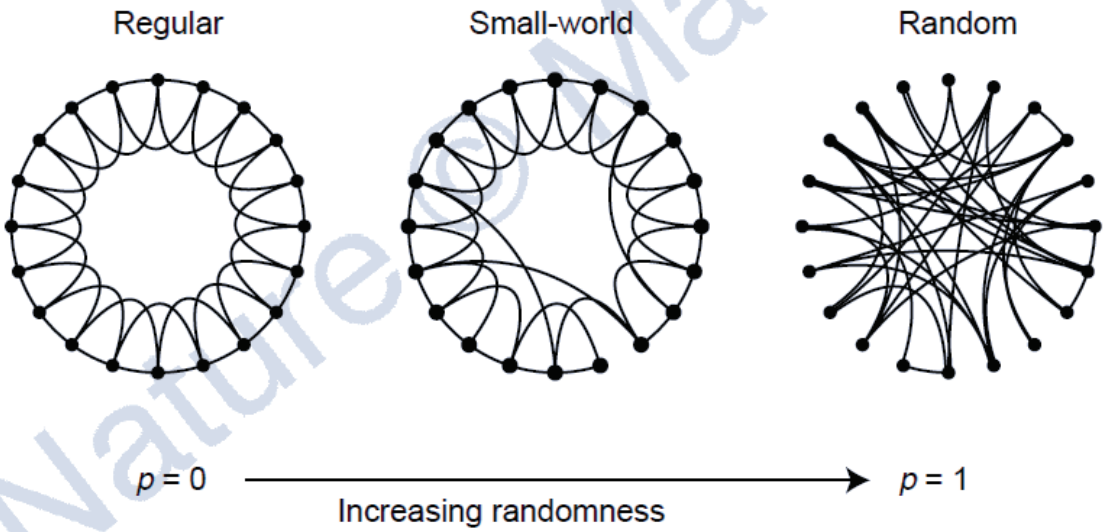

Figure 4.21. The rewiring process of a small world network, beginning with a regular ring structure and ending as an Erdos Renyi random graph, with $p = 0$ and $p = 1$, respectively. [11]

realizations of this process are shown, for different values of p. For $p = 0$, the original ring is unchanged; as p increases, the graph becomes increasingly disordered until for $p = 1$, all edges are rewired randomly. For certain intermediate values of p, the graph is a small-world network: highly clustered like a regular graph, yet with small characteristic path length, like a random graph.

A logarithmic horizontal scale has been used to resolve the rapid drop in $L(p)$, corresponding to the onset of the small-world phenomenon. During this drop, $C(p)$ remains almost constant at its value for the regular lattice, indicating that the transition to a small world is almost undetectable at the local level. [11]

For smaller networks though, as in this work, the lower bounds of the clustering coefficient and the average shortest paths are not exponentially small when compared to the initial ring substrate. Therefore the small world region is not as obvious as for larger networks. To clarify, consider the same graph for a network with $n = 128$ and $k = 8$.

To detect the region where the average shortest path length is as low as possible, and

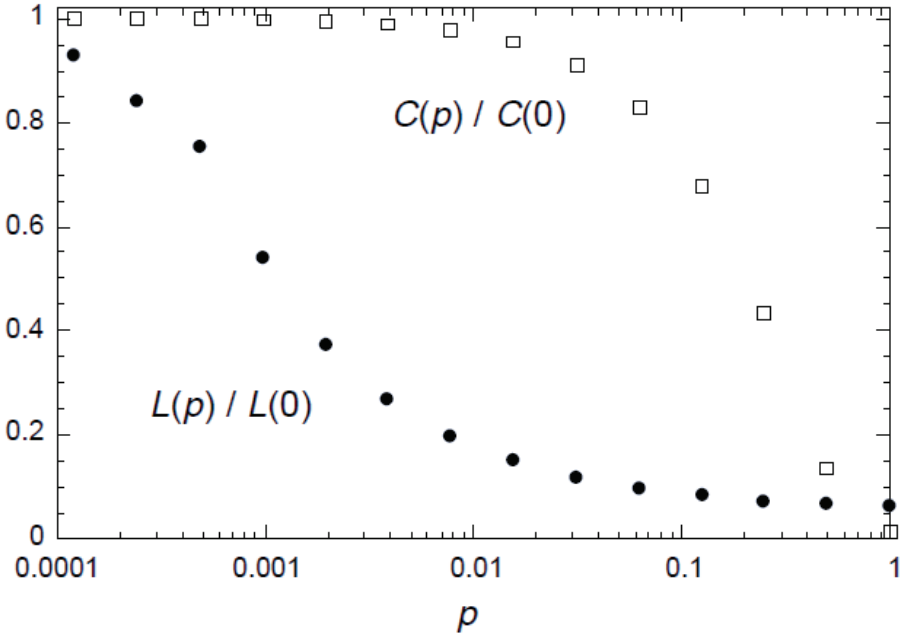

Figure 4.22. The average shortest path length $L(p)$ and clustering coefficient $C(p)$ normalized over the values of the initial ring substrate, of the small world networks as a function of p, over 100 realizations for $n = 1000$ and $k = 10$.[11]

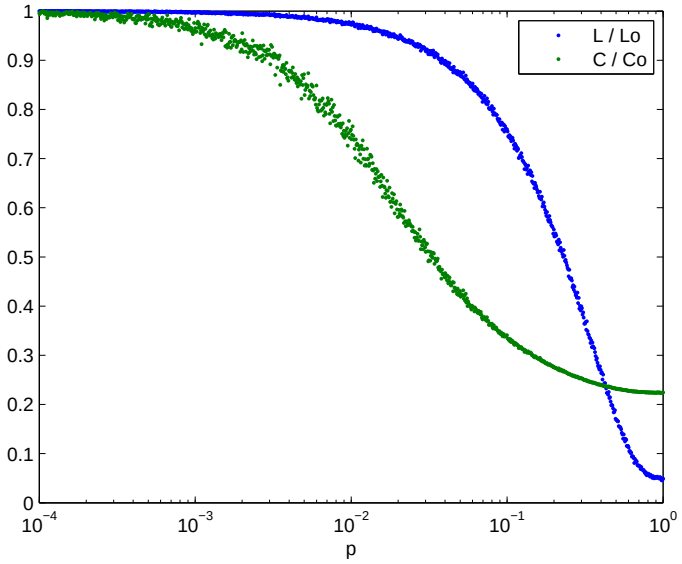

Figure 4.23. The average shortest path length and clustering coefficient normalized over the values of the initial ring substrate, of the small world networks as a function of p, over 100 realizations for $n = 128$ and $k = 4$.

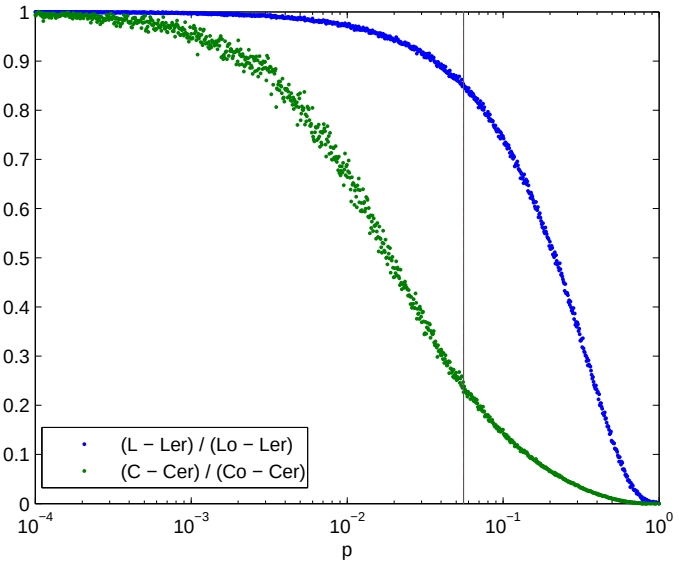

Figure 4.24. The re-normalized version of Figure 4.23. For $p = 0.0558$ the difference between the two curves is maximized.

the clustering coefficient of the network is as high as possible, we can substract the saturation values for these curves, which are the bounding values for an Erdos Renyi network with the same parameters, namely L_{er} and C_{er}. If we were to draw the same curves by removing this lower bound and strecthing the curve to the unit interval, the small world region, and the probability at where this network can be obtained becomes more apparent. However it should be noticed that the mentioned bounds still exist.

4.4.1. Statistical Comparison of Network Types

The following table compares the means and the standard deviations of fifty generated networks of each type.

Table 4.1. Network parameter means and standard deviations for ring substrates, scale free, Erdos Renyi and small world networks with $n = 128$ and $k = 4$.

n = 128 , k = 4	Ring Substrate		Scale Free γ = -1.92		Small Worlds p = 0.0558		Erdos Renyi	
	μ	σ	μ	σ	μ	σ	μ	σ
Degree	4	0	3,93	7,69	4,00	0,45	4,03	1,94
Average Degree	4	0	20,50	11,42	4,05	0,31	4,78	1,24
Average Nearest Neighbor Degree	1	2	5,17	9,92	2,70	2,21	4,63	1,89
Average Shortest Path Length	16,38	9,17	2,71	0,71	6,82	2,86	3,63	1,09
Clustering Coefficient	0,50	0,00	0,22	0,34	0,43	0,13	0,02	0,08
Node Shortest Path Betweenness Centrality	1953	0	217	952	739	723	334	286
Edge Shortest Path Betweenness Centrality	520	489	99	76	217	242	115	40
Node Random Walk Betweenness Centrality	0,2128	0	0,0395	0,0695	0,1044	0,0354	0,0571	0,0223
Edge Random Walk Betweenness Centrality	0,1025	0,0322	0,0181	0,0052	0,0483	0,0235	0,0245	0,0038
Minimum Cut	4	0	1,35	1,21	3,82	0,41	3,03	1,24

5. FAILURE SIMULATIONS

The question of how resilient, or how reliable networks are against random failures or targeted attacks has been an interesting question for a long time. Although what is meant by failure depends on the specific function of the network, it is obvious that nodes or links can fail dependently or independently. If the network under investigation is a model of the Internet, a computer may break down unexpectedly. In the case of a transportation network, a highway bridge may collapse after an earthquake, or in the case of a power grid, power lines may fail, as well as the stations from where they emanate. It should also be mentioned that all these networks can also suffer from intentional attacks, by an assailant who, by some method, selects specific elements to attack. The responses these networks give under any of these scenarios are crucial to understand the extent of the damage that can be caused as well as serving as an insight to how they can be reinforced.

From this point of view, what is meant by damage must be clarified. A network may still be functioning after the failure of certain links. In the instance of a highway network, if the direct route between two towns is no longer usable, the traffic will be directed to an alternative path. If there is such a path between all pairs of nodes in the network, after the failure events occur, the network is still connected, or in other words, maintains its connectivity. Therefore the network is still able to serve its function. However though, by itself, remaining connected does not say much. Considering the case where the failures push the network to the limit where it can barely stay connected, the lack of alternative paths between node pairs inhibit network performance. Again in the case of the highway network, after a series of failures if the network was to turn into a tree, the network would still maintain its connectivity. However, all towns would have only one route going in and out, and expected travel times between towns would definitely increase, therefore making the network function inadequately. Therefore it can be said that while controlling the connectivity, the change in network performance must also be monitored, for every failure scenario.

In brief, networks respond to failure both in terms of reliability, and performance. The concept of reliability is associated with a system's ability to maintain its function in specified

conditions. Therefore to establish a definition for reliability, the purpose of the system must be properly specified; which in turn indicates the conditions under which the system is no longer reliable, or not functioning. The purpose of a network may vary depending on the context, but all networks share the function of transmission across its links. Hence the failure scenario generally occurs when there is a disconnection in the network, that is when all or some elements of the network can no longer send signals or goods, whatever they are, to any of the specific targets. If a network is divided into several components, and there is no path that connects one component to another, the system is no longer unified, nodes on one component have no communication with the nodes on the other. This means the network is no longer capable of fully performing its transmission function.

Reliability in literature is often expressed by probabilistic measures. In network analysis, this procedure is most often done by working on probabilistic networks, which again consists of a set of nodes and a set of edges. In addition however, there are assessed probabilities for failures of nodes or edges, p_n and p_e, respectively. Connectivity is checked for every failure scenario, and averaged over all failure cases, which in turn returns a number between 0 and 1. [41]

Let K be a set of target vertices such that $K \subseteq V$ and let $s \in K$ be designated as the source vertex. The $k - terminal\ reliability$ of graph G is defined as the probability that there exists a path of operating edges from s to every vertex in K. This value is represented as $R(G, s, V)$. When $|K| = 2$, it is called the $two - terminal\ reliability$ problem. For specific target and source node sets, the reliability value is represented as $R(G, s, \{s, t\})$. [41]

Obtaining accurate p_n or p_e values may be difficult or meaningless in practice. In problems where such knowledge is absent, for modeling purposes, the assumption p_e=p is often used for simplification. For this specific value of p, the reliability value is denoted as $R(G, s, \{s, t\}, p)$. This simplification does not inhibit the detection of general failure modes but unexpected causes of failure may be overlooked. [41]

Another assumption in this model is the statistical independence of operation probabilities. In practice, the failure modes of the components of most systems are not totally independent, since there may be failures which affect more than a single component or these failures may cause a *cascading* mode of failure: failure of one component puts neighboring components under additional stresses which in turn causes an increase in their failure probability. In these examples, there is positive correlation, that is the failure of a neighboring component constitutes a major portion of the failure probability of a component. Therefore the $R(G, s, \{s, t\}, p)$ values are an overestimation of the actual probabilities. [41]

There are many methods of finding $R(G, s, \{s, t\}, p)$. However it should be understood that this value for reliability does not provide a measure for the network performance, but rather is an indicator of the fundamental limitations on performance imposed by the topology of the network. A $state$ of a probabilistic network $G = (V, E)$ is expressed by the set of operating edges $S \subset E$. There are m edges, each of them is either functional or nonfunctional. It is easy to see that there are 2^m possible states of G.

A binary function $\varphi(S)$ is defined as,

$$\varphi(S) = \begin{cases} 1 & \text{if at least one path connecting the source to the target} \\ 0 & \text{otherwise.} \end{cases} \tag{5.1}$$

Then;

$$R(G, s, K) = \sum_{S \in E} \varphi(S) \prod_{e \in S} p_e \prod_{e \notin S} (1 - p_e) \tag{5.2}$$

One possible method of calculating this value would be to identify all possible states of G, and check for connectivity. This method is computationally difficult even for networks of smaller sizes. This method is improved by Mine and Moskowitz by the Factoring Theorem

[42]:

$$R(G, s, K) = p_e * R(G \cdot e, s, K) + (1 - p_e) * R(G - e, s, K). \tag{5.3}$$

$G \cdot e$ represents the graph obtained by contracting edge e in G and $G - e$ represents the graph obtained by deleting edge e in G. $R(G, s, K)$ can be obtained by using the Factoring Theorem recursively. One other benefit of this method is that it shows the reductions that can be done in a network while keeping its reliability value close to original. There are different methods of reduction that can be applied, like *series reduction*, where a non-terminal node of degree two along with its two incident edges is removed and replaced by an edge between its two neighbors. The operation probability of this edge is the product of the operation probabilities of the two removed edges. In *parallel reduction*, a pair of edges between the same two vertices is replaced by a single edge. The operation probability given to this edge is the sum minus the product of the operation probabilities on the two original edges. Both parallel and series reductions simplify the network under investigation without altering the $R(G, s, K)$ value. [42]

Despite these simplifications, the calculation of the reliability value may still be difficult, where approximation methods [40] can be preferred.

Unlike network reliability, network performance can be measured by very different parameters for different networks. These parameters are generally based on the properties of specific paths in the network, which can be shortest paths, or the total number of available paths, or any bounded version of these. Still though, one can see that the performance measurement parameters often deal with how efficiently signals, goods, or people, whatever is moving through the veins of the network, are able to move to other nodes. For the world wide web, a web-site owner would most probably want to maximize the number of different ways his site can be reached, either directly or indirectly. Differently, in a railway or highway network, it is not this redundancy of available paths that matters the most, but rather the speed at which a target can be reached. Considering these explanations, the question of which network topology is reliable, or has high performance becomes trivial. In the blunt model

in which the cost of adding links to a network has no cost, a network designer would very likely want to connect all nodes to all others. This way, independent of the source-target node pair, the transmission can be carried out by following a single link. Moreover, the amount of alternative paths, although not optimal, is at its maximum. Therefore it can easily be said that networks in which every node is adjacent to all others, called complete networks, are the most reliable and high performance networks. But then again, how often do we see complete networks in real life? One way of rationalizing investigation of a complete network can be acknowledging that other less reinforced networks that are far from complete are some version of a complete network with many failed elements. Therefore it is reasonable to expect such a point after which the failure of an extra element does not cause extra damage, or conversely, causes damage with a bigger magnitude.

On the other hand, we can consider networks which consist of the minimum number of elements that keep it connected. The network may itself be connected, that is every node can reach every other node, but the failure of any single element disconnects the network. Such networks are called trees. If a network's primary feature is connectivity, and the abundance of alternative paths is not a priority, trees are the structures that can carry out this function with the minimum number of edges. Similar to considering random networks as failed subgraphs of complete networks, trees can be thought of failed subgraphs of any connected random network.

Most of the explanations above are trivial, however the whole picture is still incomplete. If the goal is to monitor network function and performance under different failure scenarios, one must also take into account the types of networks, not to be confused with the context of the network. Although the actual context of the network pretty much determines the type, it is better to conduct the experiment on specific network types in the literature, in addition to certain networks whose data can be used.

5.1. Network Generation

The network types in the previous chapter all differ in their degree distributions. Generation of network ensembles from a given probability distribution or a degree sequence is

already investigated in [32, 33, 34]. A *network ensemble* can be considered as the graphical representation of a set of numbers drawn from that probability distribution, generally a power-law or a Poisson distribution, or any other. These distributions are bounded by $n-1$, the maximum degree a node can have.

One issue that arises for scale free network degrees is that the probability distribution is not normalized. [30] Therefore for the generation of a scale free network, and for a given size, the probabilities obtained by the unnormalized distribution, ranging from $k = 1$ to $k = n - 1$, should be normalized. So for a scale free network of size n, the normalized probability distribution $P'(k)$ is

$$P'(k) = \frac{k^{-\gamma}}{\sum_{k'=1}^{n-1} k'^{-\gamma}}. \tag{5.4}$$

Each of these numbers specify the degree of a node. The non-increasing sorting of this sequence of numbers is called the *degree sequence*, denoted by $\{d_1, d_2, \ldots, d_n\}$. Not all degree sequences constitute a simple connected graph, though.

The initial degree sequence can be thought of as the totally unconnected graph with nodes that have a number of free stubs emanating from them, as many as each node's degree.

A *graphic sequence* is a sequence of numbers which can be the degree sequence of a simple connected graph. Obviously, maximum and minimum degrees should be in a certain limit, so $max(d_i) \leq n-1$ and $min(d_i) \geq 1$. Moreover, the sum of the degrees must be even, since every stub will connect to another stub. If the sum of degrees is odd, one stub will be left unconnected. Therefore $\sum_{i=1}^{n} d_i$ must be even. Erdos and Gallai developed a series of conditions [43] besides these under which a degree sequence becomes graphical:

$$\sum_{i=1}^{r} d_i \leq r(r-1) + \sum_{i=r+1}^{n} min\,(r, d_i) \qquad \text{for } r \leq n-1. \tag{5.5}$$

This condition imposes $n-1$ inequalities to hold, under which case the given degree

sequence is graphical, i.e. a simple connected graph can be constructed with the given degree sequence.

For example, the sequence [3 3 1 1], is not graphical, even though the sum of the numbers is even. The reason is that for this sequence, the Erdos Gallai criterion does not hold for $r = 2$:

$$3 + 3 > 2 \times 1 + min(1, 2) + min(1, 2).$$

Once a graphical degree sequence is drawn from the desired distribution, the next step is to create a simple connected network with this degree sequence. The process can be summarized by the following steps:

1. Assign each node as many stubs as it is assigned by the degree distribution.
2. Randomly select a node, connect one of its stubs to another randomly selected node, given that they both have free stubs. For these nodes to have a valid connection, there should not already be a link between them. If these conditions are satisfied, the connection is made to form a link between these nodes.
3. Upon this connecting phase, if there comes a point where there are free stubs but no valid connections, then randomly select an edge and break it until new valid connections arise, then continue on with the connecting process.
4. Continue until there are no free stubs left in the network and check if the graph is simply connected, that is, all nodes can reach one another. If not, apply edge swapping until the graph becomes simply connected.
5. To avoid statistical pitfalls caused by the connecting and breaking procedure, applying as many edge swaps as the number of edges in the network may be preferred, without disconnecting the network.

Edge swapping is a procedure that reconfigures connections without altering the degree sequence, and is very similar to the breaking and connecting step above. An edge connecting nodes i and j is broken, which leaves these nodes with one free stub for each. Then another

edge is broken between nodes p and q. Then two new connections are made between these nodes, either (i, p) and (j, q), or (i, q) and (j, p). There are no free stubs, as before, and the degree sequence is unaltered. [35]

5.2. Rank Ordering and Edge Failures

Once the network is formed, to simulate a series of failures, one of the rank ordering methods is applied. Every edge is ranked according to either shortest path and random walk betweenness values, average degree, or by the degree of the node they are incident to. Depending on this rank, and the choice, the highest or the lowest ranked edge is broken.

The process is repeated until a desired point, which can be the total fragmentation of the network, or a certain ratio of node failures.

One critical point here is to choice of reordering the links after each step. This choice is very crucial in the sense of what the simulation physically represents, since as failures occur the network deforms: the degree distribution changes, the specified paths change, and thus the betweenness values change. Therefore if one was to reorder the edges after a failure, the ranking may differ, sometimes drastically.

The choice of recalculating the rank ordering parameter after every single failure is computationally cumbersome, but is important for certain failure models. It has been discussed how betweenness measures reflect the congestion along the elements in a network under a simulation where agents starting from a specific source node travel along the network on specified paths until they reach their targets.

In this context, it is reasonable to consider the example of a highway network. If failures on the network were to be caused by congestion, the real physical situation would be that far too many vehicles try to move along one highway such that the traffic flow along this highway comes to a stop, which means that this link is no longer functional. Once this link fails, drivers who would have chosen to move along that link if it hadn't failed start to move to a new path, one that does not contain this failed highway, until that highway becomes

jammed too. Conversely, the failure of low betweenness valued elements may be caused by lack of maintenance of the link.

On the other hand, choosing not to recalculate the actual ranking after failures has its own benefits in terms of the physical representation of the model. From an attacker's point of view, most probably recalculation makes no sense, as the attacker does not have the luxury of waiting for the flow along the network to balance itself according to the new imposed conditions. Instead the reasonable thing to do from his perspective would be to rank the elements once at the beginning, and attack a certain portion of the edges, starting from the highest. Then the ratio of edges that have failed can mirror the damage capacity of the attacker.

From this point on in this work, the simulations where the recalculation procedure is carried out will be referred to as *continous ranking*, and those in which the ranking is carried out prior to failures and never again will be referred to as *simple ranking*.

5.3. Measured Network Parameters

After every failure the network is altered. Depending on the chosen ranking method and the state of the network, the changes in the network parameters can be big or small. The simulations in this work monitor five different parameters of the network after failures.

5.3.1. Percentage of Failed Edges

The simulations move forward along a generated network by failing edges one at a time, therefore the independent variable in these simulations is the number of failed elements. For better tractability, this number is divided by the initial number of edges in the network to obtain the *percentage of failed edges*.

5.3.2. Fragmentation Ratio

As previously stated, failures can be defined in different ways, depending on the function of the network. However most networks primarily model flows: particles moving along the edges with the goal of reaching a specific target. In this sense, any event under which the probability of reaching a target becomes zero for a particle is a certain failure scenario.

A simply connected network consists on n many nodes where any one node can reach any other, either via a lengthy path, or very quickly. If the network was disconnected though, the number of components would increase, which means no member of one component can reach the members of another component. Therefore as failures occur, keeping an eye on the number of disconnected components can be a reflective measure of how damaged and non-functional the network has become.

For a better understanding, the measure is normalized by n to be fixed in the unit interval, and called the *fragmentation ratio*.

5.3.3. Ratio of Disconnected Node Pairs

Related to the number of components, this measure also bears in itself the sizes of the components formed. This point is critical yet not covered by the previous parameter, since the disconnection of a network with $n = 100$ into two components of order 1 and 99 or 50 and 50 cannot be considered similar failures only because the number of components are identical.

If there were an agent for every node pair (i, j), such that it would start from i and move to reach j, for a disconnected network, all agents with these two nodes in different components would have no possibility of reaching their targets. The number of these agents is this parameter called the *number of disconnected node pairs*.

If n^i were to denote the number of nodes of the component labelled i,

$$\text{number of disconnected node pairs} = \sum_{i \neq j} n^i n^j. \tag{5.6}$$

For easier interpretation, this measure can be normalized by the number of disconnected node pairs of an empty network,

$$\text{ratio of disconnected node pairs} = \frac{\sum_{i \neq j} n^i n^j}{n\left(n-1\right)/2}. \tag{5.7}$$

5.3.4. Clustering Coefficient

The clustering coefficient of the network is a measure of how locally redundant a network is, since a node with a high clustering coefficient has a high number of edges connecting its neighbors and the number of alternating paths emanating from that node are also plenty. Therefore this measure can also be interpreted as an indicator of the number of alternating paths in the network.

5.3.5. Efficiency

As the failure magnitude grows, the lengths of the paths between two given nodes in the network also grow. This means that extra energy has to be spent to do the same work of reaching from one node to another. If the energy spent on moving from one node to another was proportional to the length of the path chosen, then the minimum energy would be spent by moving along the shortest path.

However summing these lengths can be technically difficult when the network becomes fragmented, since in that case, the distances between disconnected pairs reach ∞ and summing over these values is meaningless. To overcome this issue, the efficiency parameter is proposed.

Efficiency of a network is defined as the sum of the inverses of the shortest paths between nodes [44]. In mathematical form,

$$\text{efficiency} = \sum_{i>j} \frac{1}{l_{ij}}. \tag{5.8}$$

This measure ranges between 0 and 1, where 0 means that the given network consists of a number of isolated nodes, and all shortest path length values are equal to ∞. An efficiency value of 1 means every node can reach every other node in one step, which points to a complete network.

6. VULNERABILITY ANALYSIS FOR EDGE FAILURES ON NETWORKS

Vulnerability and robustness of complex networks against random failures and targeted attacks of nodes is investigated in [45, 46, 47, 48], however the failure of edges is generally overlooked. The analysis in this work is the result of twenty randomly generated network ensembles of each type, with $n = 32, 64, 128$; and $\bar{k} = 4, 6, 8$. Every simulation is carried out with both simple and continuous ranking.

6.1. Ring Structures

6.1.1. Continuous Ranking

Figure 6.1 depicts the fragmentation process of a ring substrate. For $k = 2$, the structure becomes a single cycle, the first failure makes the network a tree, and every next failure causes disconnection, regardless of the failure scheme.

As the average degree is increased, the consequences of different failure schemes start to differ. In terms of the speed of fragmentation, failure of lowest average degree links seem to be the most critical scheme, as one would expect. Attacking the most vulnerable edge of the network at every deformed state is the method that will disintegrate the network as quickly as possible. However this method is not very damaging to the network performance, at least not as much as the failures of high betweenness valued links, which causes failures of bigger magnitudes.

In terms of the betweenness methods, it is important to understand that not all edges have the same betweenness in the initial structure. The edges that connect points that are farther apart have higher betweenness values, since they act as shortcuts for paths created by links that cover smaller distances. Therefore if the links with high betweenness values were failing, the first failure would occur on one of these longer ranged links. This failure creates the asymmetry that creates the extra stress that is shared by the elements nearby; in other

words, the paths crossing that portion of the ring now have fewer alternatives, therefore the links that carry this extra burden become the links with the highest betweenness values, and this damaged portion would be attacked until the connection is no longer there, and the ring is no longer a ring but rather an arc. Then the highest betweenness values would concentrate on the middle of this arc, since the most node pairs consist of one node from one side and one node from the other side. The process would go on to disconnect these arc portions from the middle until all nodes are isolated.

On the other hand, if the link with the lowest betweenness value were to fail, then, the shorter ranged links would fail until the point where so few of them are left that they become more important than a few of the relatively longer distance links. This process continues towards the failure of longer ranged links, until the network is totally isolated. This failure scheme keeps the network connected until the latter stages.

One important point is that the random walk betweenness and the shortest path betweenness ranking methods do not seem to make any difference.

Similarly, the failure of the highest average degree links keep the network connected with the most possible number of failures, since the failures repeat a cycle that starts with a node losing a degree, and all others losing one as well. Only after all links have lost a degree, the cycle of losing the second degree begins. Therefore failures occur until all nodes have degree 2, which is enough to keep a ring substrate connected.

Figure 6.2 brings out the differences in some methods that are similar in terms of fragmentation speed. The magnitude of the failures of high betweenness valued links cause a very early jump in the number of disconnected pairs: in other words, although slow at fragmenting, these failure schemes are good at dividing the network into larger sub networks, creating failures of bigger magnitudes. Interestingly, failures of those ranking methods that are slower in terms of fragmentation seem to undergo a transition phase where the ratio of disconnected pairs makes a rather quick jump. This is caused by the fact that these methods clear out all redundancies in the network before disconnecting it, or in other words, there still exists a minimum spanning tree until the very late. After that point however, every failure

accounts for a huge increase in this parameter.

As for the local redundancies, although counterintuitive, Figure 6.3 suggests a noticeable increase in the average clustering coefficient of the network when the highest ranked links in terms of betweenness fails. This is caused by the definition of this coefficient: if the number of contacts of a node decrease, there is a chance of an increase in the clustering coefficient of that node. Consider a node, A, with several neighbors, B, C and D, of which D is not connected to the other nodes in this set of neighbors, B and C. The removal of the link between nodes A and D actually increases the clustering coefficient of node A, since node D only contributes negatively. In this context, we can call node D a *bad neighbor* for node A. Most probably, node A is also a bad neighbor for node D, and the clustering coefficient of node D will also increase after the failure of the edge between them. One other process that indirectly contributes to this increase is that a node with zero degree is no different than a node with degree one in terms of its clustering coefficient, hence the disconnection of this node leaves the average clustering coefficient of the network unchanged.

Considering these processes in the larger scale, the high ranked links in terms of betweenness must somehow be those edges that contribute negatively to the clustering coefficient. In the example of a ring substrate with 12 nodes and average degree of 4, the clustering coefficient of every node is $1/2$, since the number of edges connecting the neighbors is 3. When one of the long range edges fail, the clustering coefficient of the node that falls in between this link is decreased to $1/3$, but the nodes that are at the both ends of this link have $2/3$.

A more general explanation can be made by relating the measure of betweenness to that of clustering coefficient. Betweenness values of elements that lie inside certain localities, where there is a high redundancy of alternative paths, is relatively lower when compared to elements that connect these localities, but lie in an unlocalized region themselves. Lying in an unlocalized region with weak redundancies directly results in having a low clustering coefficient. In general, this causes these links or nodes to become the only alternative for the nodes in the local structure to reach other local structures. Therefore, the nodes with high betweenness values are bad neighbors whose removal increases the clustering coefficient,

but good trasmitters such that their failure disconnects the *good neighbors* from the rest of the network.

Also considering the ratio of disconnected pairs at the point where the clustering coefficient peaks, it can be said that at the point the network is so fragmented that it consists of very small connected subgraphs consisting of a few nodes connected with a few edges.

The decrease in the efficiency of the network is shown in Figure 6.4. The results suggest that the fastest decrease in efficiency is caused by the failure of edges with the highest betweenness values. This results is in accordance with the number of pair wise disconnections, since as this number increases quickly, the efficiency rapidly decreases. Therefore it can be considered reasonable that lowest average degree edges are not as critical for the performance of the network, despite being faster at fragmentation, as the betweenness ranking methods.

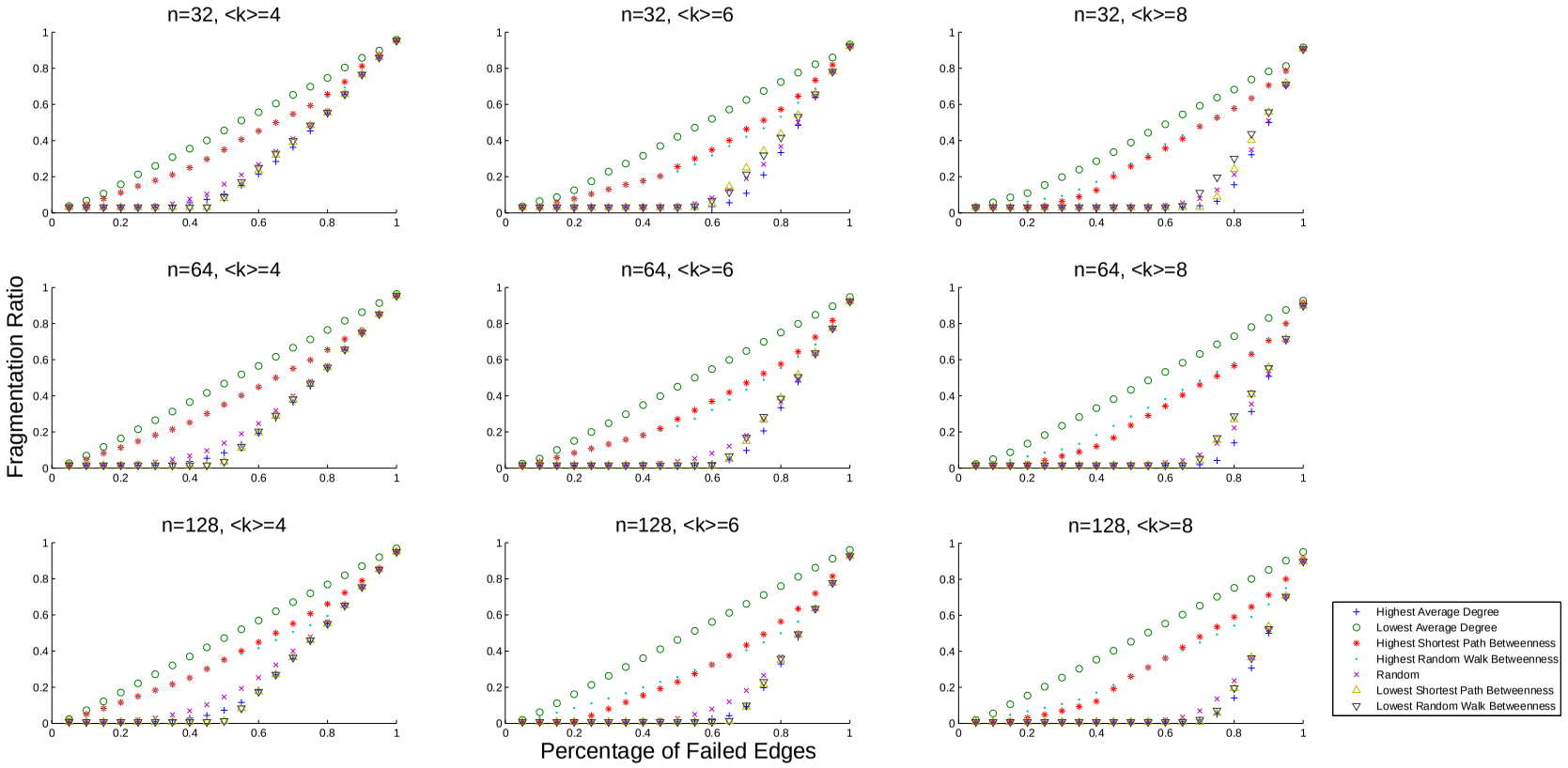

Figure 6.1. The graphs of fragmentation ratio versus the percentage of failed elements of continuous ranking methods for ring substrates of given order and average degree

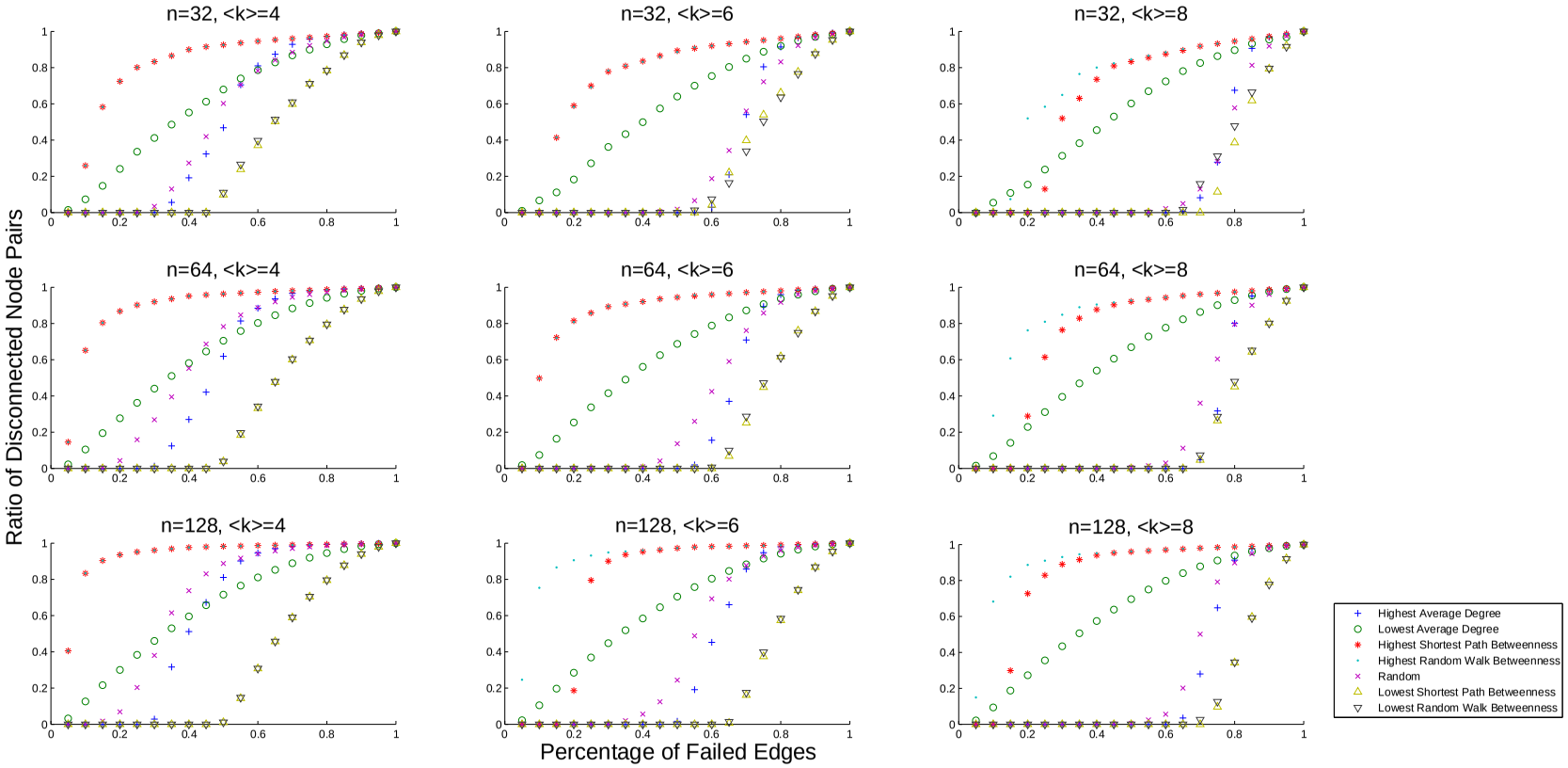

Figure 6.2. The graphs of the ratio of disconnected node pairs versus the percentage of failed elements of continuous ranking methods for ring substrates of given order and average degree

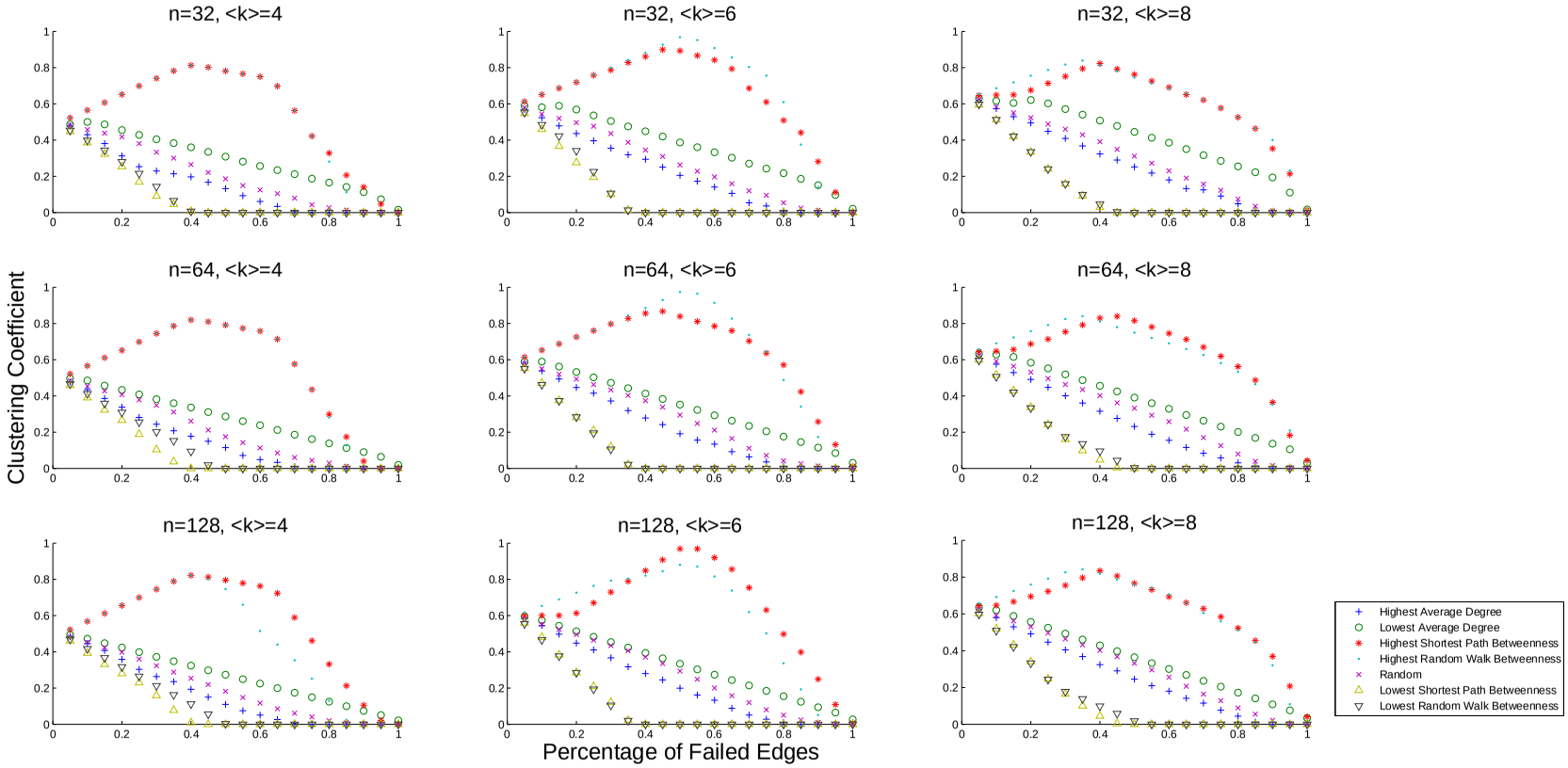

Figure 6.3. The graphs of clustering coefficient versus the percentage of failed elements of continuous ranking methods for ring substrates of given order and average degree

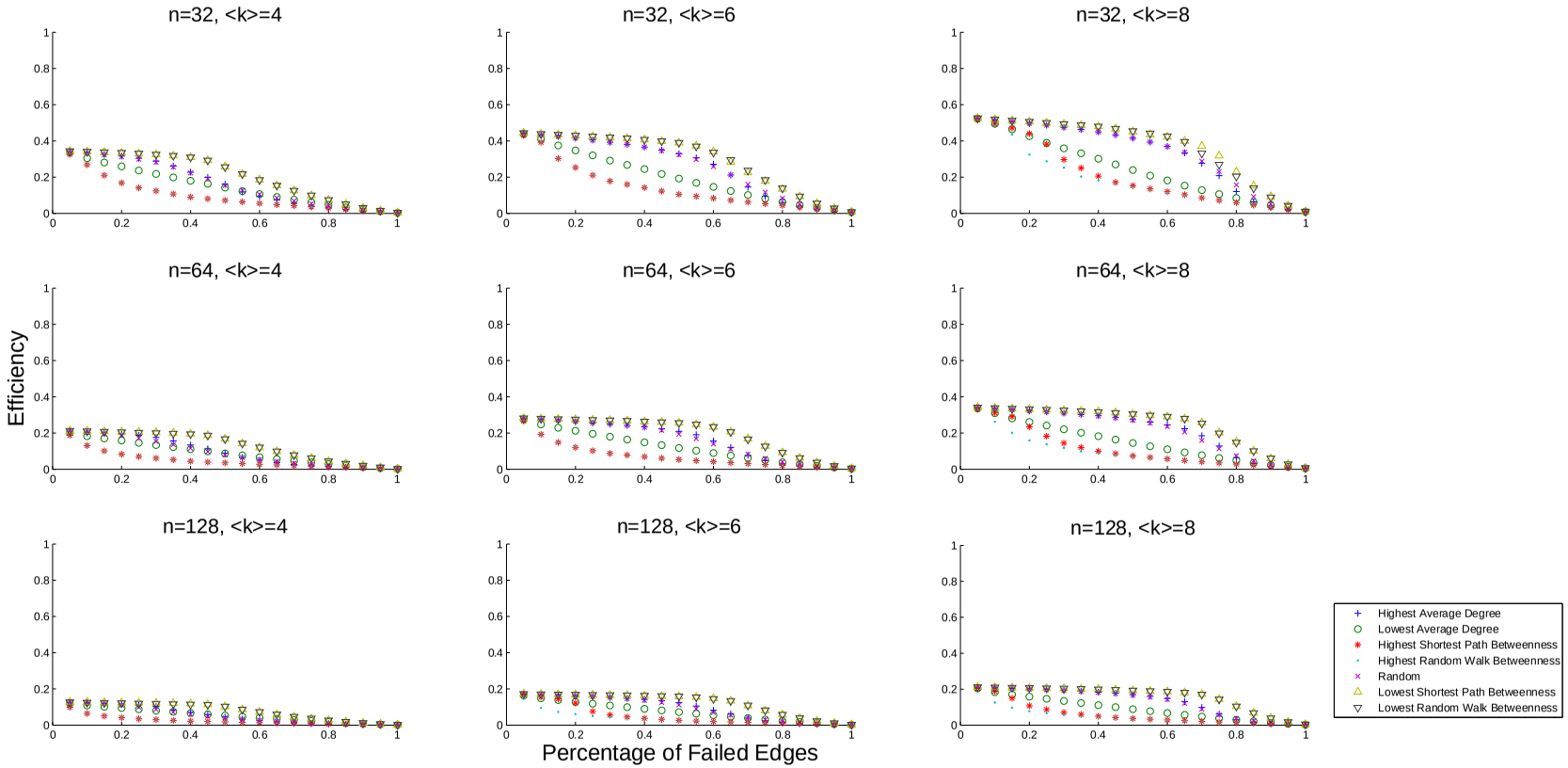

Figure 6.4. The graphs of efficiency versus the percentage of failed elements of continuous ranking methods for ring substrates of given order and average degree

6.1.2. Simple Ranking

For the simple ranking methods, the results are rather interesting, simply because most methods seem to behave similarly. First of all it is important to notice that for the initial form of the ring structure, when the ranking is carried out, all links have the same average degree. The links have only $k/2$ different betweenness values, directly proportional to the geodesic distance inbetween the nodes they connect. In these simulations, if two or more edges have the same minimum or maximum value, one of them is selected randomly for failure. Therefore the procedure becomes no different from the random ranking failure scheme if all edges are ranked equally.

The interesting result of Figure 6.5 is that whatever method is chosen in simple ranking, the fragmentation speed is more or less the same. Therefore for such networks with deterministic degree distributions, simple ranking methods do not make a big difference. Thus it can be said that the most reasonable thing an attacker can do if he is going to go with simple ranking is attacking links at random.

Still though, a slight difference between some schemes can be noticed. The high and low betweenness valued link failures lie at the very bottom, as they bear no difference from the highest average degree failures of continuous ranking: All long ranged links fail, then medium ranged links fail, and so on. Moreover, the failure of the lowest or the highest betweenness edges do not seem to differ either, and the process is pretty much the same, only reversed in some sense.

The random methods lie slightly above others, because there is a slight chance that a certain number of failures may end up happening in such a sequence that the network may disconnect very early. However this probability is rather small, therefore when averaged over twenty networks, the result is only slightly different from others. Figure 6.8 agrees with the results, can only very slight differentiate between these methods in terms of how fast they efficiency is decreased.

Figure 6.6 shows how the ratio of disconnected pairs undergo what can be called a

phase transition, which is expected since once the failures begin, the network is stripped of its redundancies and is very vulnerable, such that every link failure creates a disconnection.

Figure 6.7 does not exhibit the bigger increase in the clustering coefficient as in the continuous ranking methods, but is the only parameter that can differentiate between these methods in simple ranking. High betweennes valued link failures are still slower at reducing the clustering coefficient, since the longer range links are actually *bad neighbors* for the nodes they connect. Therefore until they are all removed, the clustering coefficient stays pretty much the same.

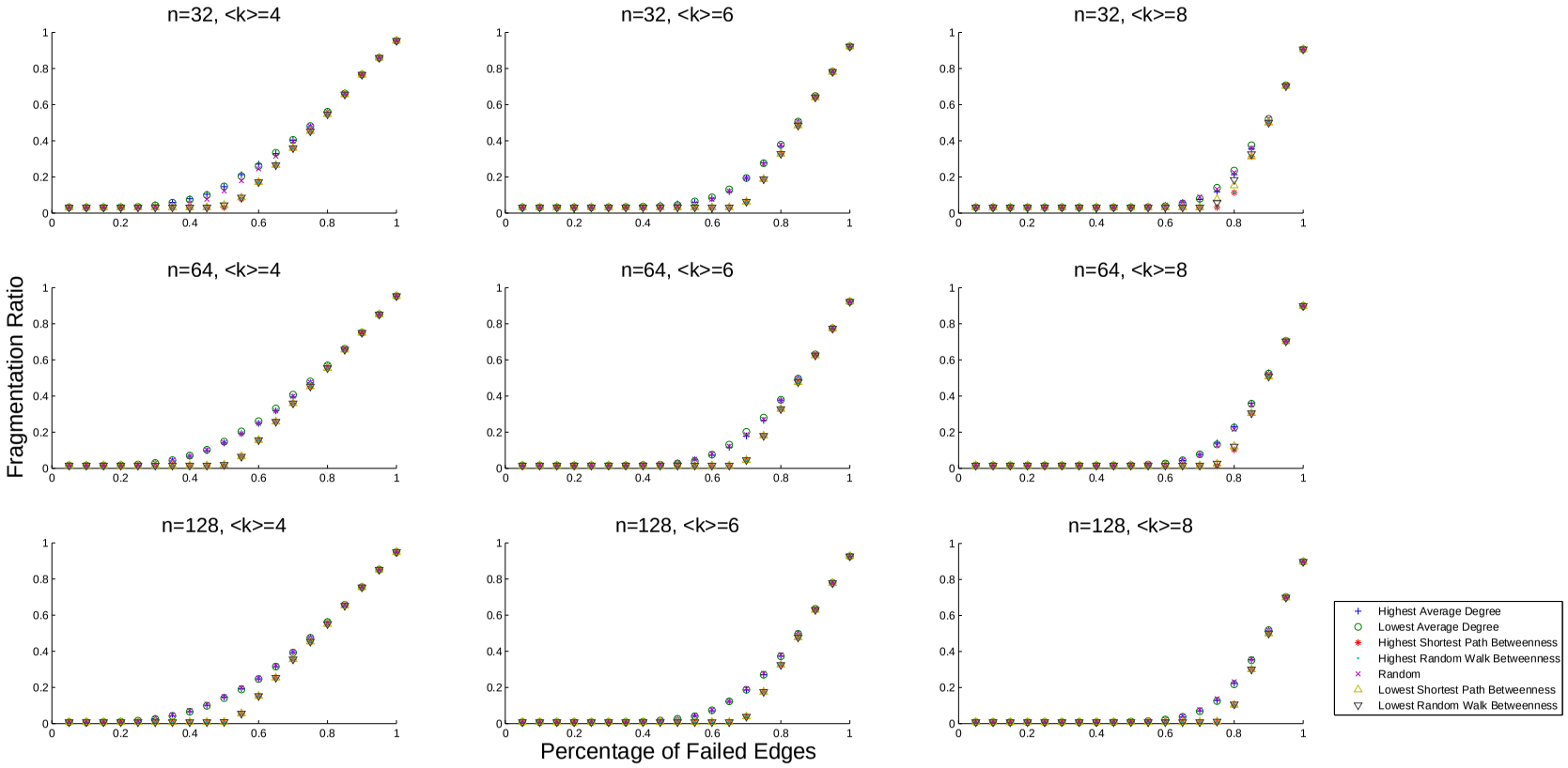

Figure 6.5. The graphs of fragmentation ratio versus the percentage of failed elements of simple ranking methods for ring substrates of given order and average degree

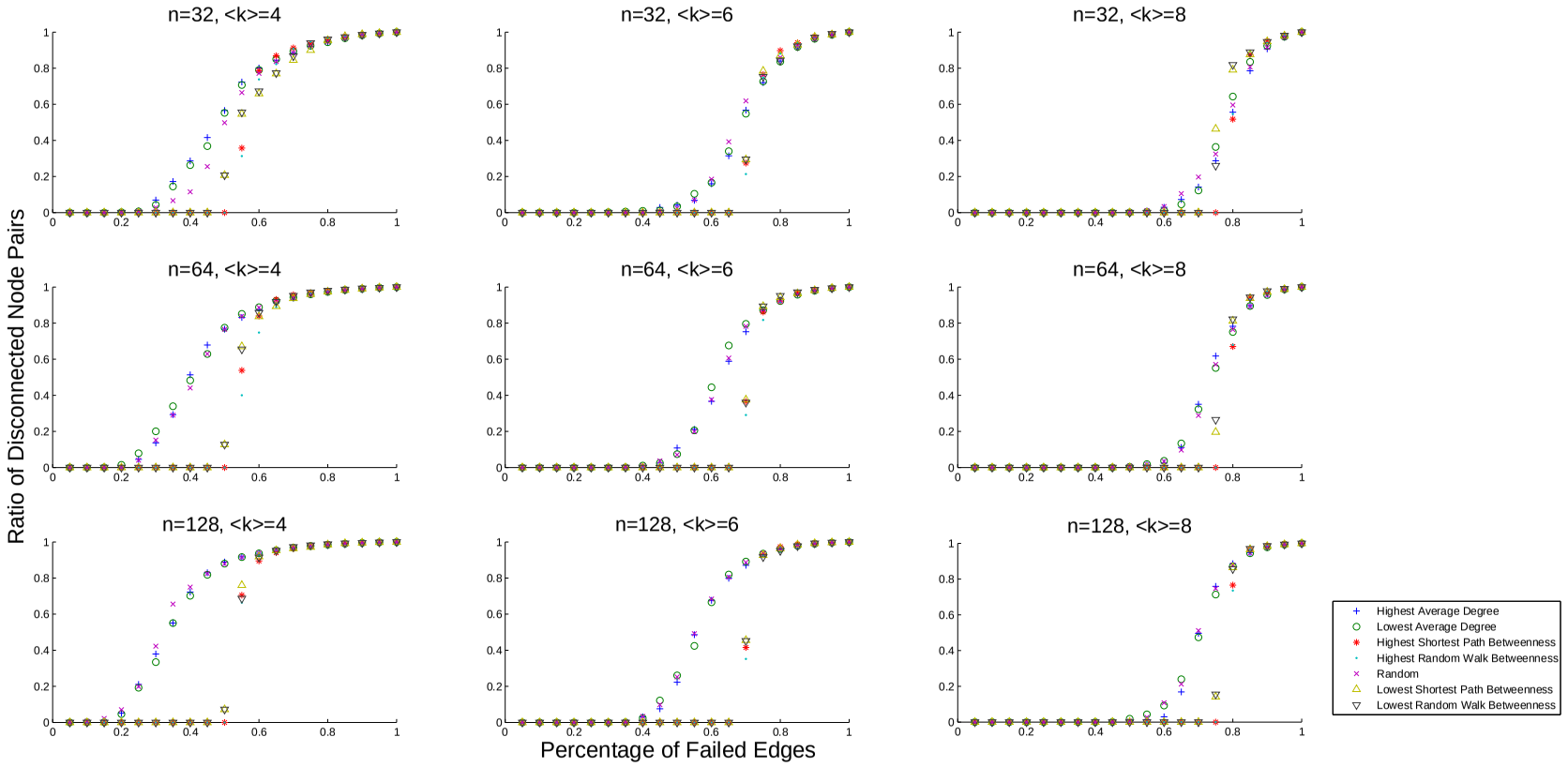

Figure 6.6. The graphs of the ratio of disconnected node pairs versus the percentage of failed elements of simple ranking methods for ring substrates of given order and average degree

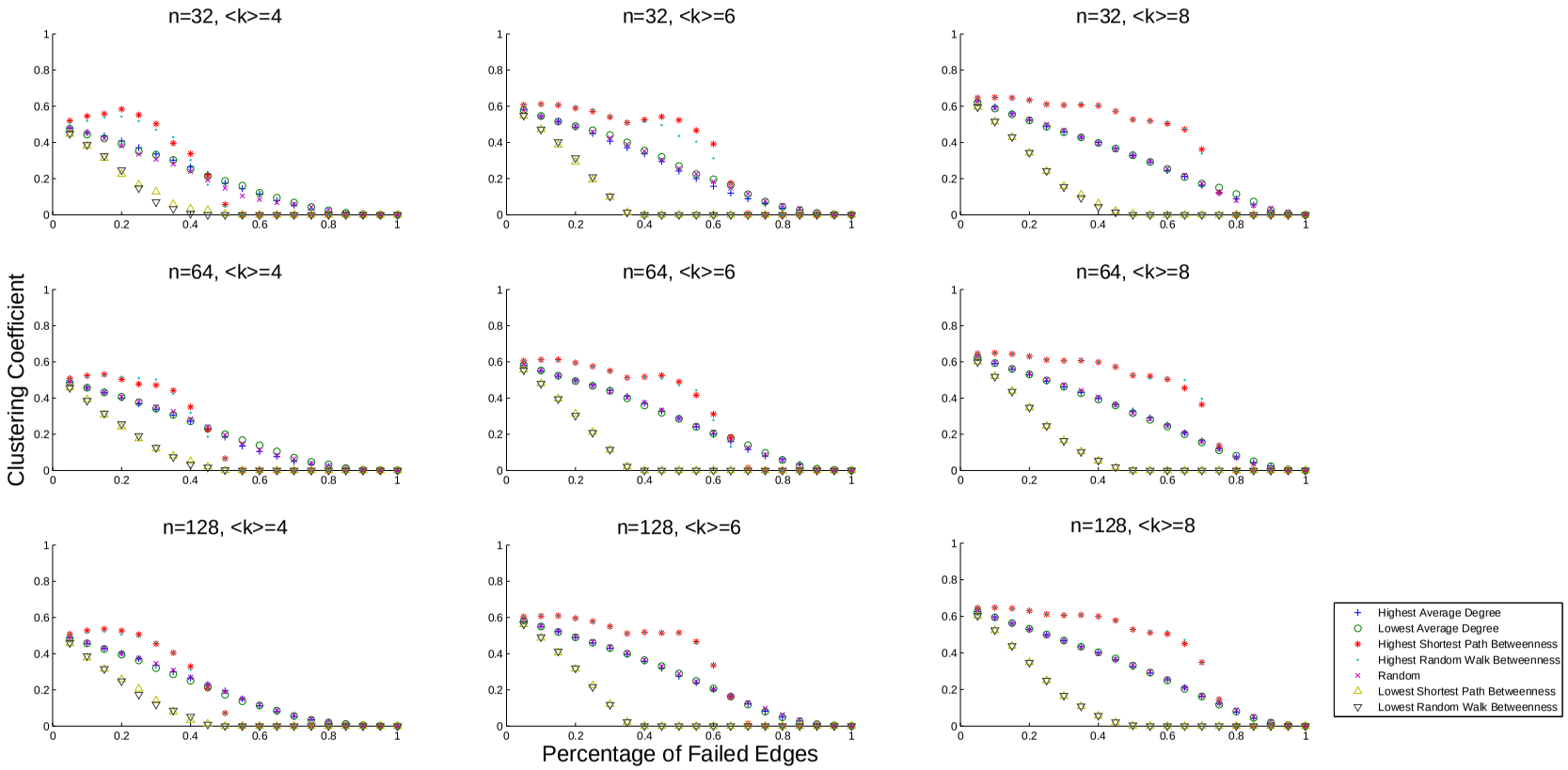

Figure 6.7. The graphs of clustering coefficient versus the percentage of failed elements of simple ranking methods for ring substrates of given order and average degree

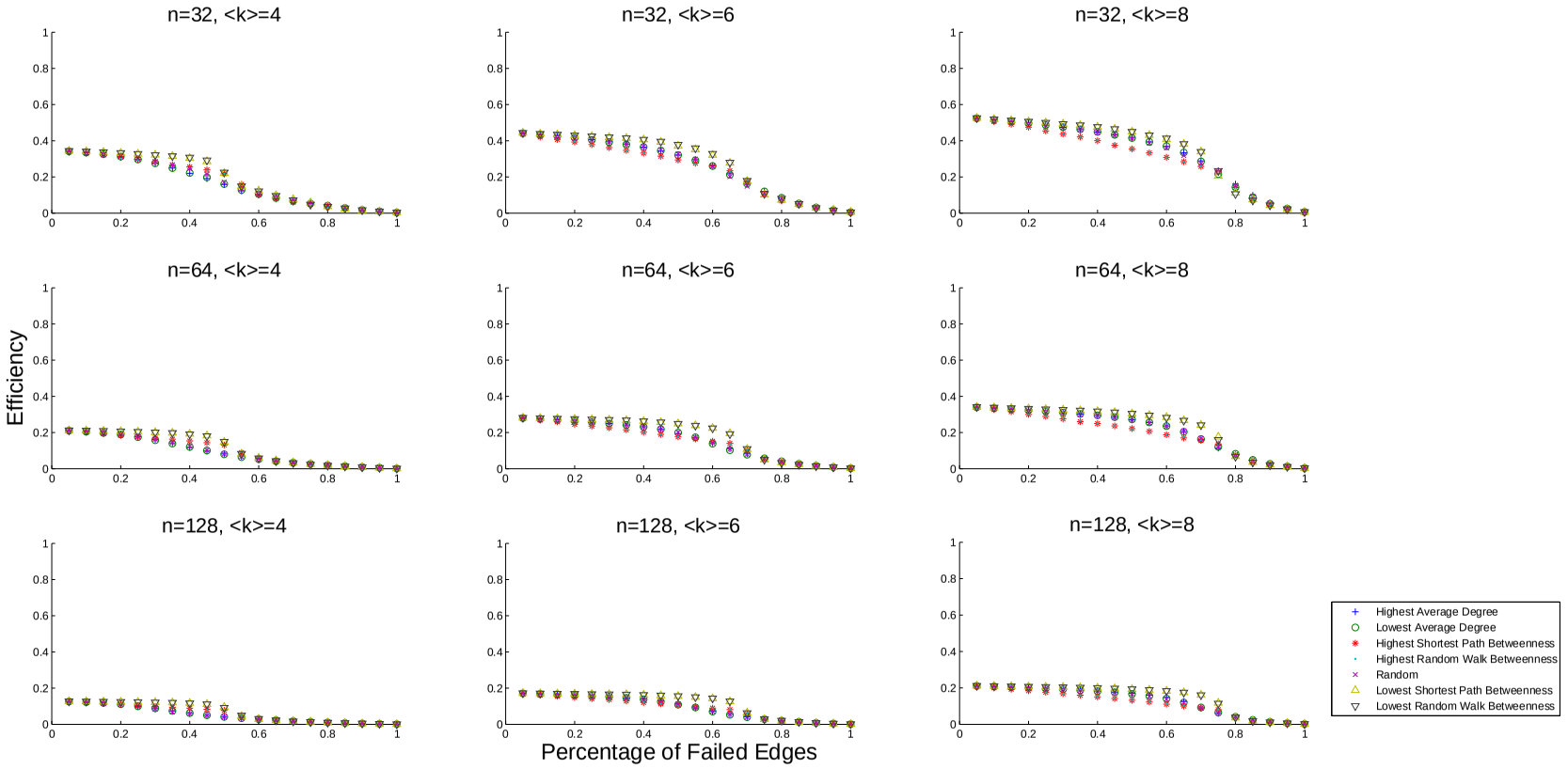

Figure 6.8. The graphs of efficiency versus the percentage of failed elements of simple ranking methods for ring substrates of given order and average degree

6.2. Erdos Renyi Networks

6.2.1. Continuous Ranking

Figure 6.9 suggests for low average degree edge failures and low random walk betweenness edge failures; the linearity of the fragmentation ratio curve depends on the sparsity of the network. For relatively lower average degrees, these schemes are very damaging to the network, as they form the upper bound of the fragmentation curves. As the average degree grows or the network order decreases, i.e. the sparsity decreases, these schemes lose their effectiveness, and the failures of high betweenness valued edges become the most damaging scheme.

This result can be explained by the fact that Erdos Renyi networks only rarely bear any local structure, as proven by the very low average clustering coefficient. Therefore it can be said that betweenness methods fail to make a difference in networks with lower clustering coefficients. Therefore for relatviely more dense networks, these schemes have higher fragmentation curves.

One interesting point that can be made is that for the mentioned more sparse networks, random walk betweenness ranking manages to cause disconnections quicker than the shortest path betweenness ranking. In an almost chaotic and totally random network structure, it is not reasonable to expect shortest path betweenness to return the edges that would disconnect the network, at least not as much as the random walk betweenness, which uses more path information.

For the number of disconnected pairs, from Figure 6.10, it can be seen that failure of the highest betweenness valued links are above the lowest average degree link failures. It has been mentioned that the former method creates larger disconnected components after relatively many link failures, where the latter creates small disconnections with every few links failure. Therefore their position in this figure means out of these two different processes, failure of the higher betweenness valued links cause more loss of connectivity.

The failure of higher average degree links, along with the failure of the lowest shortest path betweenness valued links, form the lower bound. One noticeable difference between the random walk betweenness and the shortest path betweenness can be found here: Although when high ranked link failures according to these orderings results in similar consequences, failure of the lowest random walk betweenness valued links induces an increase in disconnections a lot earlier than that of the shortest path betweenness. A low shortest path betweenness value suggests that that specific link lies only on a few shortest paths, compared to other links, however for random walk betweenness, the paths that are longer than the shortest path make a difference: These links will definitely be considered as more central, since one way or another they are going to lie on some path, long or short, which will contribute to their betweenness value. Therefore it can be expected that the links with the lowest random walk betweenness values are not as far from the mean random walk betweenness value than the lowest shortest path betweenness valued links.

Figure 6.11 shows that the local structure is very weak for Erdos Renyi networks, which is understandable since the construction procedure is totally random. Therefore its disappearance is not very apparent. However the increase in the average clustering coefficient for the failure of links with high betweenness values can be immediately noticed. The parameter peaks at the points where about 60 percent to 90 percent of all edges have failed, which corresponds to a ratio of disconnected pairs very close to a hundred percent.

At this point, the network consists of very little connected subgraphs that have the smallest number of *bad neighbors* as possible, which causes the slight increase in the clustering coefficient. It should be noted though this increase is also caused by the very low clustering calues at the initial formation. Another reason is the relationship between the betweenness measures and the clustergin coefficient. As previously stated, the clustering coefficient is also an indicator of abundance of alternative paths, which means there are more number of paths sharing the load between any source-target pair. A low clustering coefficient signals a few number of incoming or outgoing edges from vertices, being the only option in or out. This sort of dependency of a node to an edge requires the edge to stay unconnected to the other neighbors of the node, but open up to new regions of the network. Therefore it is reasonable to expect the failures of high betweenness valued edges to cause the removal of

the *bad neighbors*, and thus increase the overall clustering coefficient by a certain amount.

For the network performance, it is seen in Figure 6.12 that the schemes that constitute the lower bound for the number of pair wise disconnections are the upper bound for the efficiency of the network, and vice versa. It is reasonable to think that these two measures are reflective of one another.

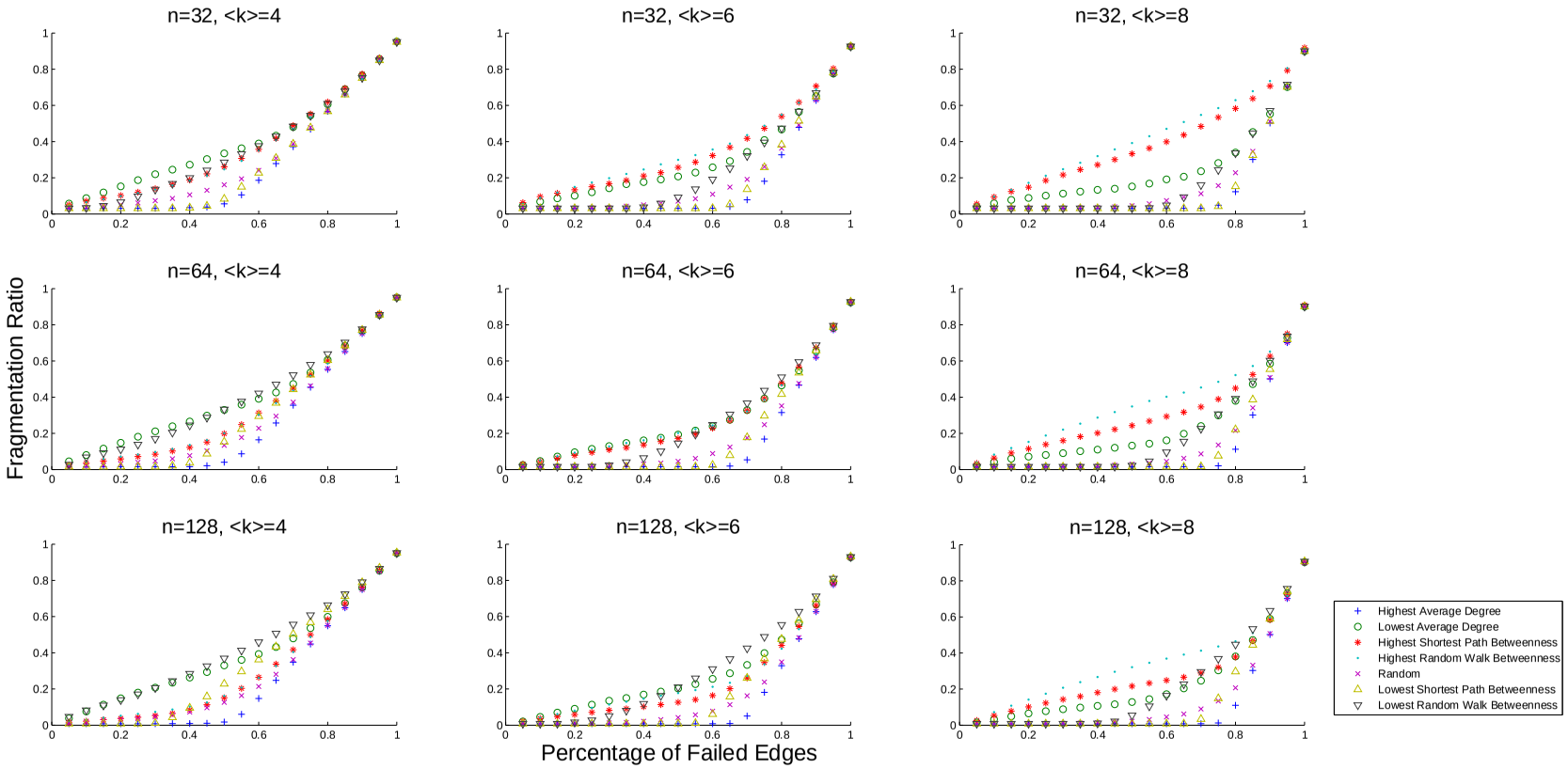

Figure 6.9. The graphs of fragmentation ratio versus the percentage of failed elements of continuous ranking methods for Erdos Renyi networks of given order and average degree

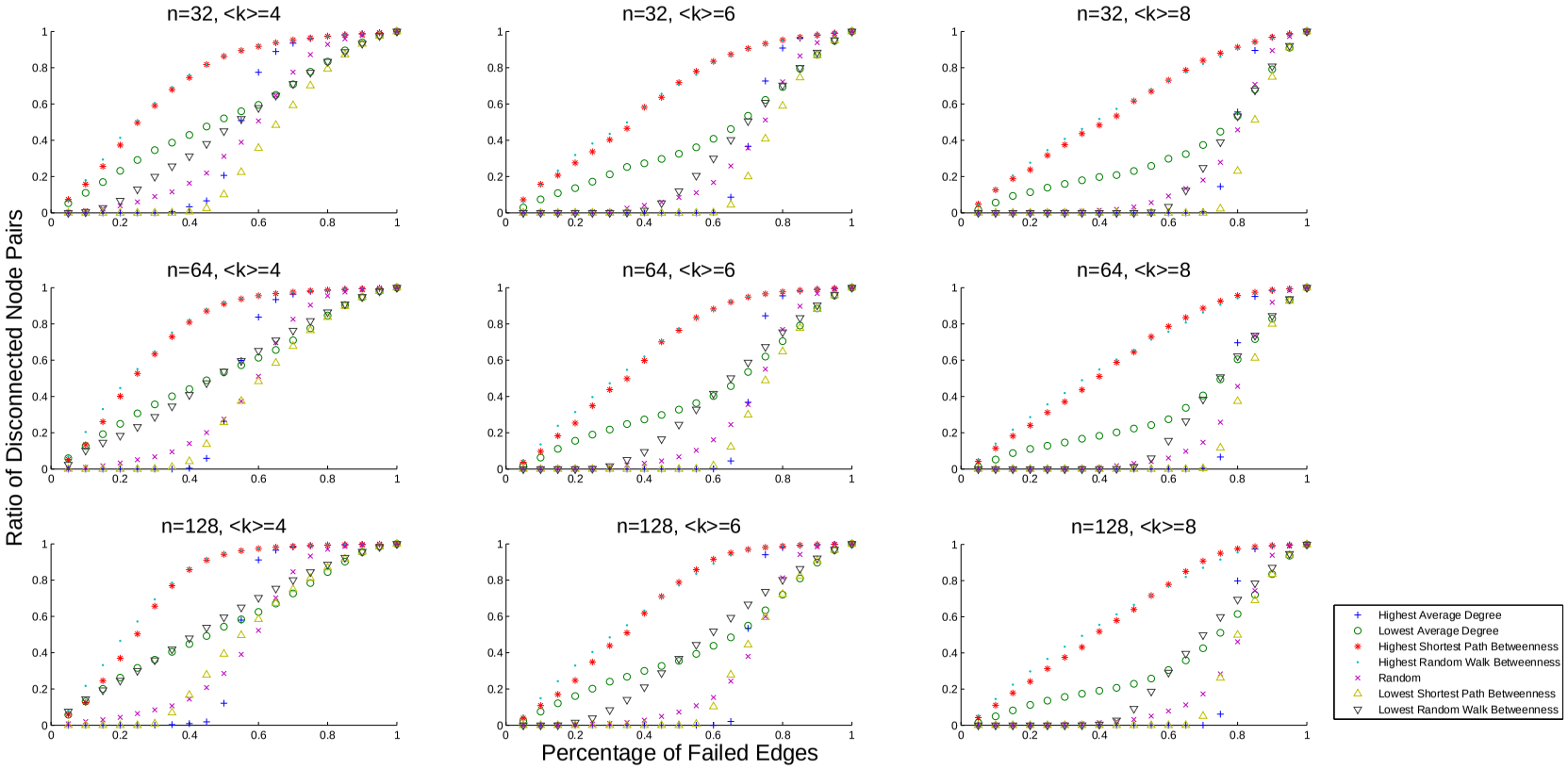

Figure 6.10. The graphs of the ratio of disconnected node pairs versus the percentage of failed elements of continuous ranking methods for Erdos Renyi networks of given order and average degree

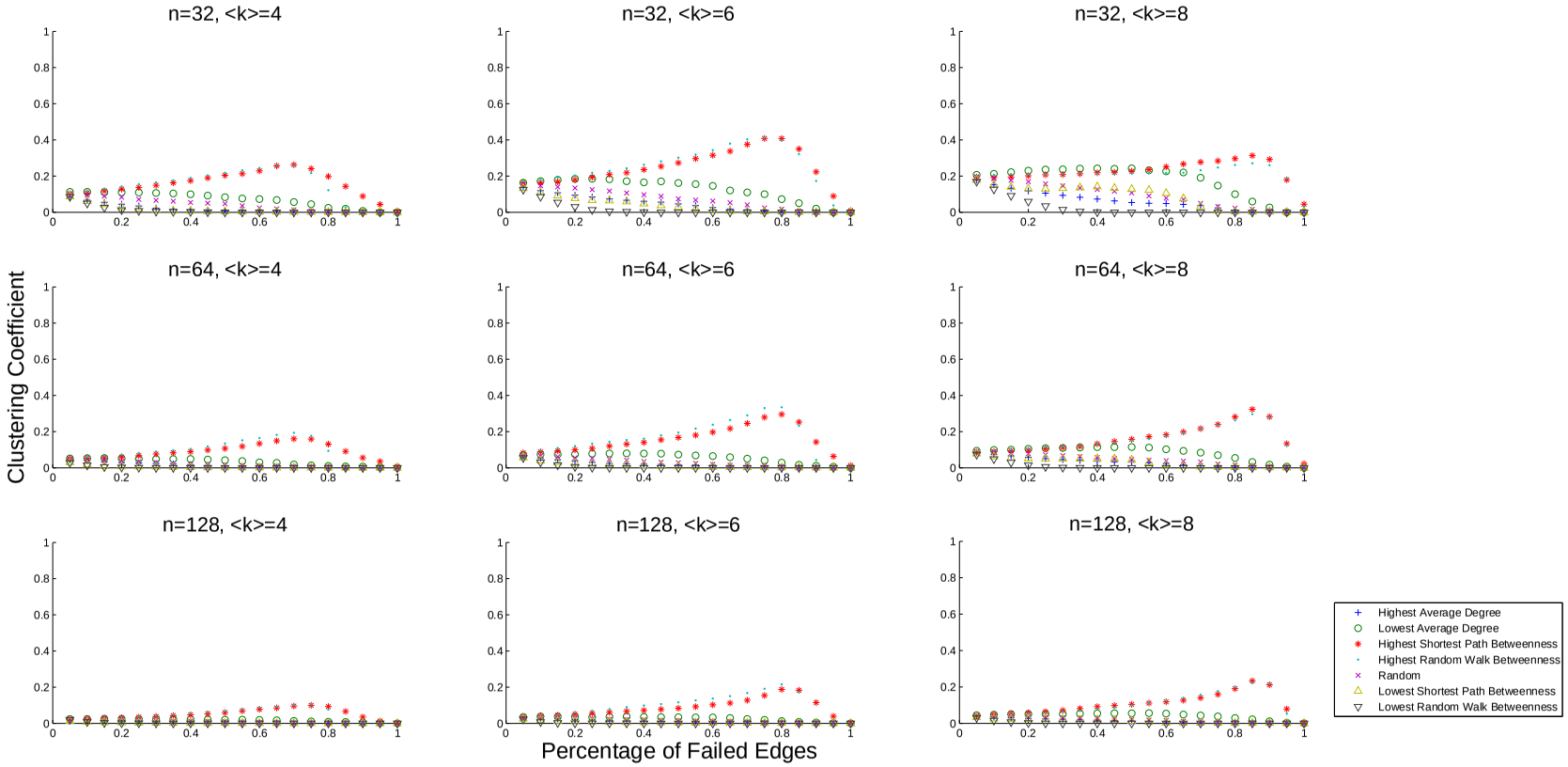

Figure 6.11. The graphs of clustering coefficient versus the percentage of failed elements of continuous ranking methods for Erdos Renyi networks of given order and average degree

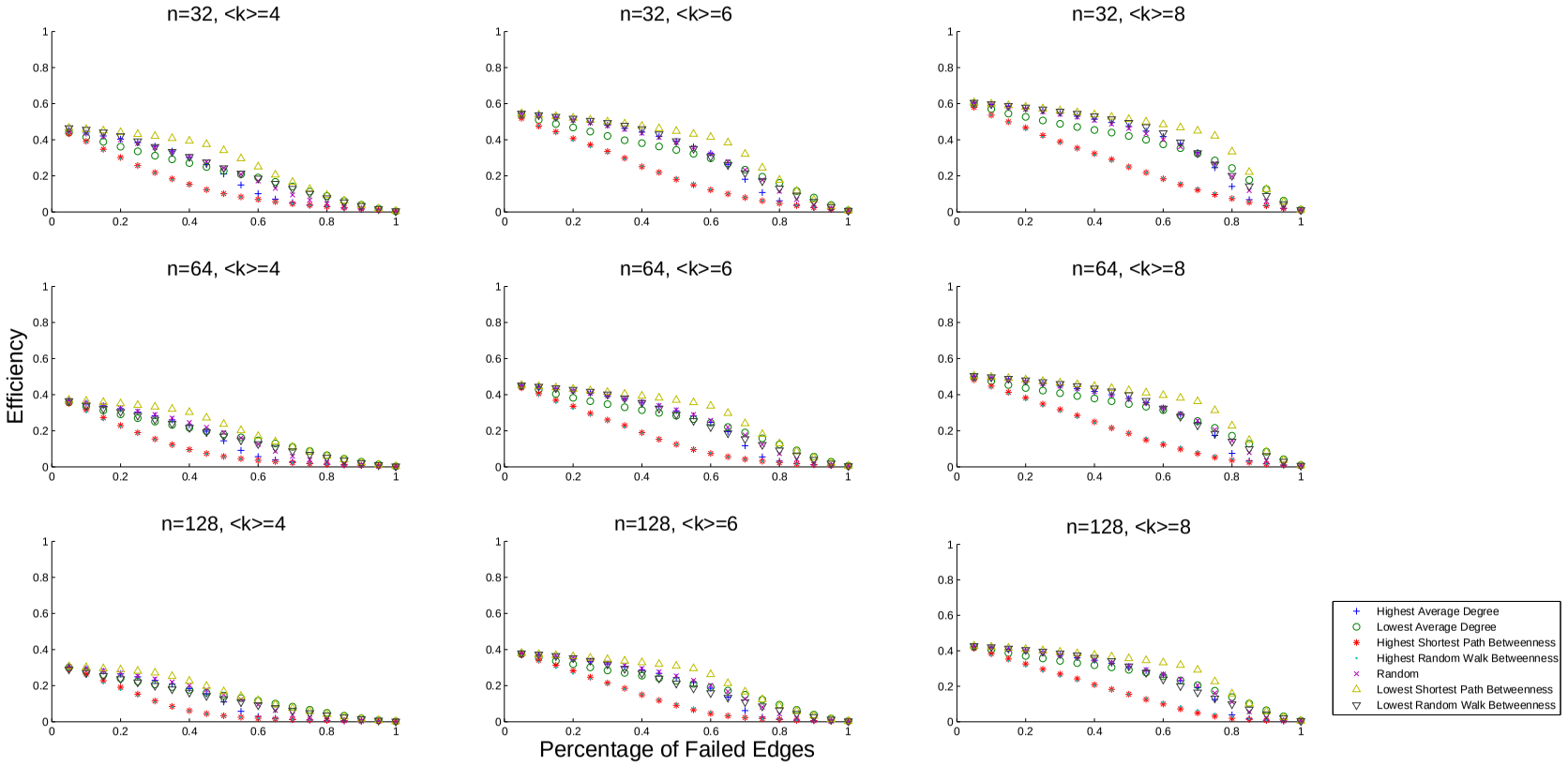

Figure 6.12. The graphs of efficiency versus the percentage of failed elements of continuous ranking methods for Erdos Renyi networks of given order and average degree

6.2.2. Simple Ranking

Simple ranking, as the case for ring substrates, fails to differentiate between several ranking methods. Figure 6.13 shows how all methods remain slow to disconnect the network when compared to the continuous ranking methods.

One interesting result is how the failure of high shortest path betweenness valued links fails to differ even slightly from that of low shortest path or low random walk betweenness valued links. The reason for this result is that for totally random and chaotic network formations such as the Erdos Renyi network, the shortest path betweenness distributions have a relatively normal distribution with very little variance, when compared to that of a scale free network which has a power-law distribution of edge shortest path betweenness values. Therefore the difference between a high betweenness link and a low betweenness link is very small, and for larger Erdos Renyi networks, the difference becomes very indistinguishable, so much that the fragmentation curves for this method bears no difference from that of the random ranking method.

However this is not the case for the random walk betweenness values, where the difference between the variances of the edge random walk betweenness distributions for these two network types is not of the same order as that of the shortest path betweenness distributions. Therefore the distinction between a low and a high random walk betweenness value does make a difference, as in Figure 6.13. Figure 6.14 shows the ratio of disconnected pairs through failure, but pretty much reflects the same results as that of Figure 6.13. One interesting point is that all schemes tend to display a transition phase, where there is a quick increase in the ratio of disconnected node pairs, and after that increase the curve settles and converges slowly to 1.

As for the clustering coefficient, from Figure 6.15 it can be seen that the increase for the high betweenness failure schemes is not so visible once the simple ranking method is used. This clearly is caused by the inability of the simple ranking to capture the shifts in paths throughout the network as failures occur, which can be drastic for a very disordered Erdos Renyi network. The same reason lies beneath why any of the methods fail to make a

drastic difference for the efficiency drop, as in Figure 6.16. The lowest average degree and high random walk betweenness valued edge failures are again more successful in terms of efficiency drop, but the difference is very small. The conclusion that can be made here is that for an Erdos Renyi network, once a certain amount of edges fail and the network is at a deformed state, the paths and initial rankings all lose their effectiveness, because the paths have all shifted and one edge that was not as important is very probably the most important edge at that deformed state.

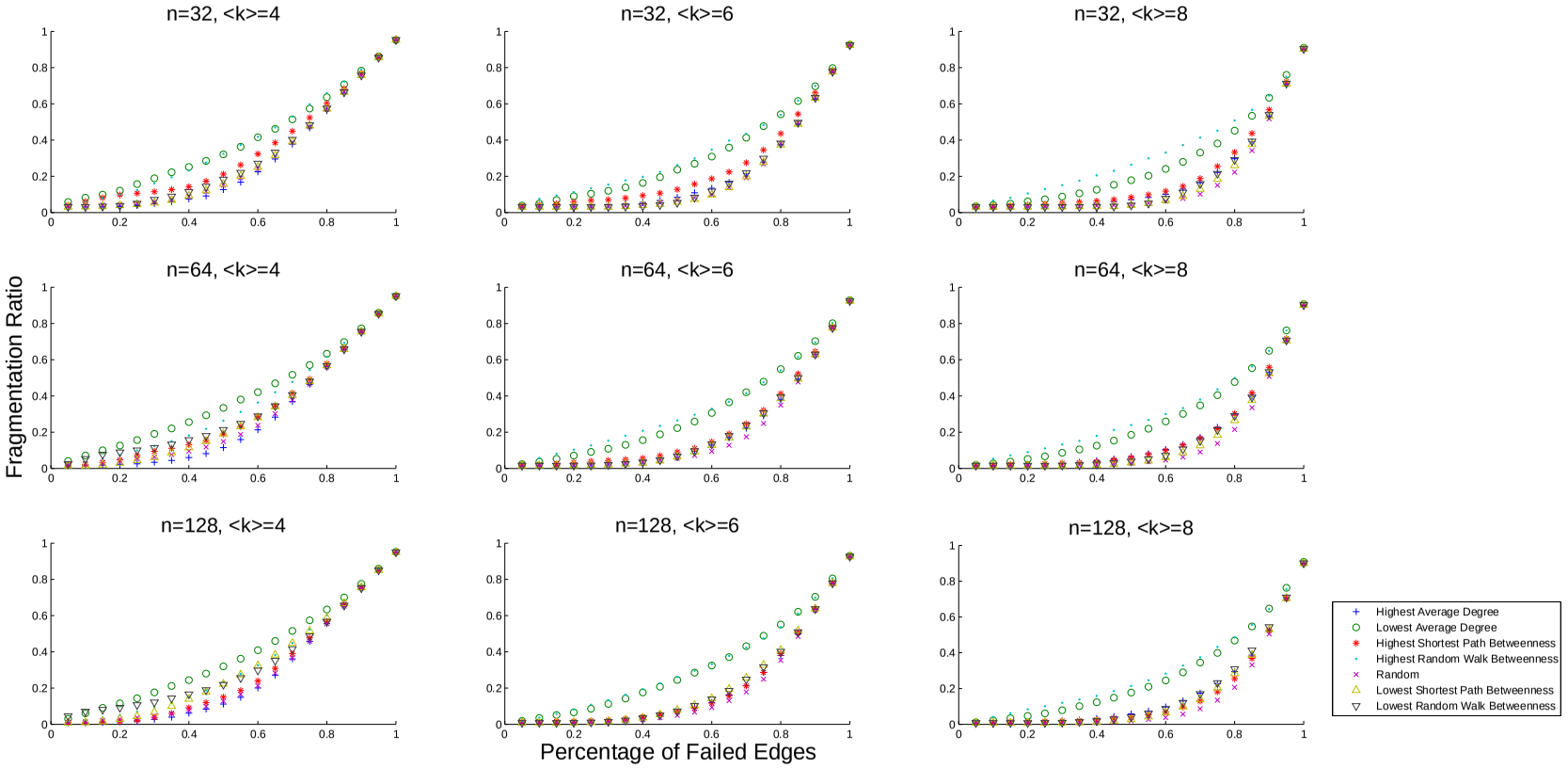

Figure 6.13. The graphs of fragmentation ratio versus the percentage of failed elements of simple ranking methods for Erdos Renyi networks of given order and average degree

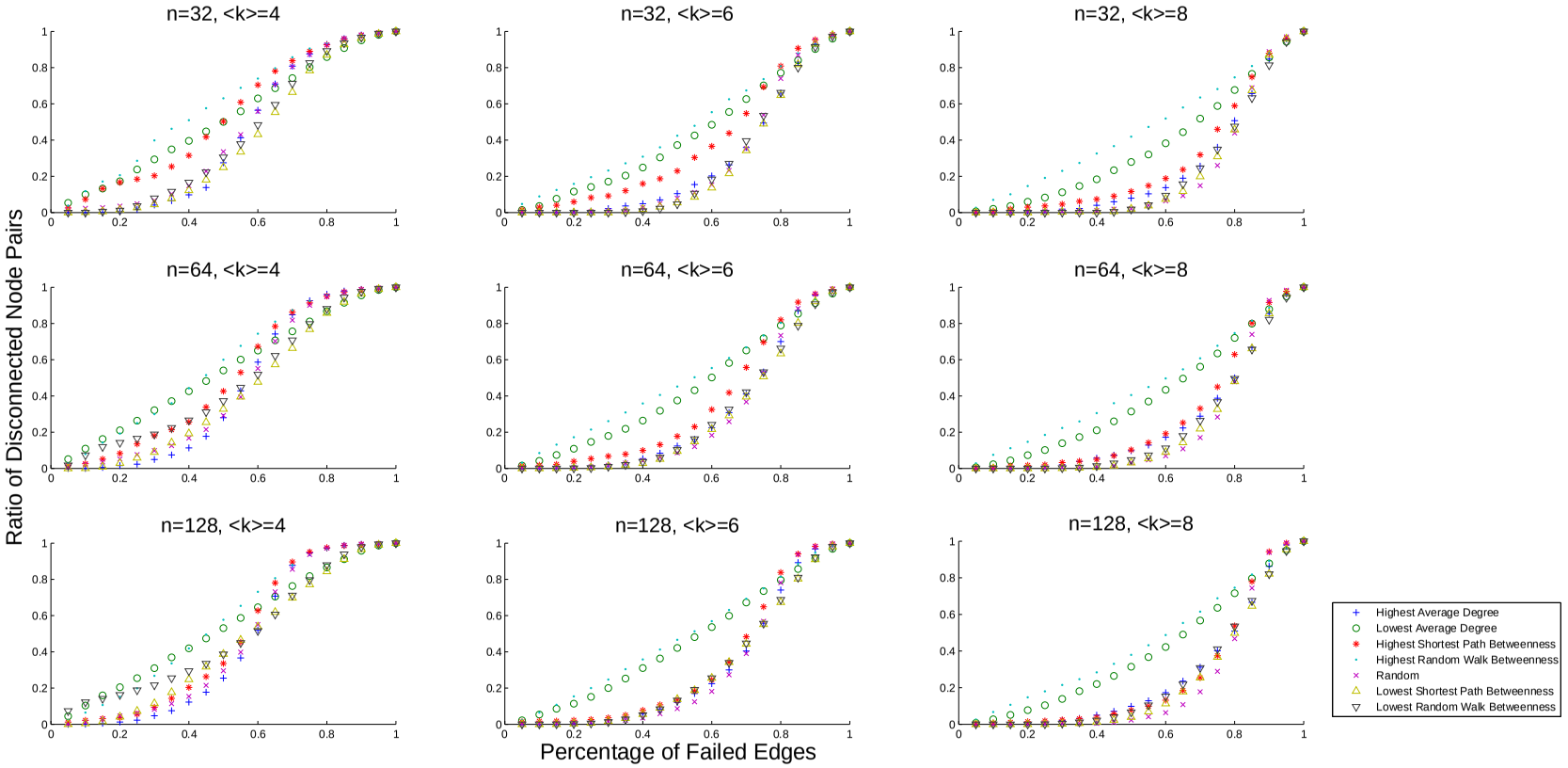

Figure 6.14. The graphs of the ratio of disconnected node pairs versus the percentage of failed elements of simple ranking methods for Erdos Renyi networks of given order and average degree

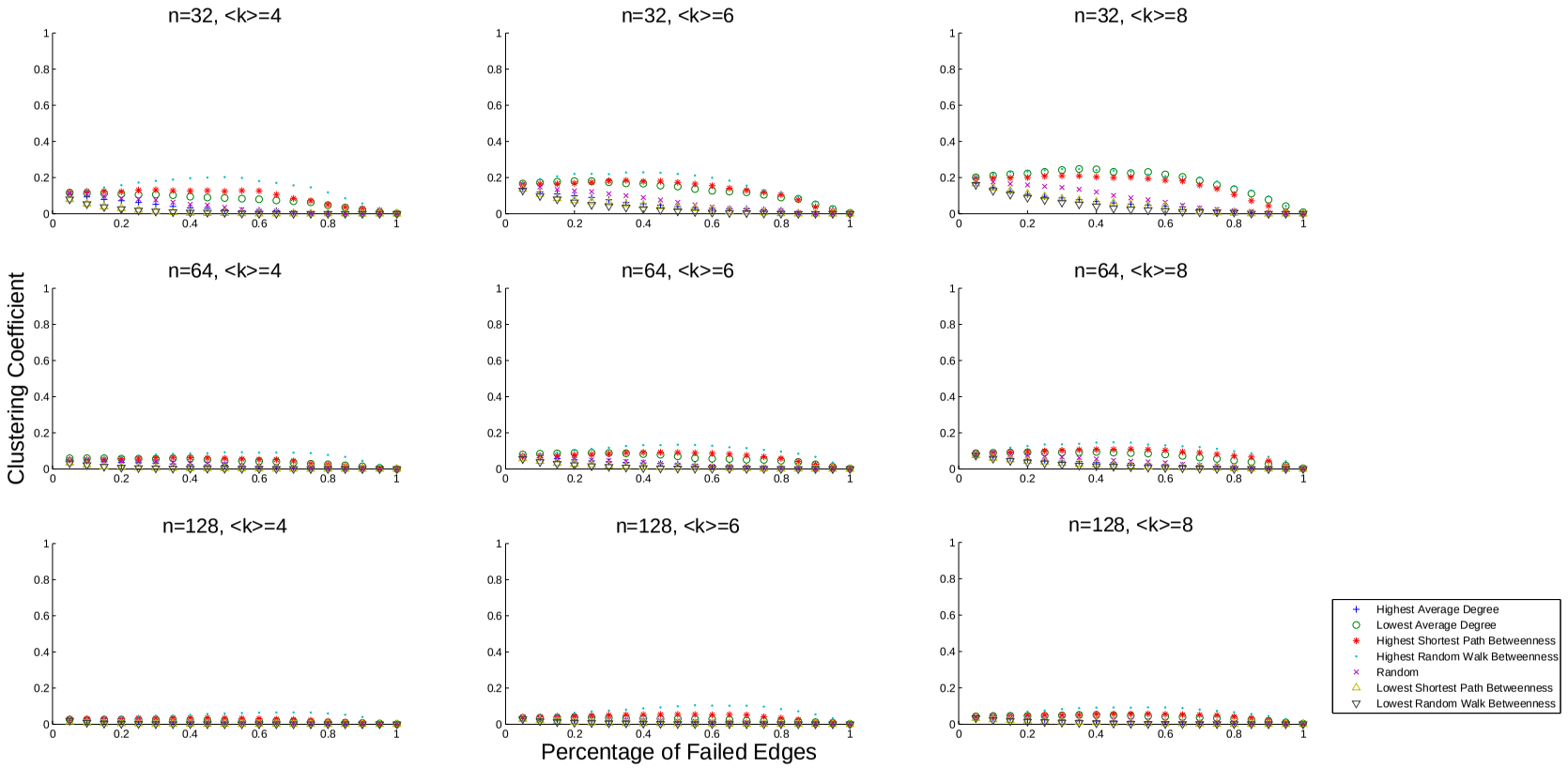

Figure 6.15. The graphs of clustering coefficient versus the percentage of failed elements of simple ranking methods for Erdos Renyi networks of given order and average degree

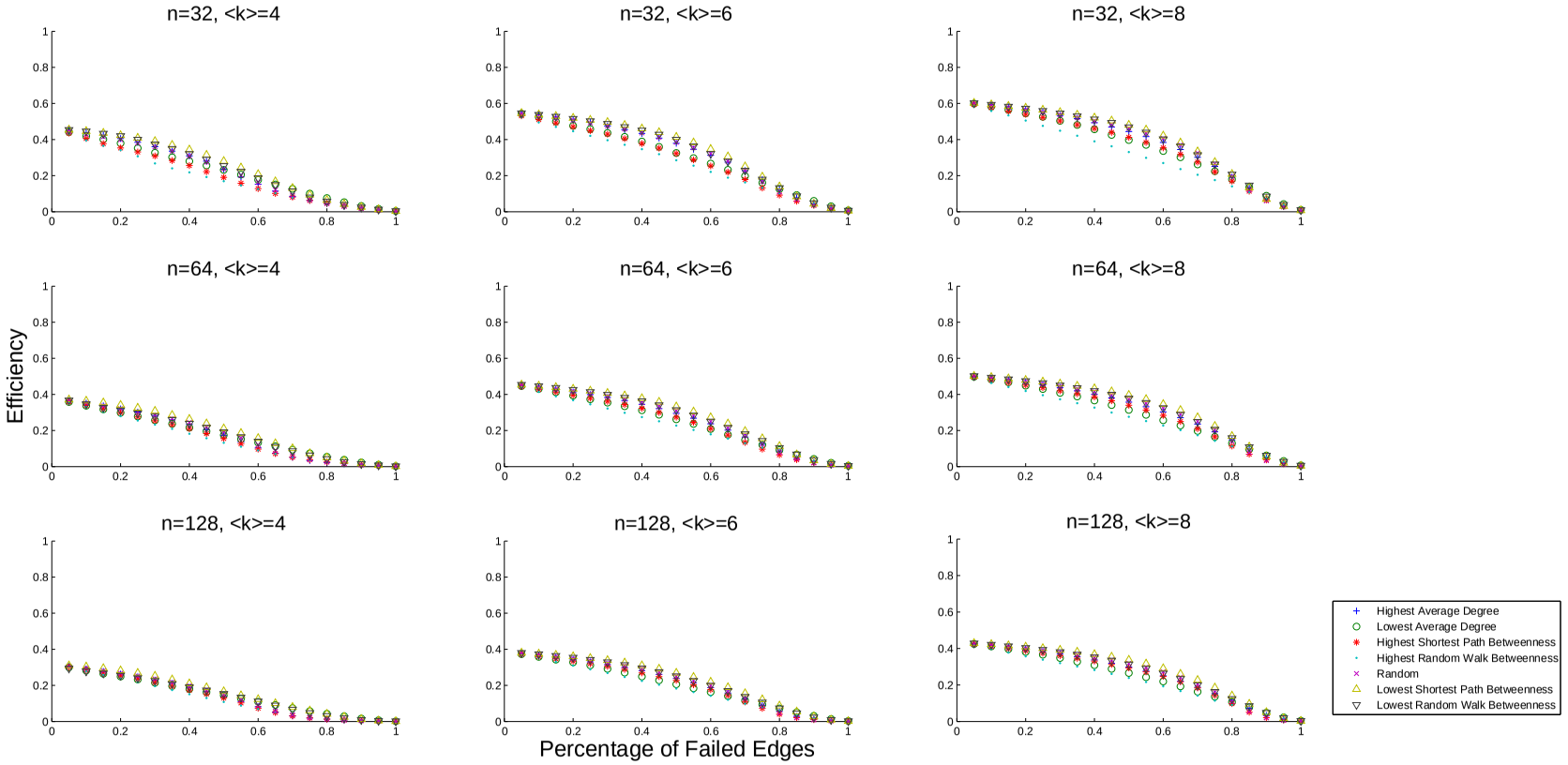

Figure 6.16. The graphs of efficiency versus the percentage of failed elements of simple ranking methods for Erdos Renyi networks of given order and average degree

6.3. Scale Free Networks

6.3.1. Continuous Ranking

As mentioned, scale free networks are generally defined by the slope of their degree distribution on the logarithmic plot. This slope defines the average degree, depending on the size of the network. Scale-free networks in real life generally have slopes between -2 and -3, and the average degrees are very small when compared to the network size.

One very characteristic property of the scale free networks is their disassortative nature. The hubs are most often connected to low degree nodes, therefore local structures is small when compared to that of a ring structure. This property is also reflected in the betweenness distributions, which are also power-law: some edges have enormous betweenness values, and most edges have little.

Using the relationship between the the power law distribution and the average degree, it is possible to generate scale-free networks with the desired average degree, although they are not in abundance in real life.

For the number of components in Figure 6.17, unlike the Erdos Renyi networks, we see that the upper bound is not linear but closer to bilinear, or a concave curve to say the least. This difference is caused by the very fundamental difference between the Erdos Renyi networks and the networks with power law degree distributions. It should be understood that for a fixed number of node and edges, an ER network has more number of nodes that have their degree equal to the average degree of the network. On the other hand, SF networks find this balance on a more logarithmic scale, there are a few nodes with very big degrees that increase the average degree of the network, such that without them the average degree of the network would fall abruptly. To summarize statistically, the difference in the variances of the degree distributions of these two network types is huge. As it follows, there is a bigger number of nodes that have degrees smaller than the average. Therefore the failure of links of the nodes with the smallest degrees induces a very fast rate of fragmentation for the power law distributions.

As the average degrees increase, failure of the edges with the highest betweenness values again converge to this curve, along with the increase in the separation between the upper and lower bounds of the fragmentation curves. This is because as the average degree increases, the set of edges that are low in terms of the degree of the node they are incident to and the set of edges that have high betweenness values have more overlap. In other words, the number of edges that are incident to low degree nodes but have larger betweenness values is increased.

A clearer explanation of the disconnection proneness of scale-free networks under the failure of high betweenness valued edges is the power-law distributions of these values. However the difference between the random walk and shortest path betweenness distributions should be emphasized: as can be seen from Figure 4.19, the edge random walk distributions show smaller probabilities for low values when compared to shortest path distributions. This is because there are more edges with shortest path betweenness values smaller than the mean value than that of the random walk betweenness. This also causes the difference between the failure schemes in which the edges with lowest betweenness values fail. The lowest shortest path betweenness valued edges are more abundant than the edges with low random walk betweenness, therefore the fragmentation takes longer for low shortest path betweenness valued edge failures.

The number of disconnected pairs, in Figure 6.18, also exhibit a similar pattern for high betweenness link failures, growing very fast at first, but then the increase rapidly decays.

Figure 6.19 shows that the increase in the average clustering coefficient for the Erdos Renyi networks is not visible for scale free networks, although a non-decreasing trend can be seen for low betweenness values and low average degrees. This is mainly because the initial average clustering coefficient of a scale free network is already very high when compared to an Erdos Renyi network, therefore at the state where the ratio of pairwise disconnections saturate, the clustering coefficient of the network at this deformed state is not higher than the initial state, unlike the Erdos Renyi networks. However it should be noticed that even though there is no increase, the clustering coefficient of both these network types are very close at these percentages of edge failures.

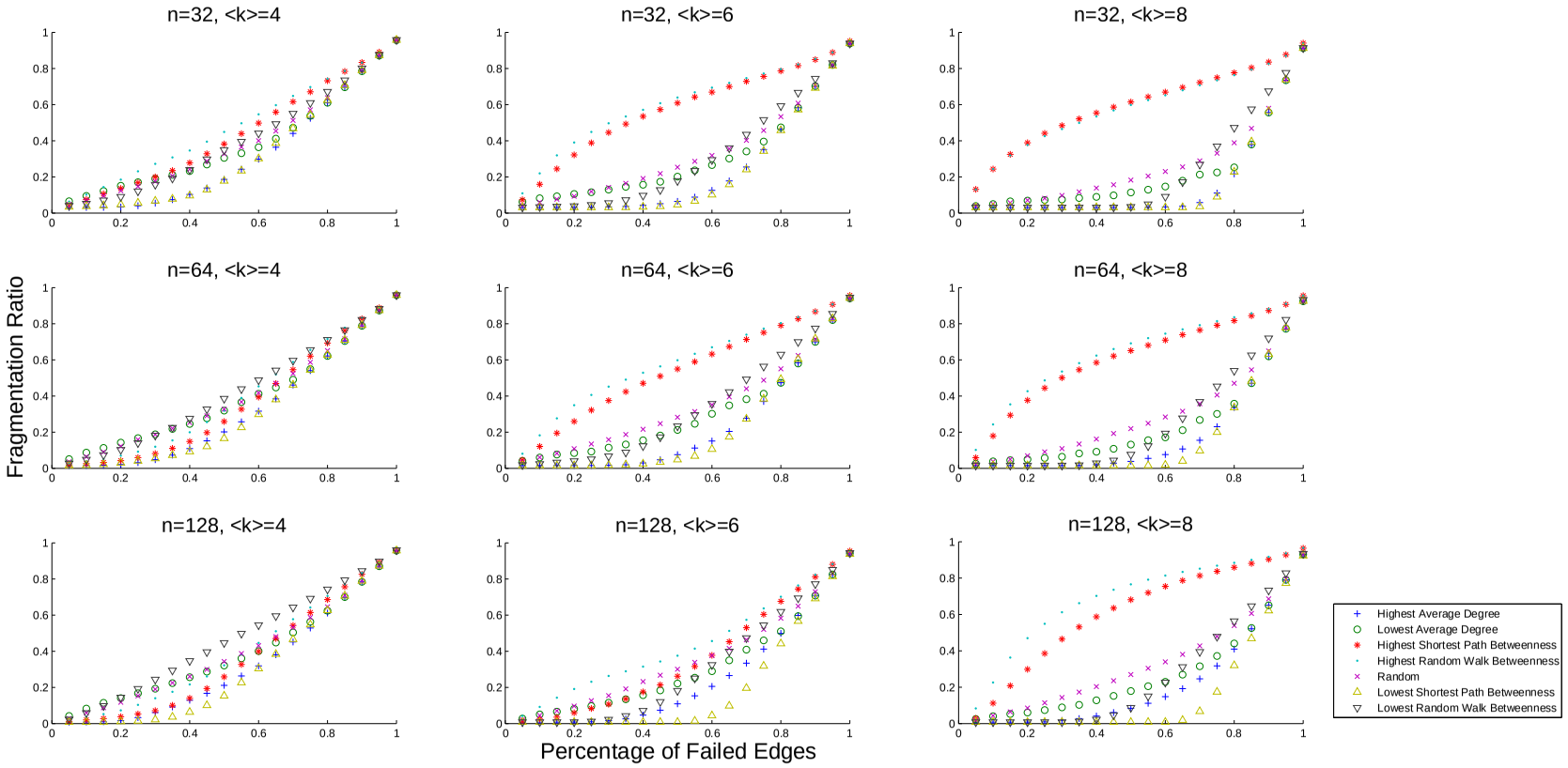

Figure 6.17. The graphs of fragmentation ratio versus the percentage of failed elements of continuous ranking methods for scale free networks of given order and average degree

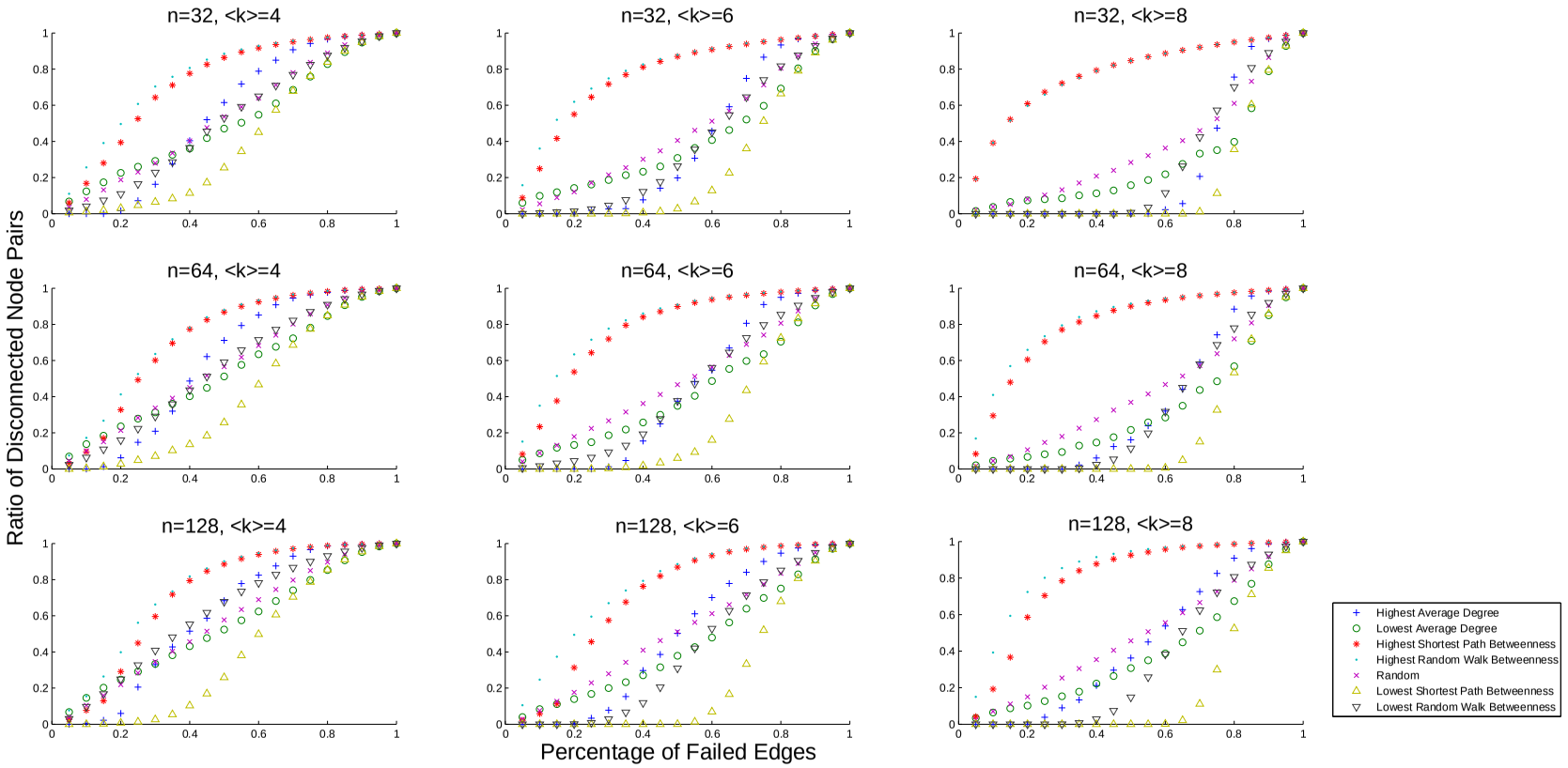

Figure 6.18. The graphs of the ratio of disconnected node pairs versus the percentage of failed elements of continuous ranking methods for scale free networks of given order and average degree

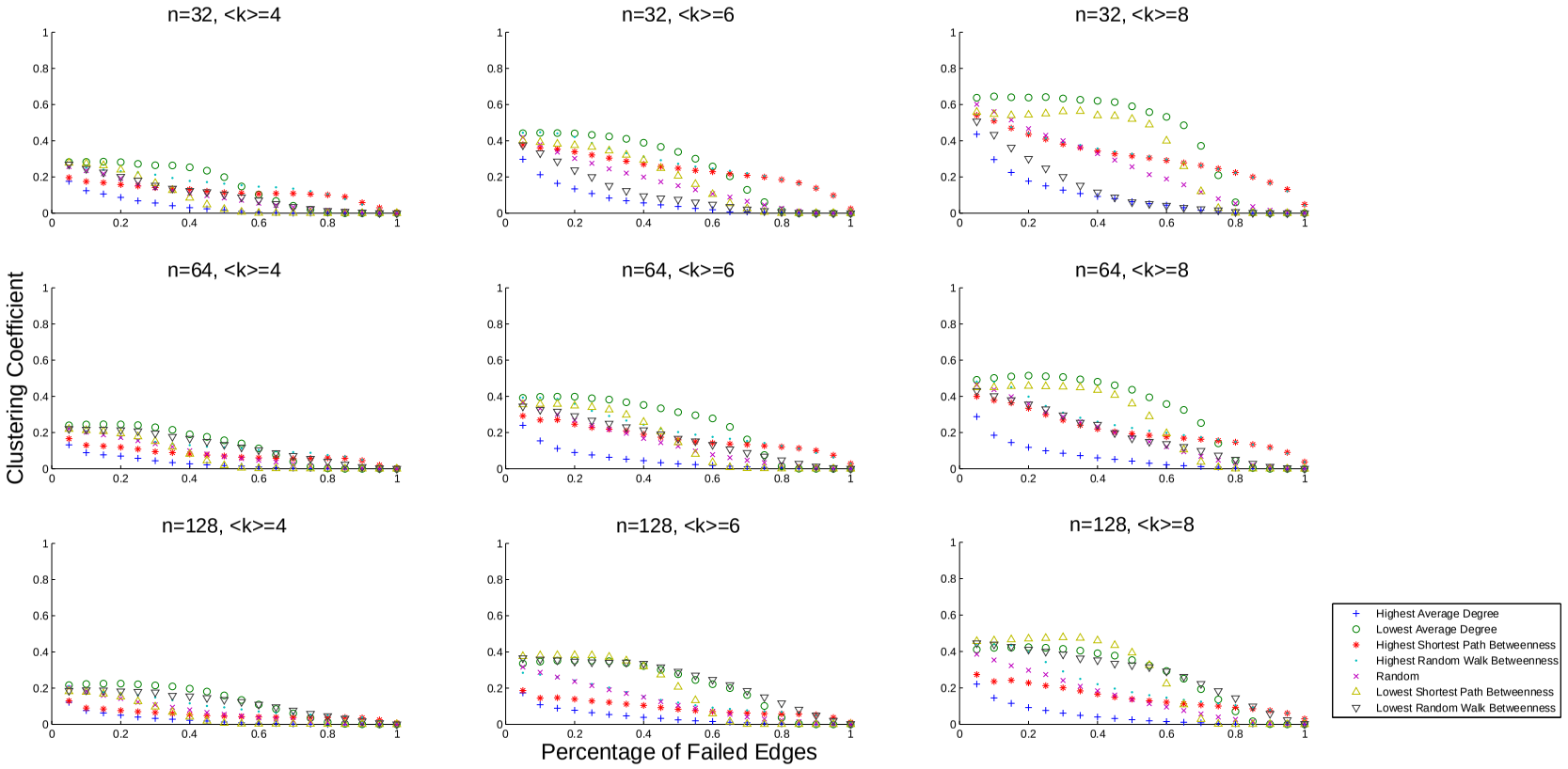

Figure 6.19. The graphs of clustering coefficient versus the percentage of failed elements of continuous ranking methods for scale free networks of given order and average degree

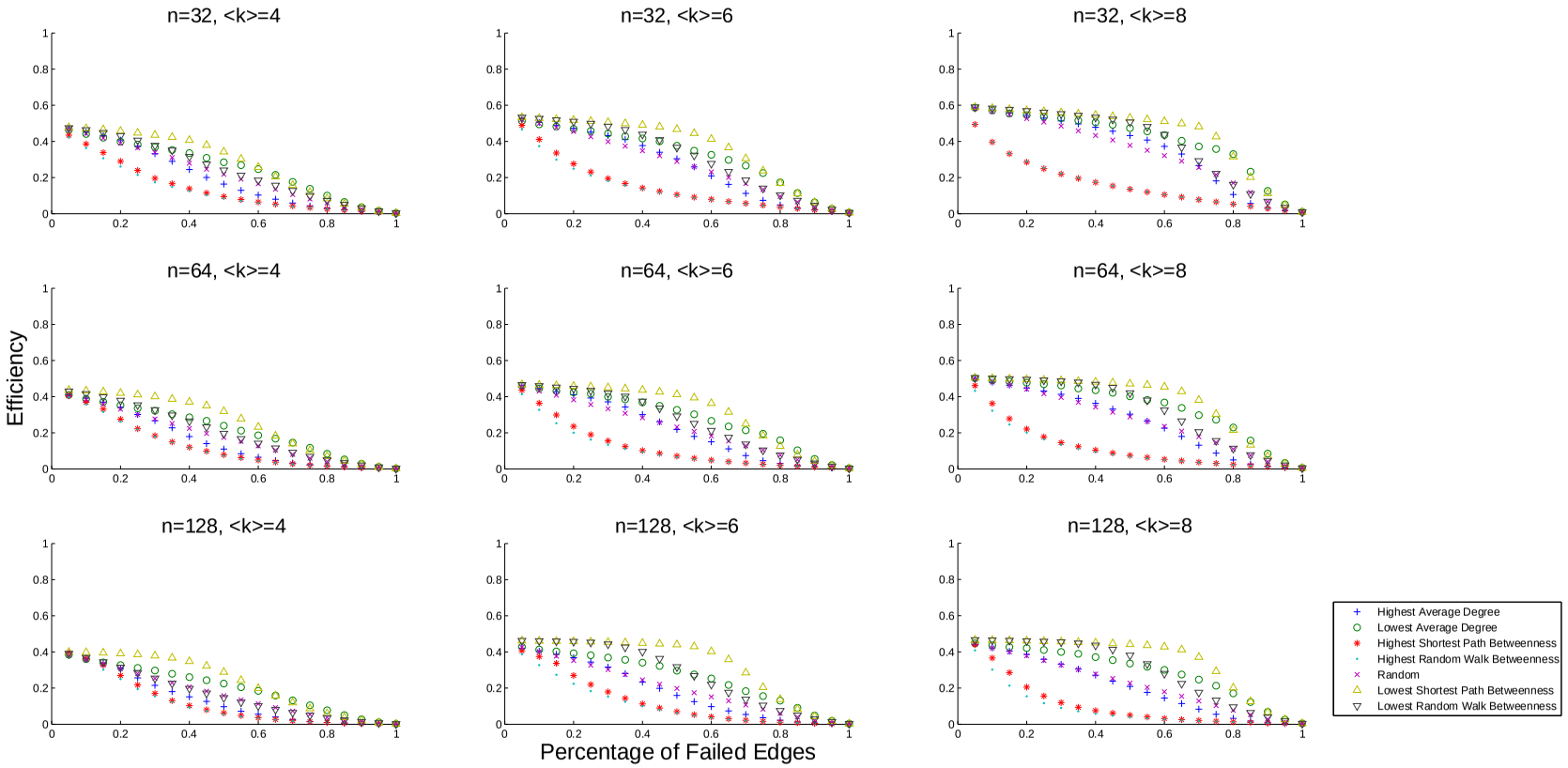

Figure 6.20. The graphs of efficiency versus the percentage of failed elements of continuous ranking methods for scale free networks of given order and average degree

6.3.2. Simple Ranking

For simple ranking methods, it can be immediately observed from Figure 6.21 that the concave curves are now more close to linear, hence it can be said that the fragmentation is not as efficient. One other point is that the difference between the failures of lowest random walk and shortest path betweenness edge failures for continuous ranking methods seem to disappear for simple ranking methods.

One other difference of the simple ranking method is that for different ranking methods, the decrease in the efficiency of the network is not identical like that of the Erdos Renyi network; on the contrary, the curves are very distinct. Therefore it can be said that in terms of efficiency, there is no difference between simple ranking at continuous ranking.

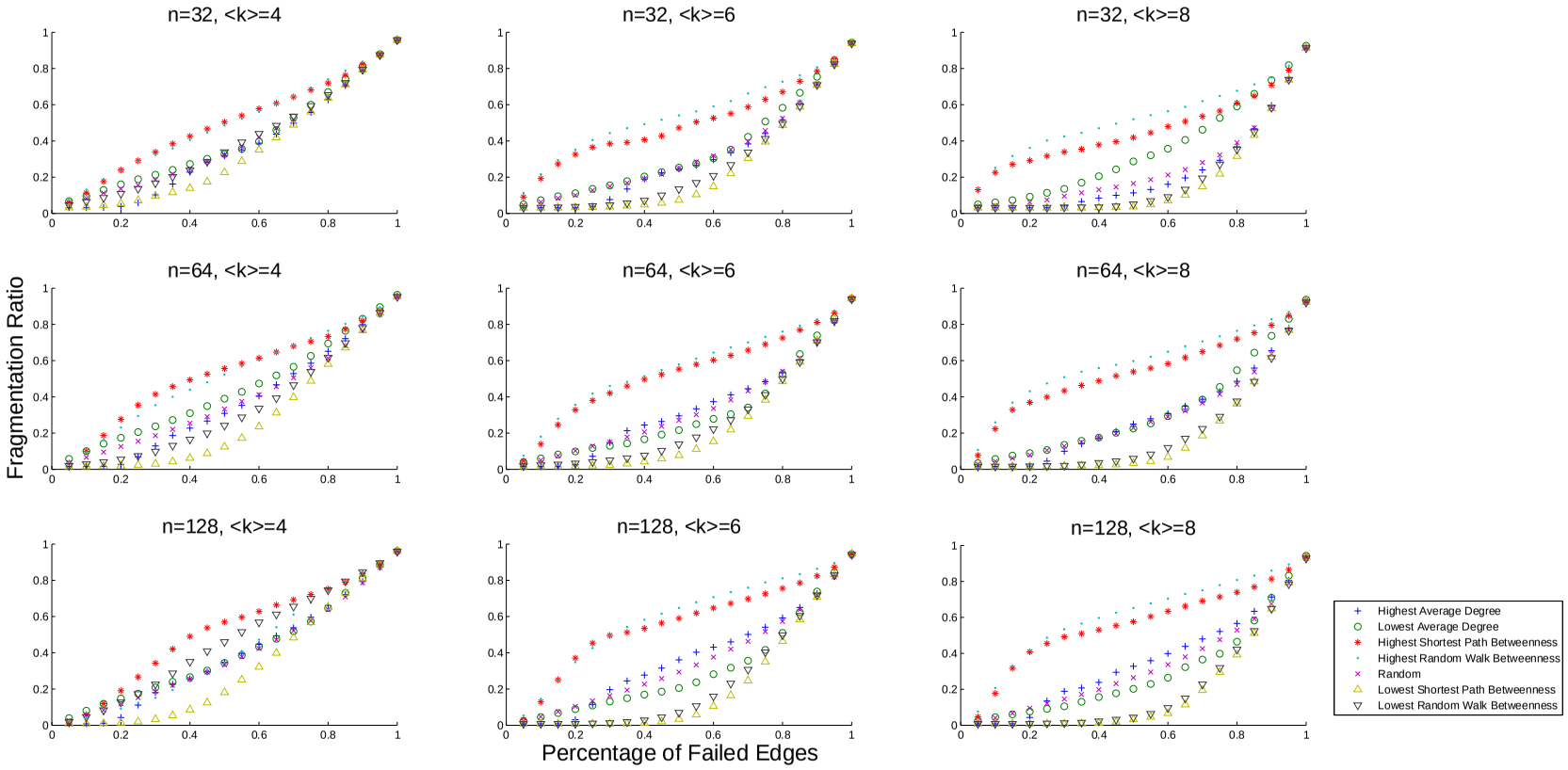

Figure 6.21. The graphs of fragmentation ratio versus the percentage of failed elements of simple ranking methods for scale free networks of given order and average degree

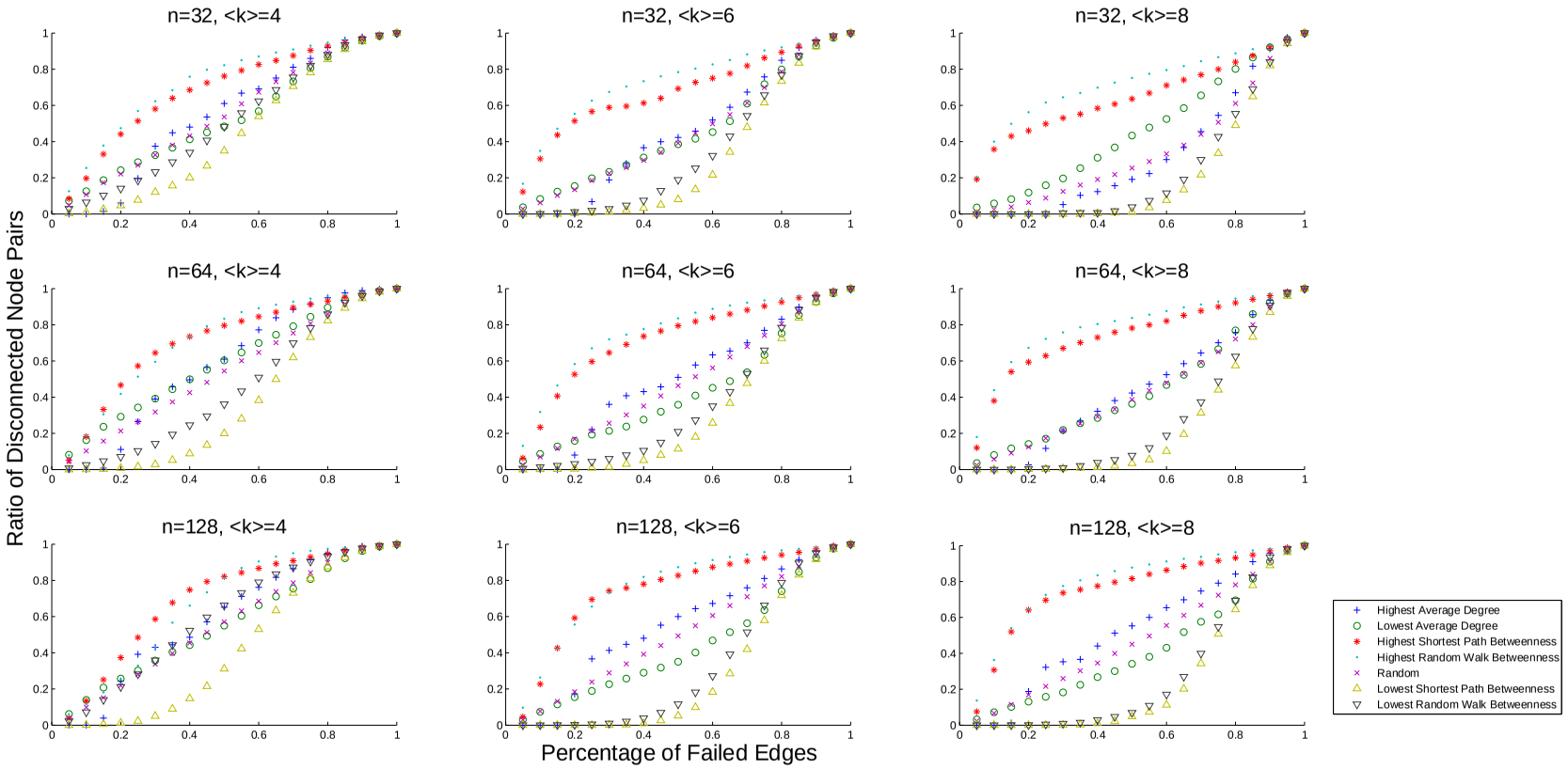

Figure 6.22. The graphs of the ratio of disconnected node pairs versus the percentage of failed elements of simple ranking methods for scale free networks of given order and average degree

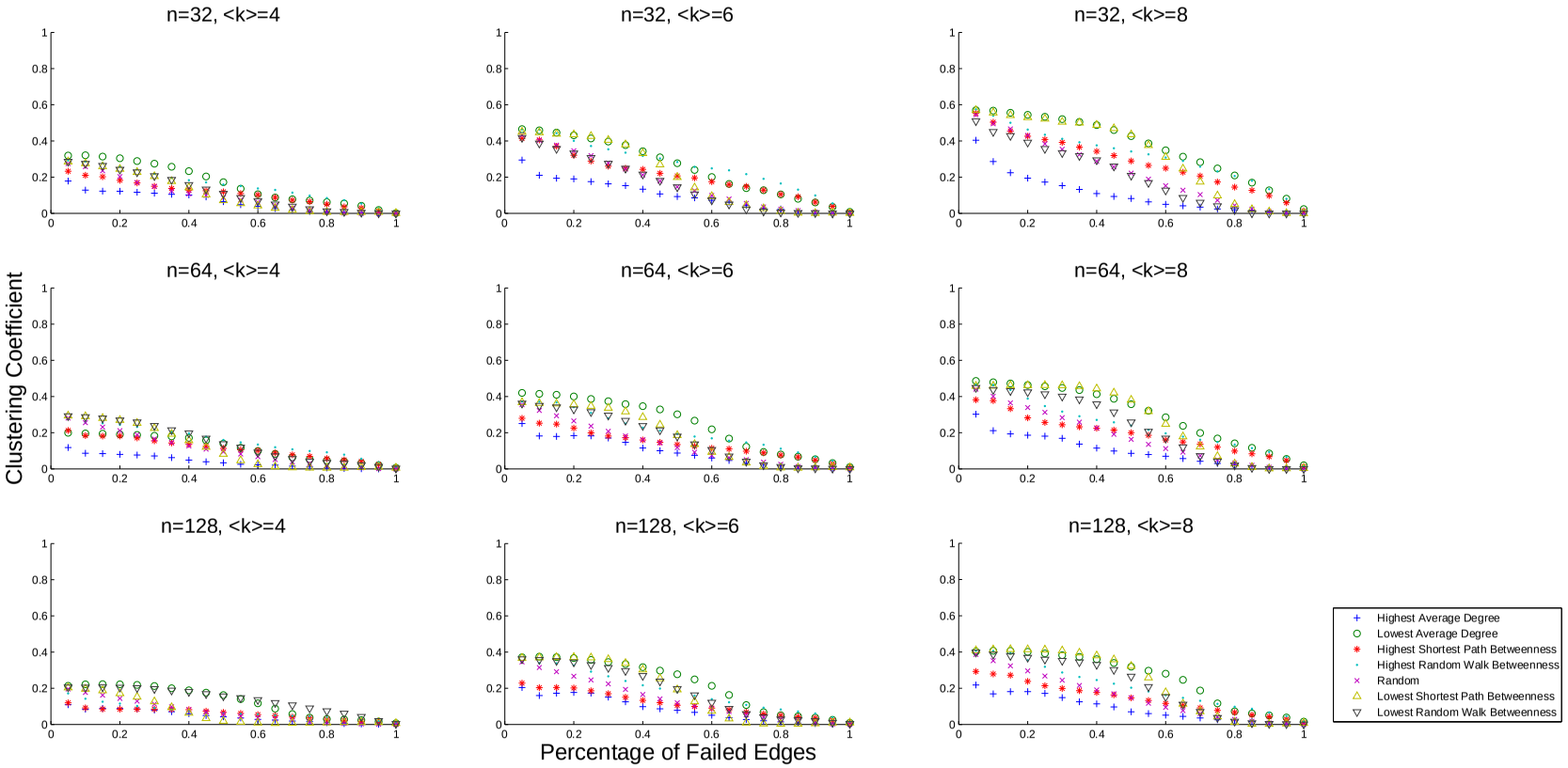

Figure 6.23. The graphs of clustering coefficient versus the percentage of failed elements of simple ranking methods for scale free networks of given order and average degree

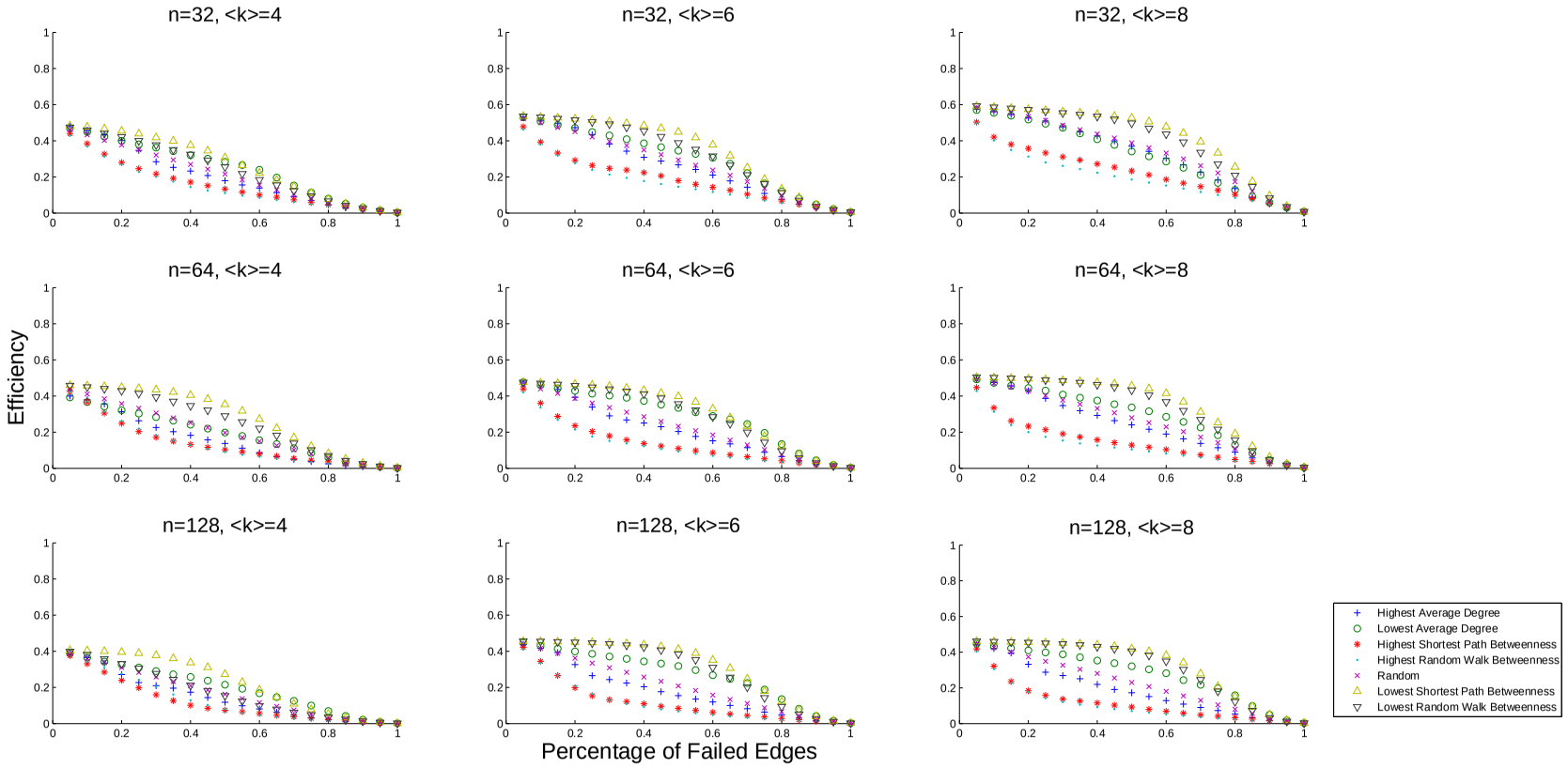

Figure 6.24. The graphs of efficiency versus the percentage of failed elements of simple ranking methods for scale free networks of given order and average degree

6.4. Small World Networks

6.4.1. Continuous Ranking

For continuously ranked failures in small networks, as seen in Figure 6.25, the lowest average degree edge failures are very critical, followed by high betweenness valued edge failures. Other curves are also very similar to that of the ring substrates, which is reasonable because small worlds are actually slightly altered ring structures. The difference from the curves of the ring structure is the position of the lowest random walk betweenness valued edge failure curve, which has now become relatively more critical. This is obviously caused by the introduction of the long range links. These links are formed at the expense of thinner regions of the ring, since they are formed by the rewiring of such short range edges, and they take control of the shortest paths, in other words, most shortest paths run through these links. Therefore the unfirom betweenness distribution is altered, it now has a bigger variance. This means there are links with lower betweenness values than in the original ring structure, and their failure makes the small world network more prone to disconnection since they lie at these zones where the ring has become thinner.

Figure 6.26 shows almost no difference to the corresponding figure of the ring structure. The clustering coefficient is slightly lower, however the curves are ranked and shpaed pretty much identically. Similarly for the efficiency, the initial efficiency value is higher for a small world network, but failure schemes cause similar reactions to the case of the ring structures.

In all the figures, the only difference is the relatively more critical position of the lowest shortest path betweenness valued edges failure curve. For example, for the clustering coefficient curves in Figure 6.27, this failure scheme reacts differently from the ring structure: the decrease is not as sharp. This is because the small world transformation causes the formation of bad neighbors with low shortest path betweenness values, since they are short range links lying on the outer rim of the ring. Therefore their removal counteracts the expected sudden drop in the clustering coefficient, therefore the curve is not as steep as it is for regular ring structures.

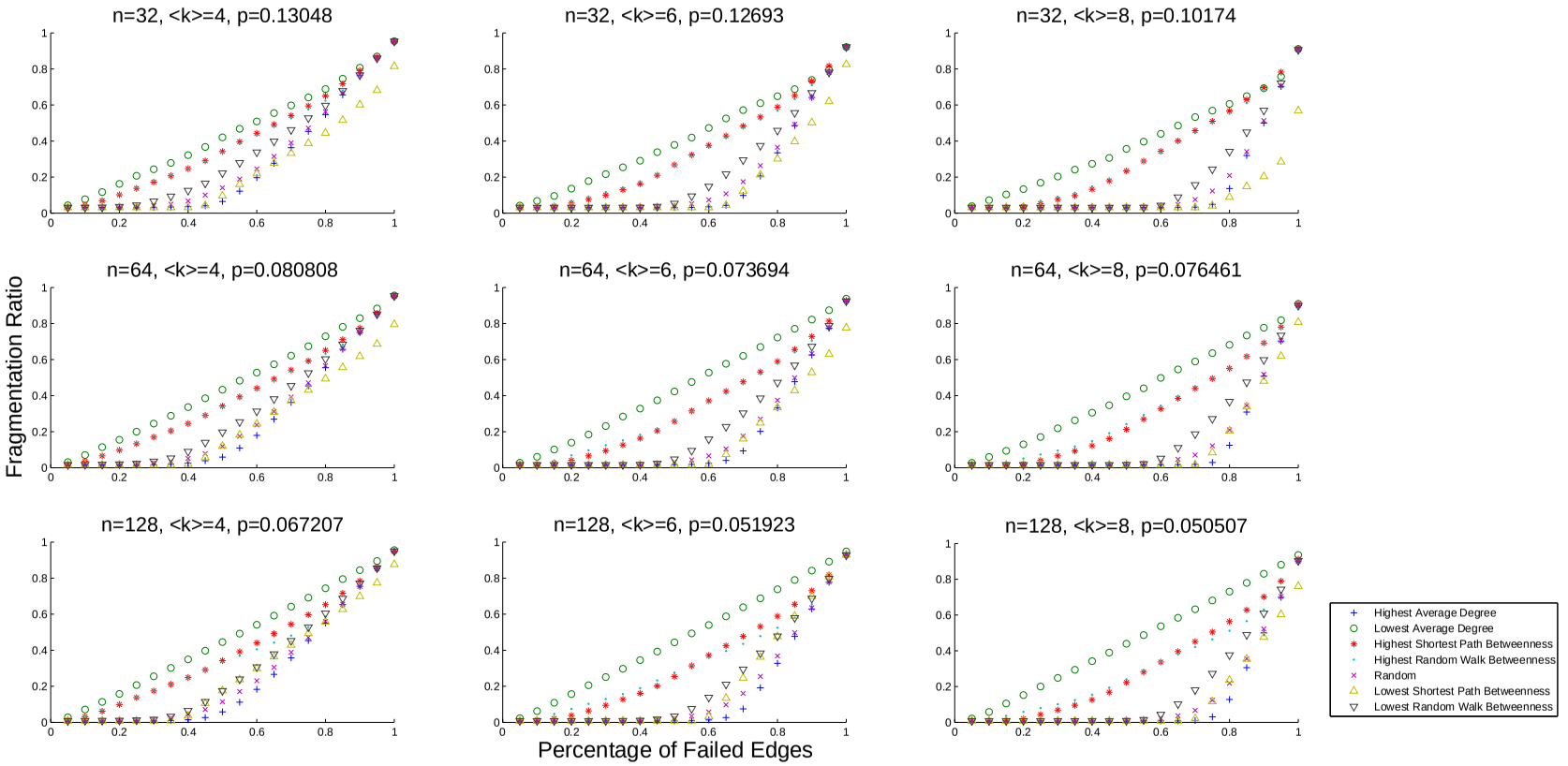

Figure 6.25. The graphs of fragmentation ratio versus the percentage of failed elements of continuous ranking methods for small world networks of given order and average degree

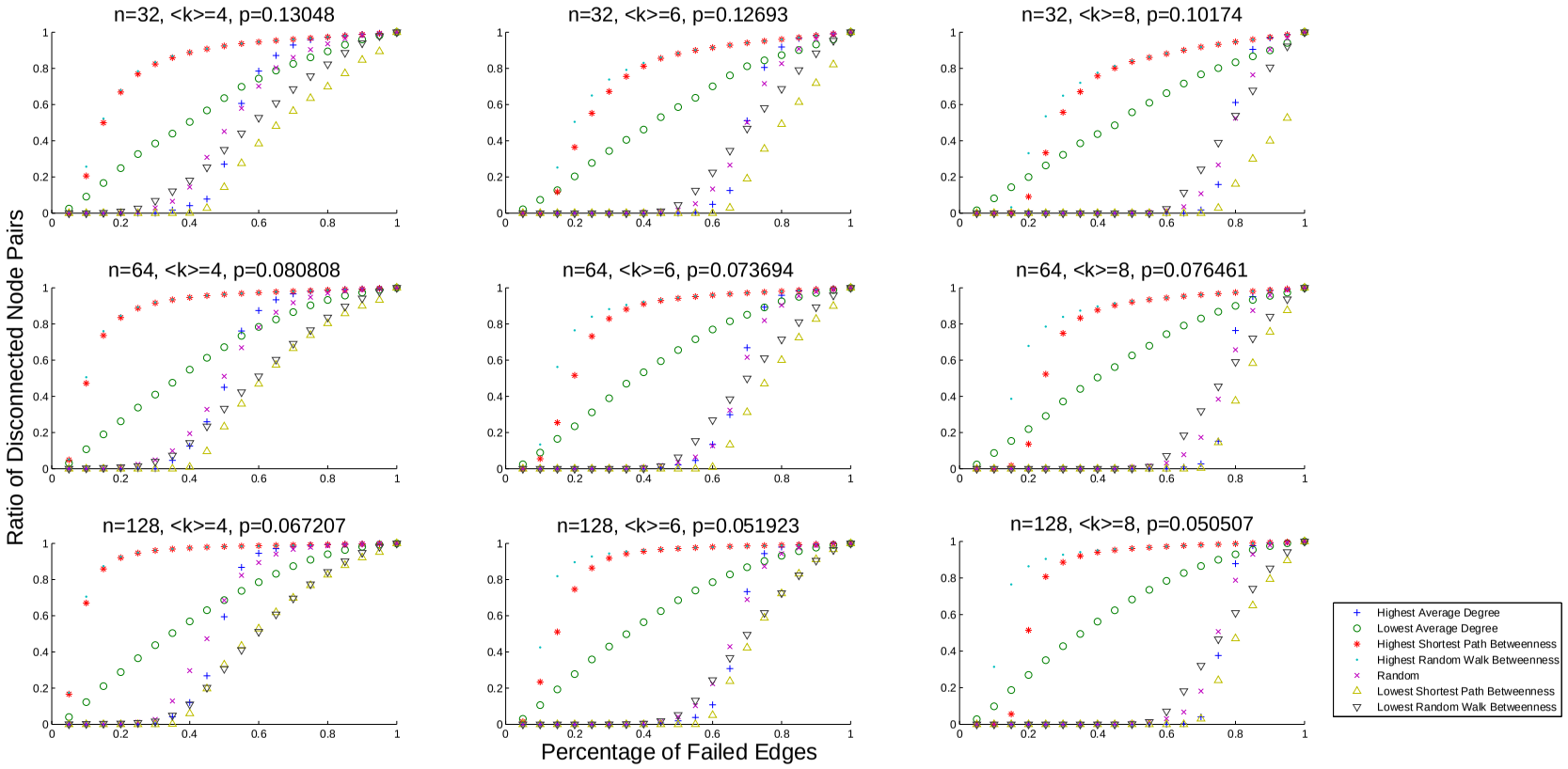

Figure 6.26. The graphs of the ratio of disconnected node pairs versus the percentage of failed elements of continuous ranking methods for small world networks of given order and average degree

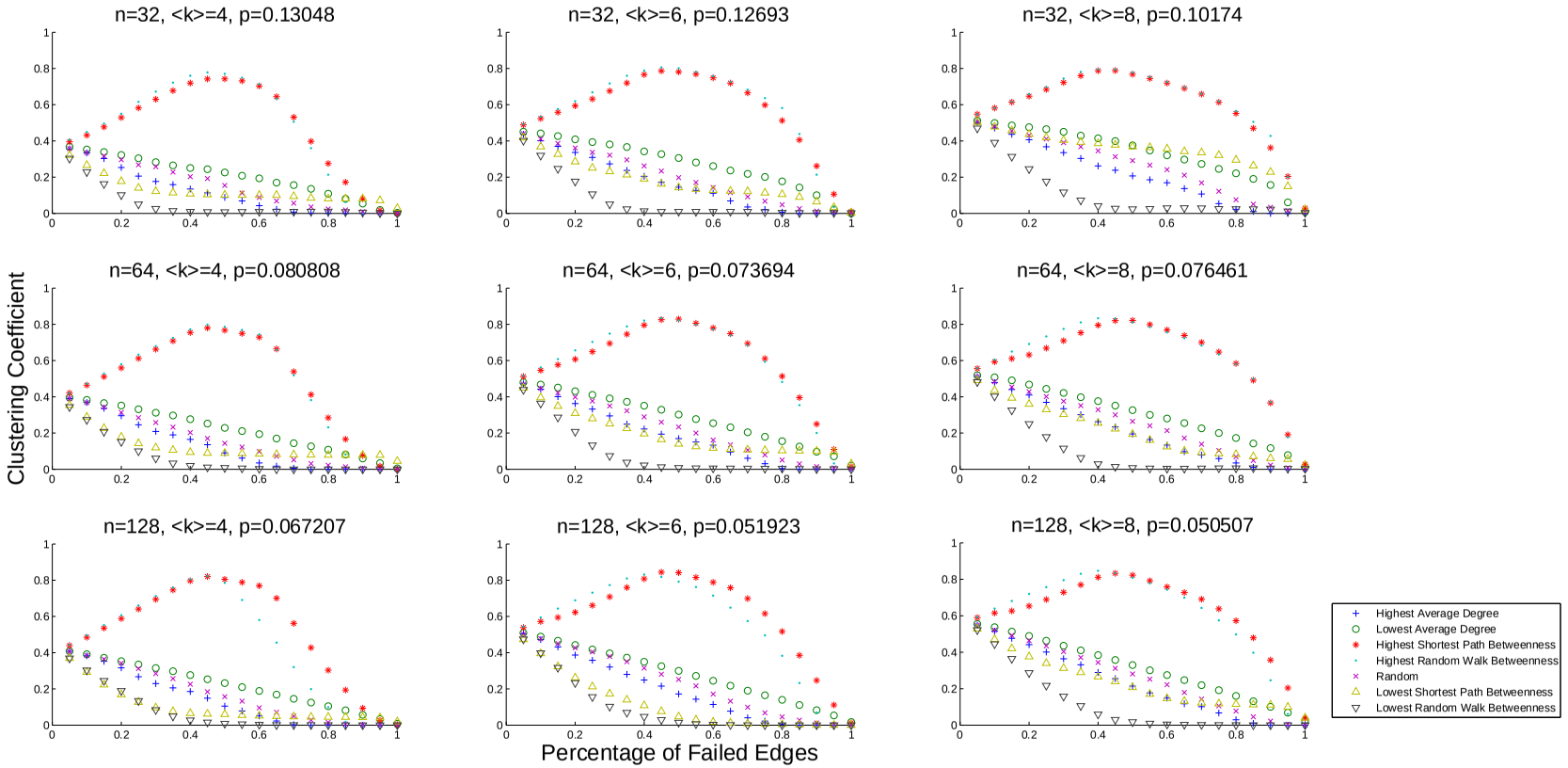

Figure 6.27. The graphs of clustering coefficient versus the percentage of failed elements of continuous ranking methods for small world networks of given order and average degree

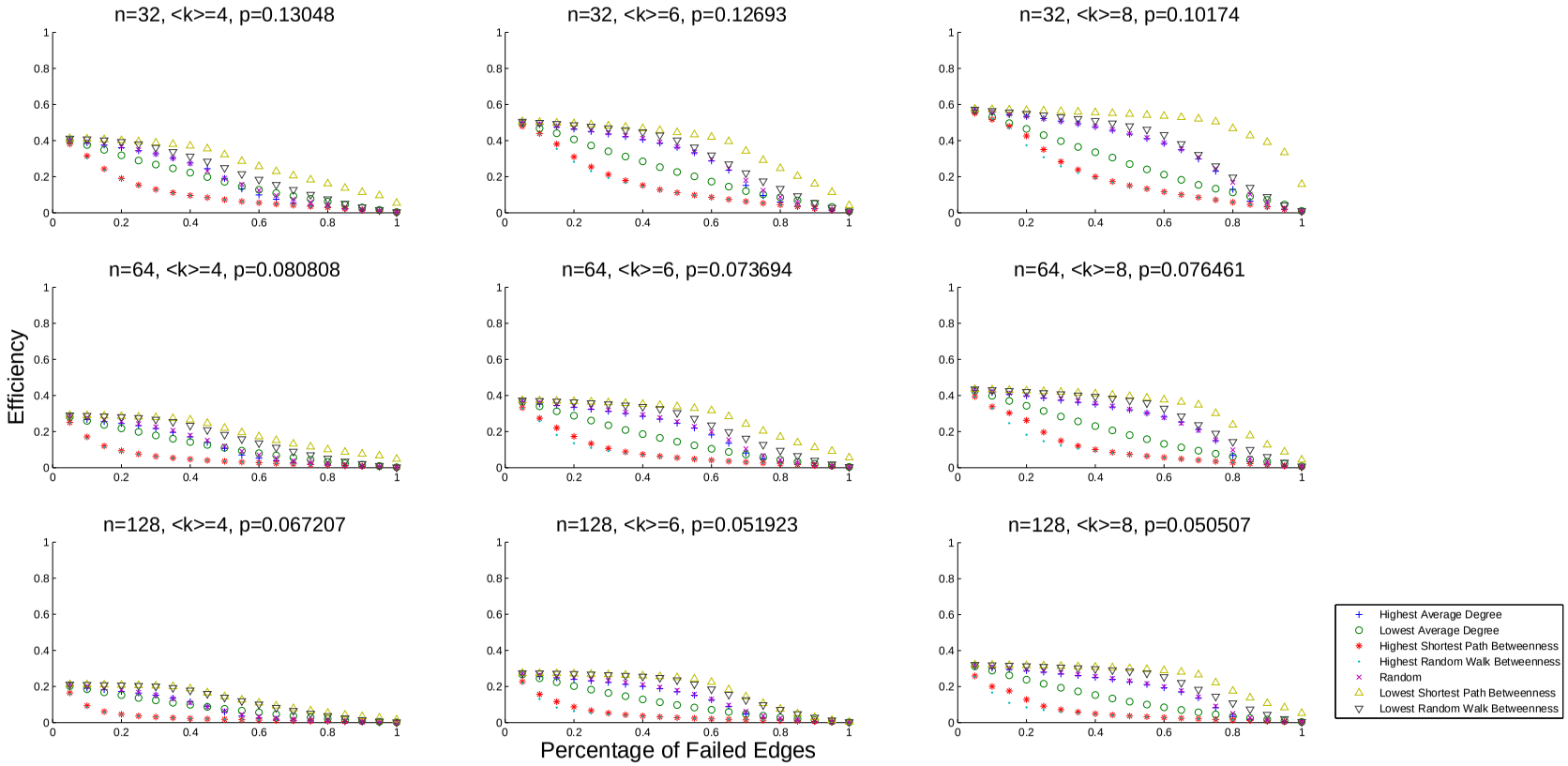

Figure 6.28. The graphs of efficiency versus the percentage of failed elements of continuous ranking methods for small world networks of given order and average degree

6.4.2. Simple Ranking

It can be seen from Figure 6.29 that the lowest shortest path betweenness valued edge failure scheme is very resistant against fragmentation. This difference is caused by the introduced long range links that have high shortest path betweenness values (but not as high random walk betweenness values) and keep the network intact. So it is reasonable to expect low fragmentation until these edges are broken, which occurs only until very late for this failure scheme.

Figure 6.30 is very helpful terms of showing where small world networks stand. All curves have the s-shape seen for the simple ranking of ring substrates, but unlike that case where most schemes are identical, they ranked exactly in the order of the Erdos-Renyi network. In other words, the diffrent failure schemes have managed to differentiate, but the response of the network still resembles that of the ring structure.

The rise of the average clustering coefficient is less obvious in the case of simple ranking.

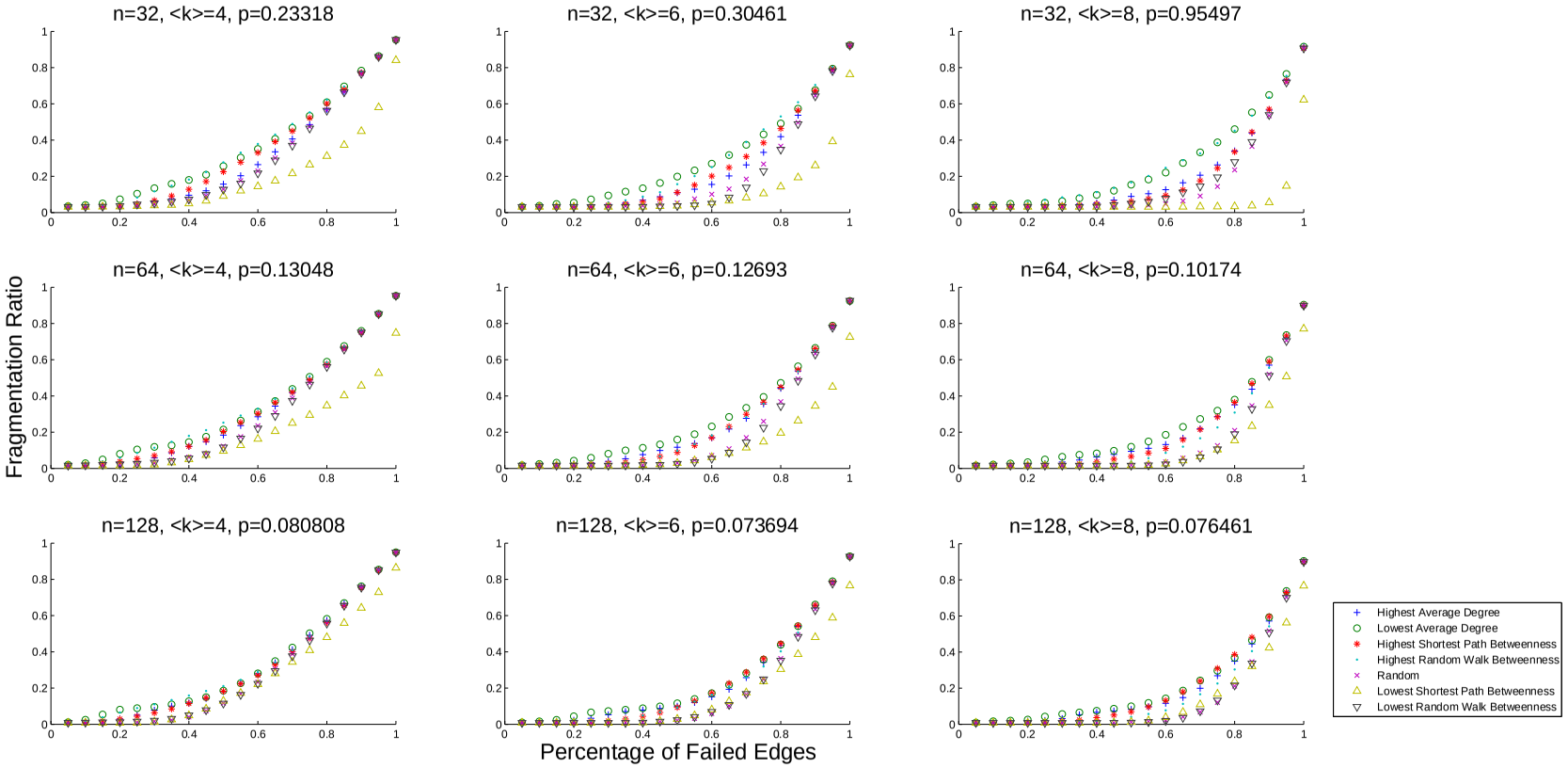

Figure 6.29. The graphs of fragmentation ratio versus the percentage of failed elements of simple ranking methods for small world networks of given order and average degree

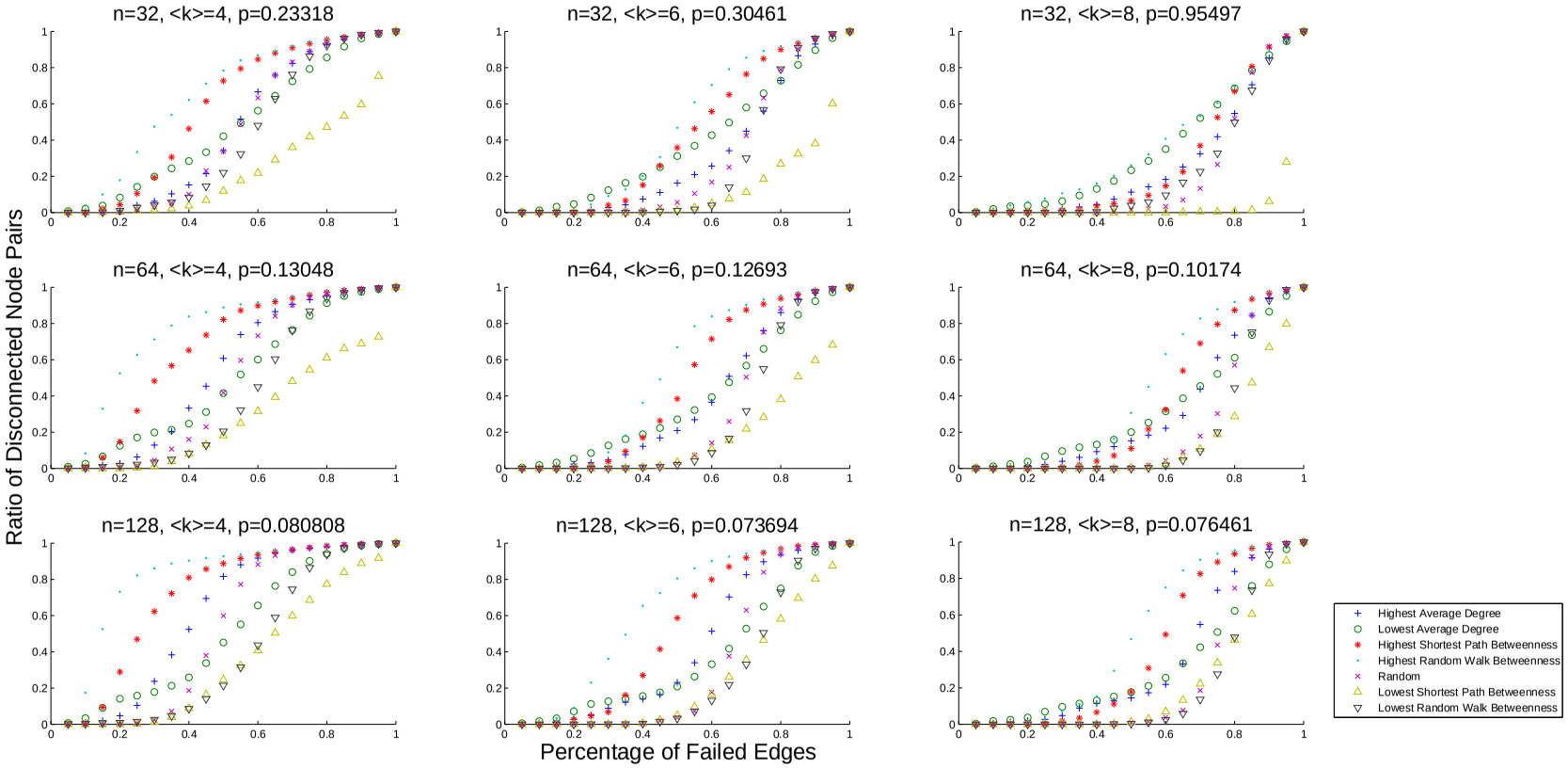

Figure 6.30. The graphs of the ratio of disconnected node pairs versus the percentage of failed elements of simple ranking methods for small world networks of given order and average degree

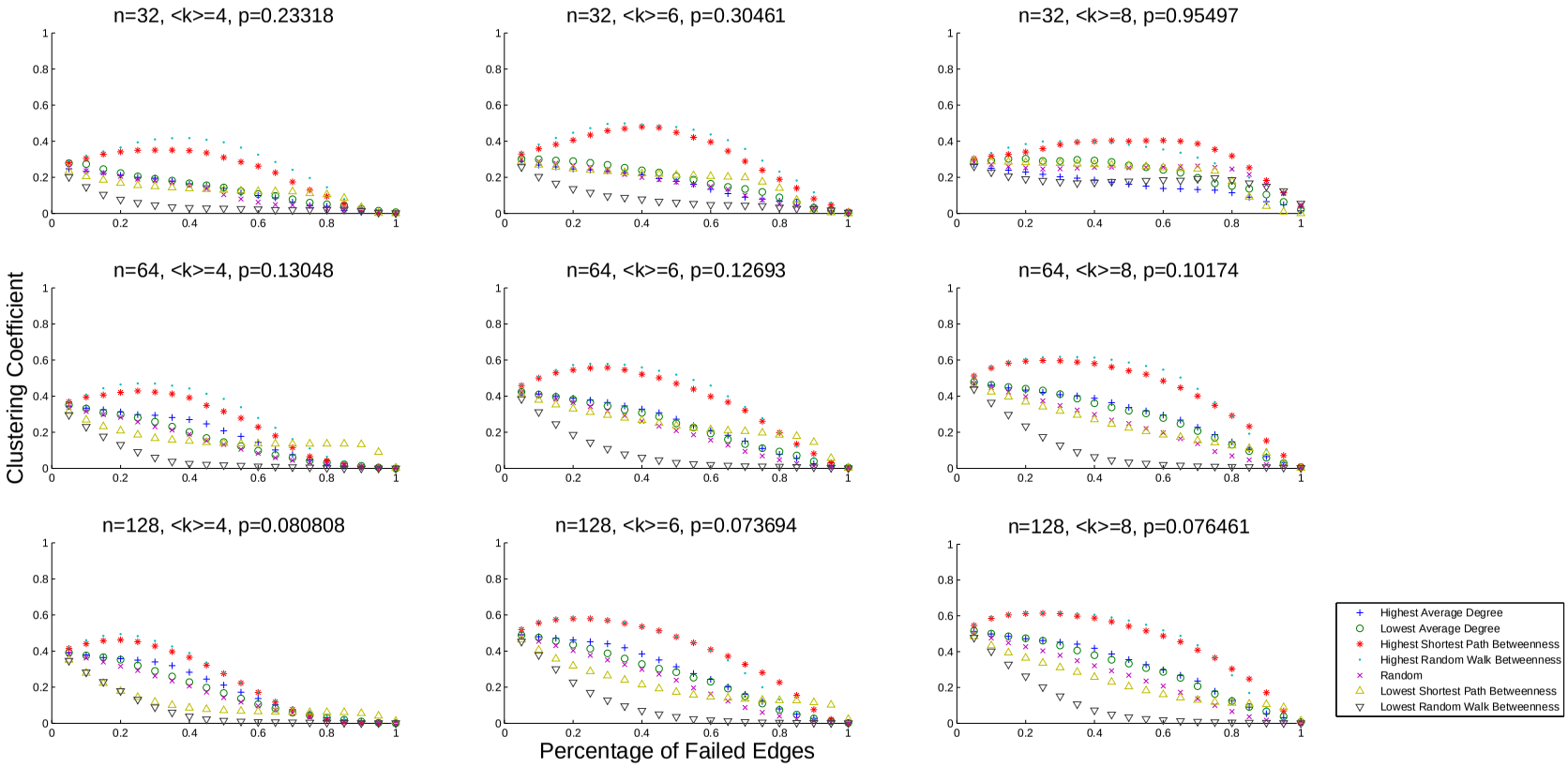

Figure 6.31. The graphs of clustering coefficient versus the percentage of failed elements of simple ranking methods for small networks of given order and average degree

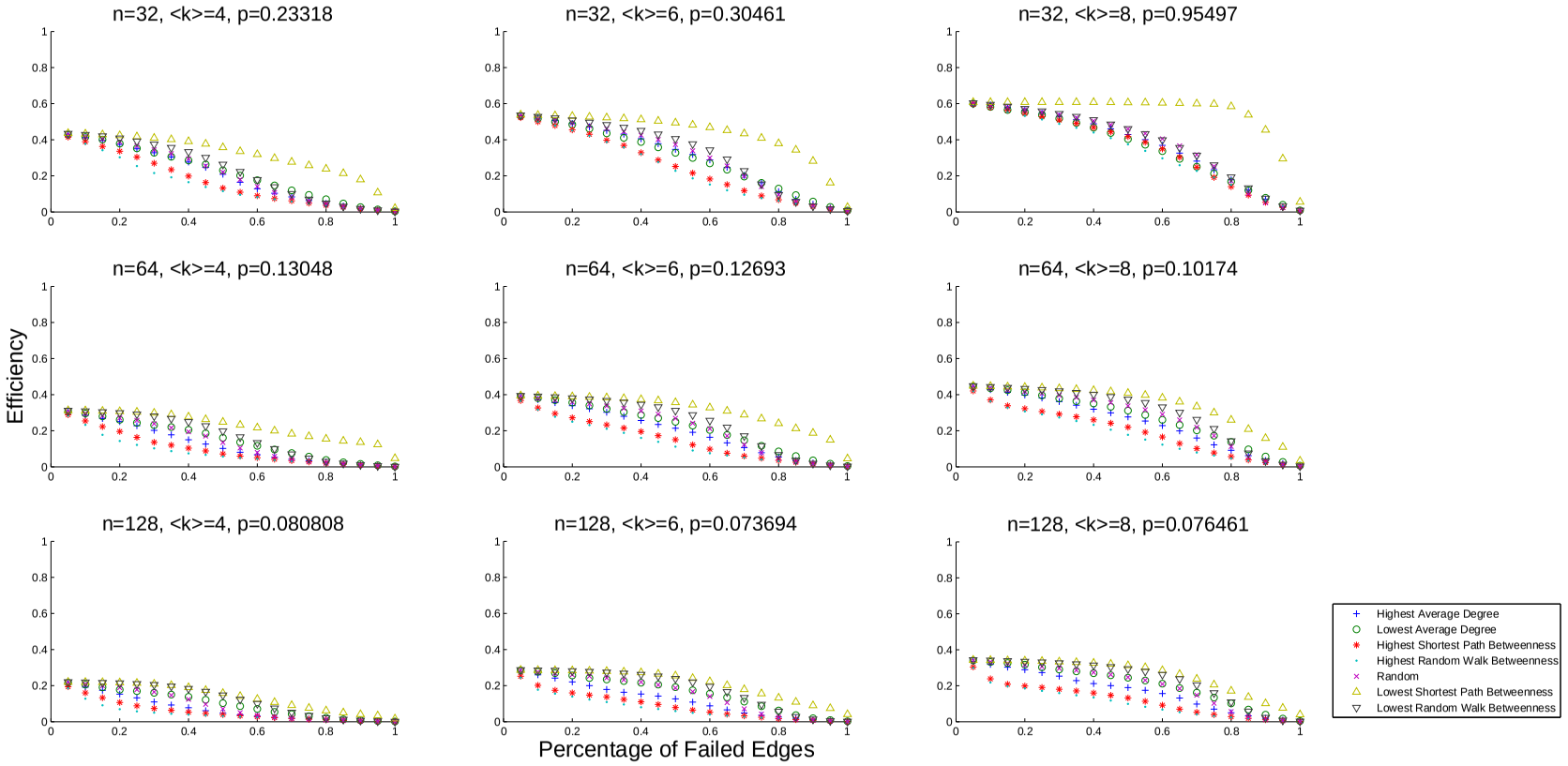

Figure 6.32. The graphs of efficiency versus the percentage of failed elements of simple ranking methods for small world networks of given order and average degree

7. VULNERABILITY ANALYSIS OF TRANSPORT NETWORKS

Vulnerability and robustness of infrastructure networks against failures have been investigated in [49, 50, 50, 51, 52, 53, 54, 56, 57], with subjects ranging from metabolic neural networks to power grids and gas networks. Transportation networks are also an intriguing subject for vulnerability analysis [58, 59]. This chapter carries out simulations for several Turkish transportation networks, Istanbul highway network [60], Istanbul rapid transit network [61] and Turkish railway network [62]. The statistical properties of these networks are given in Table 7.1.

It can be seen from these numbers that the three networks are very similar. They have tree-like structures, very low clustering coefficients and high average shortest path values. Average degrees are only slightly above 2, and the average nearest neighbor degree is smaller than 3. In these conditions, since the efficiency and clustering coefficients are low, it is more useful to consider the fragmentation ratios and the ratio of disconnected node pairs, as in the following figures.

The behavior is very similar for each of these three networks, which is only normal since they have almost identical structures. The low variance of the degree distribution causes uniformity, which maakes it difficult for any failure scheme to make a difference for continuous ranking, as well as simple ranking. The differences between the failure schemes is only highlighted in the ratio of disconnected node pairs, which reflects the results of the ring structures and the Erdos Renyi networks. The difference is however, there is no region where the disconnections are 0, the first failure immediately causes disconnection. Therefore there is no s-shape, but the ranking of the failure schemes in terms of how critical they are remains unchanged.

Figure 7.1. Three real transportation networks: Istanbul highway network, Istanbul rapid transit network and Turkish railway network.

Table 7.1. Basic network parameters for three real transportation networks.

Trasnport Networks	Istanbul Highway Network	Istanbul Rapid Transit Map	Turkish Railway Network
Order	52	192	97
Average Degree	2,42	2,19	2,08
Average Nearest Neighbor Degree	2,73	2,50	2,57
Average Shortest Path Length	6,91	15,93	9,85
Clustering Coefficient	0,0192	0,0035	0,0000

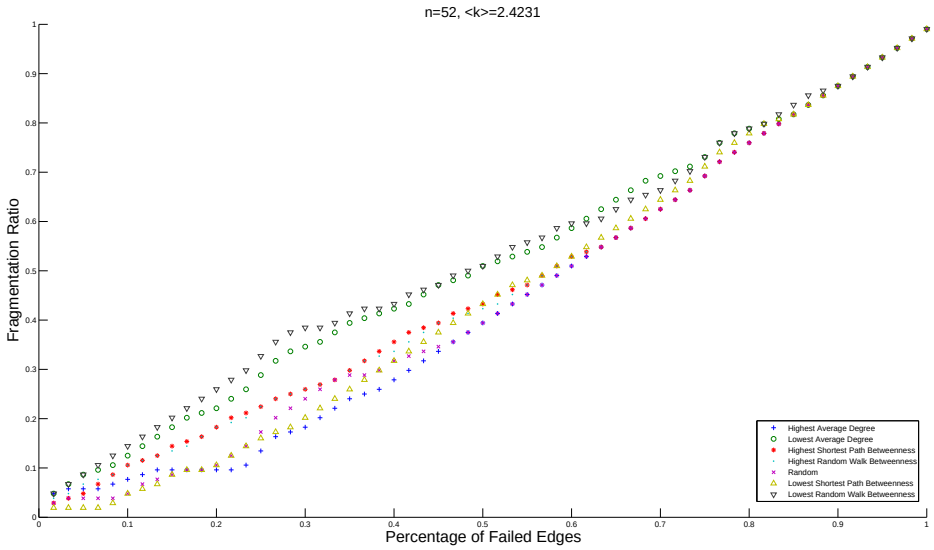

Figure 7.2. The fragmentation ratio versus the percentage of failed elements of continuous ranking methods for the Istanbul highway network

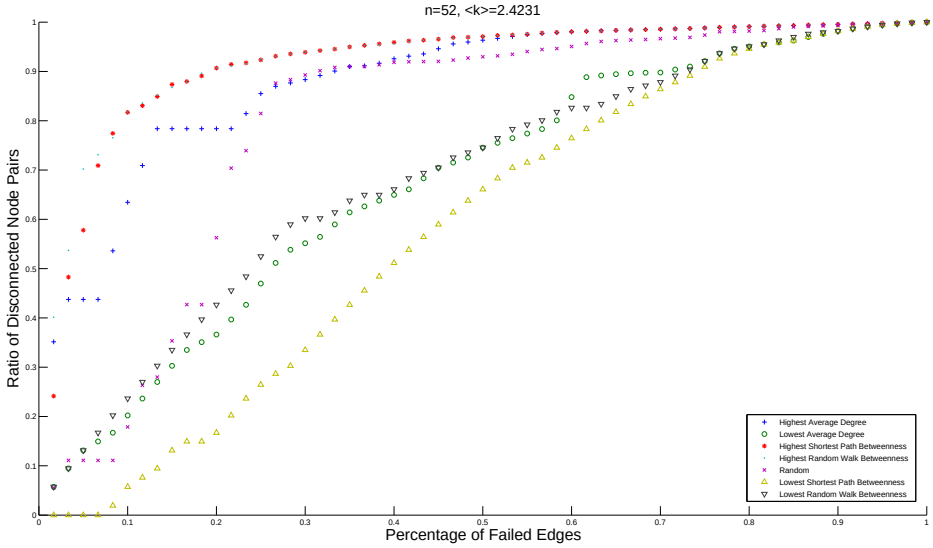

Figure 7.3. The ratio of pairwise disconnections versus the percentage of failed elements of continuous ranking methods for the Istanbul highway network

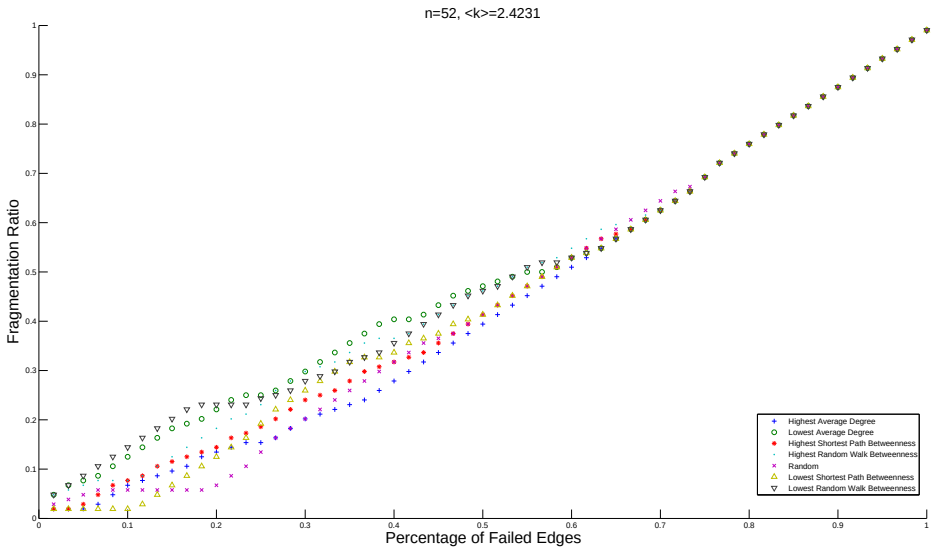

Figure 7.4. The fragmentation ratio versus the percentage of failed elements of simple ranking methods for the Istanbul highway network

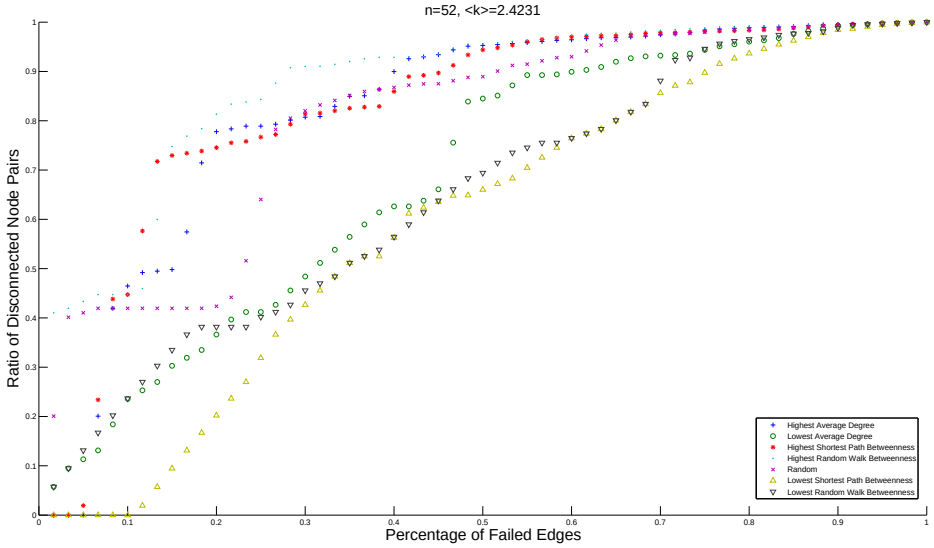

Figure 7.5. The ratio of pairwise disconnections versus the percentage of failed elements of simple ranking methods for the Istanbul highway network

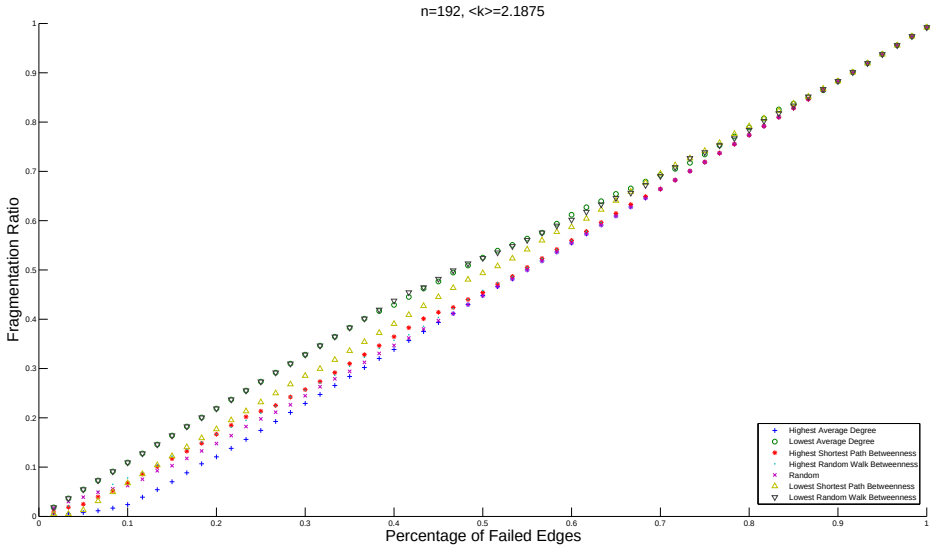

Figure 7.6. The fragmentation ratio versus the percentage of failed elements of continuous ranking methods for the Istanbul rapid transit network

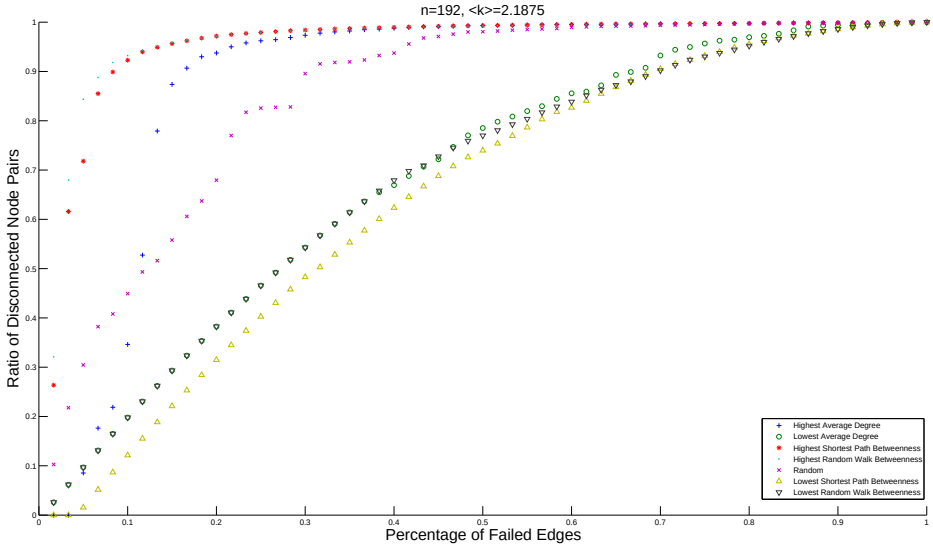

Figure 7.7. The ratio of pairwise disconnections versus the percentage of failed elements of continuous ranking methods for the Istanbul rapid transit network

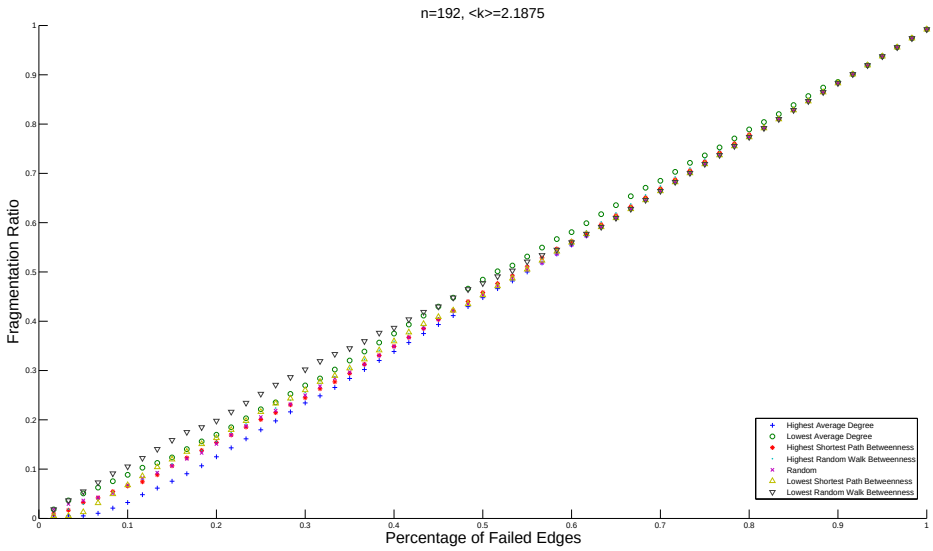

Figure 7.8. The fragmentation ratio versus the percentage of failed elements of simple ranking methods for the Istanbul rapid transit network

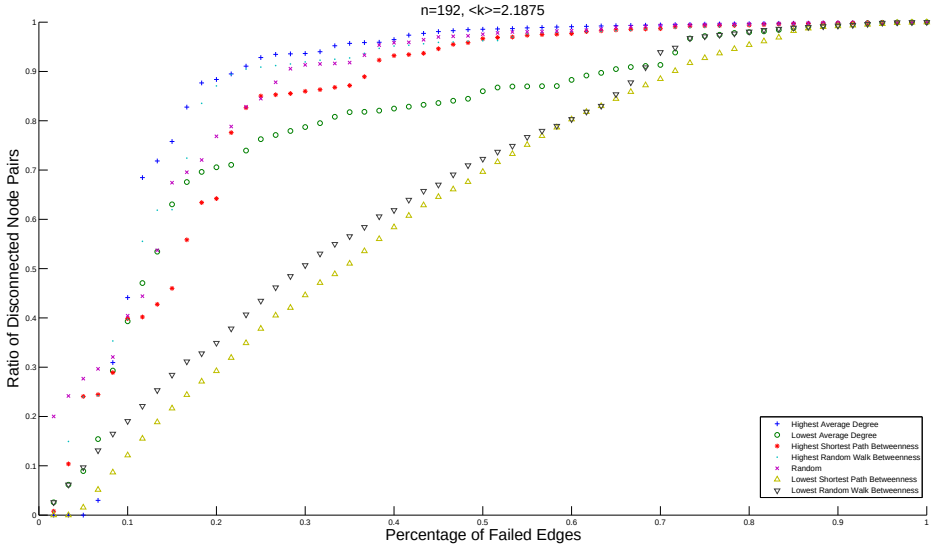

Figure 7.9. The ratio of pairwise disconnections versus the percentage of failed elements of simple ranking methods for the Istanbul rapid transit network

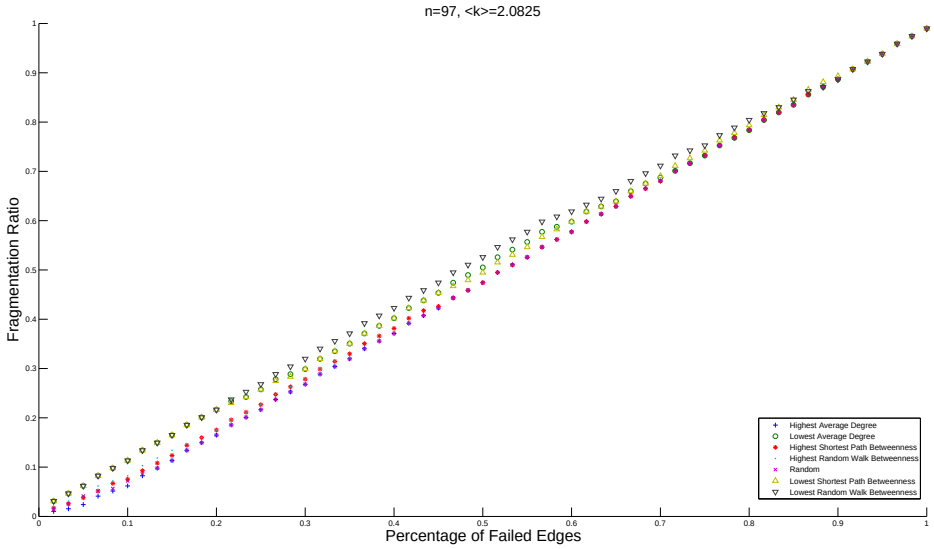

Figure 7.10. The fragmentation ratio versus the percentage of failed elements of continuous ranking methods for the Turkish railway network

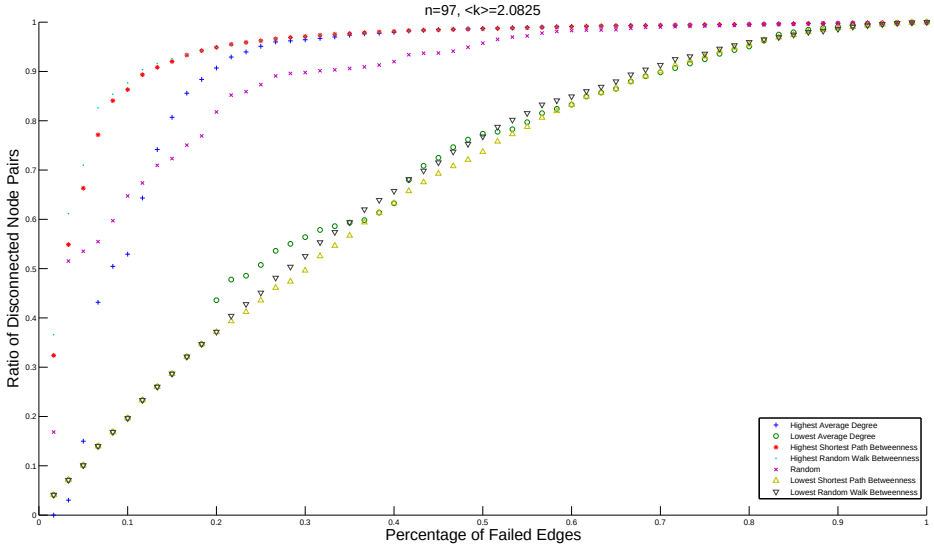

Figure 7.11. The ratio of pairwise disconnections versus the percentage of failed elements of continuous ranking methods for the Turkish railway network

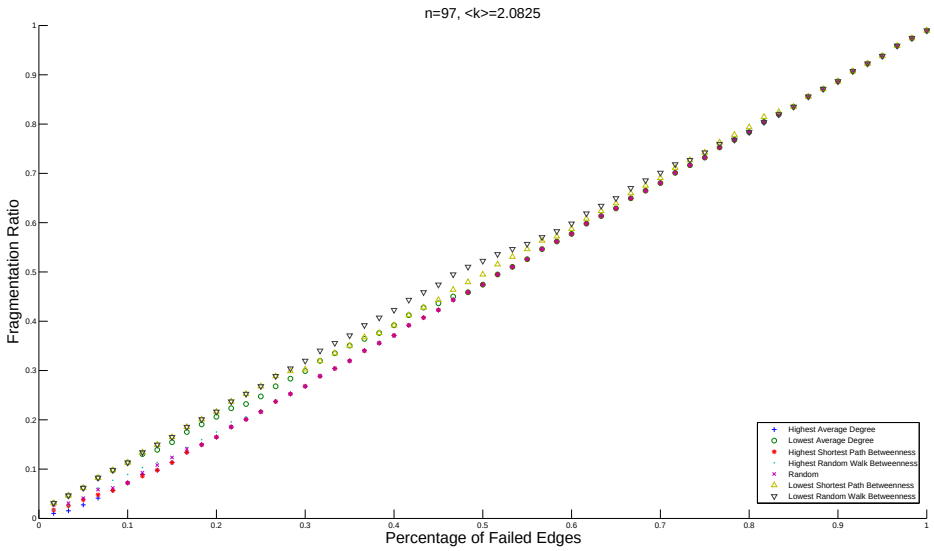

Figure 7.12. The fragmentation ratio versus the percentage of failed elements of simple ranking methods for the Turkish railway network

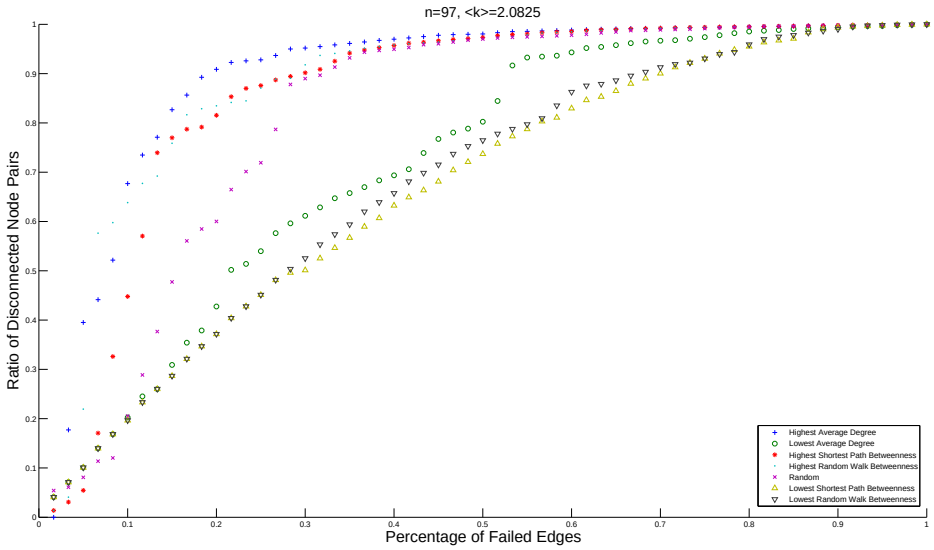

Figure 7.13. The ratio of pairwise disconnections versus the percentage of failed elements of simple ranking methods for the Turkish railway network

8. CONCLUSIONS AND FUTURE WORK

In every developed city, infrastructures formed huge webs that became very difficult to manage. Traffic problems, power shortages occur as a result of simple failures on these networks. Therefore these infrastructure networks are in need of detailed analysis of performance and response against a range of failure scenarios. Using the basics of graphy theory, complex networks can be thoroughly analyzed. Shortest paths, minimum cuts, degree distributions and other measures can be used to understand the response of these networks under failures. In addition the investigation of connectivity correlations also helps understanding the topology of these networks.

In order to define failure scenarios, proper ranking of the network elements is essential. Degree of a node is beneficial, but not satisfactory by itself. In order to measure the importance of any node or edge to a network, betweenness centrality parameters are used. Shortest path betweenness is a good fit in the sense that it perfectly models a simplified flow algorithm along the network to identify the usage of specific elements. The critical point here is the optimality of the flow, such that it minimizes energy using the information. On the other hand, random walk betweenness also ranks elements in the same manner, but the optimality constraint is lifted. The flow is no longer capable of using the global map information, as in the case of shortest path betweenness, and moves in a totally random manner. These two extremes are good representations of the function of a network.

Erdos Renyi networks represent total disorder. Ring substrates are exactly the opposite, they obey total order. Between these two extreme lies small world and scale free networks. Small world networks have high local clustering and low average shortest paths, therefore is an optimized version of these two extreme network formations. Scale free networks are very interesting in the sense that they have huge variances in their degree distributions, also in their betweenness distributions. The ordered structure coexists with the disorder, but more importantly, there is a strict hierarchy between elemets: few are rich, and many are poor.

In order to address the vulnerability, reliability, or robustness of networks against fail-

ures, the function, structure and the topology of the network must be thoroughly analyzed. For the next step, use of graph theoretical reliability formalism is helpful, yet inefficient and unrepresentative since it requires a correct probability estimation for failures. Therefore a more simple and to the point method would be to carry out simulations of different failure schemes.

An important point about the network responses against ordered failures is the relationship between the betweenness values and the clustering coefficient. Regions with strong local clustering are generally connected with high betweenness valued elements that lie in less clustered regions. The extent of this nonuniformity defines the network response. Failure of the high betweenness valued links is therefore very critical in most cases.

Another failure scenario, most likely to be overlooked, is the failure of links connecting low degree nodes. Counterintuitively, low degree nodes play a crucial rol in the functioning of networks. One reason is that they are very easily disconnected from the network, so for applications in which connectivity is of utmost importance, this is an important problem. Another reason is that although appearing insignificant, there is a possibility that these nodes still lie on very critical paths along the network, ones that strongly damage the network in the case of failure. Therefore when compared with the degree, betweenness values are more representative of an element's importance to the network.

Istanbul transportation networks such as the Istanbul Highway network and the rapid transit network have low average degrees, big average shortest path lengths and almost zero clustering, most likely due to the geodesic constraints. These networks are almost tree like, there are no regions with strong clustering and no long range links that connect these regions, therefore they do not exhibit optimality in terms of both reliability and performance. Similar to the network types given above, these transport networks are very prone to disconnection and a serious fall of performance under the failure of high betweenness valued edges.

I am hoping to expand on this subject. One point I would like to analyze in depth is how the local clustering information and the global shortest path information are related. The connection of the strongly localized regions also fall into the category of community

detection in networks.

One other point I would like to elaborate on is the development of the betweenness measures by various definitions of the selected paths. As mentioned, these measures can be thought of as the result of an agent modeling. In this sense, random walks can be diversified in a variety of ways, which I believe can yield very surprising results. In this sense, one interesting problem would be to define a random walk that can mimic a shortest path, without using the global knowledge, to a certain extent.

Finally, I would like to elaborate on the failure modes of different networks; that is, how different types of networks change, and what they turn into under series of various failure schemes. I believe this sort of analysis can be helpful to see what properties networks actually have in common.

REFERENCES

1. Diestel, R., *Graph Theory*, Springer, New York, 2000.

2. Harary, F., *Graph Theory*, Perseus Books, Massachusetts, 1994.

3. West, D. B., *Introduction to Graph Theory*, Prentice Hall, NJ, 2000.

4. Cvetkovic, D. M., M. Doob and H. Sachs. *Spectra of Graphs: Theory and Applications*, Academic Press, New York, 1979.

5. Bollobas, B., *Random Graphs*, Cambridge University Press, New York, 2001.

6. Caldarelli, G. and A. Vespignani, *Large Scale Structure and Dynamics of Complex Networks: From Information Technology to Finance and Natural Science*, World Scientific, NJ, 2007.

7. Newman, M. E. J., "Assortative Mixing in Networks", *Physical Review Letters*, Vol.89, No.20, pp.208701+, October 2002.

8. Newman, M. E. J., "Mixing patterns in networks", *Physical Review E* Vol. 67, No.2, pp.026126+, February 2003.

9. Na, M. B. and R. Pastor-Satorras, "Epidemic spreading in correlated complex networks", *Physical Review E*, Vol.66, No.4, pp.047104+, October 2002.

10. Pastor-Satorras, R., A. Vazquez and A. Vespignani, "Dynamical and correlation properties of the Internet", *Physical Review Letters*, Vol.87, No.(25), January 2001.

11. Watts, D. J. and S. H. Strogatz, "Collective dynamics of small world networks", *Nature*, Vol.393, No.6684, pp.440-442, June 1998.

12. Barrat, A. and M. Weigt, "On the properties of small world network models", *The Euro-*

pean Physical Journal B - Condensed Matter and Complex Systems, Vol.13, No.3, pp.547-560, January 2000.

13. Newman, M. E. J., S. H. Strogatz and D. J. Watts, "Random graphs with arbitrary degree distributions and their applications", *Phys Rev E Stat Nonlin Soft Matter Phys*, Vol.64, No.2, August 2001.

14. Stephenson, K. and M. Zelen, "Rethinking centrality: Methods and examples", *Social Networks*, Vol.11, No.1, pp.1-37, March 1989.

15. Dekker, A. H., "Centrality in Social Networks: Theoretical and Simulation Approaches", *Proceedings of SimTecT 2008*, Melbourne, Australia, 12-15 May 2008, pp 33-38, May 2008.

16. Borgatti, S. P., "Centrality and network flow", *Social Networks*, Vol.27, No.1, pp.55-71, January 2005.

17. Borgatti, S. P. and M. G. Everett, "A Graph-theoretic perspective on centrality", *Social Networks*, Vol.28, No.4, pp.466-484, October 2006.

18. Brandes, U., "A faster algorithm for betweenness centrality", *Journal of Mathematical Sociology*, Vol.25, pp.163-177, 2001.

19. Doyle, P. G. and L. J. Snell, "Random Walks and Electric Networks", January 2000.

20. Noh, J. D. and H. Rieger, "Random Walks on Complex Networks", *Physical Review Letters*, Vol.92, No.11, pp.118701+, March 2004.

21. Friedberg, S. H. and A. J. Insel, "Convergence of matrix powers", *International Journal of Mathematical Education in Science and Technology*, Vol.23, No.5, pp.765-769, September, 1992.

22. Newman, M. E. J., "A measure of betweenness centrality based on random walks", *Social Networks*, Vol.27, No.1, pp.39-54, January 2005.

23. Cormen, T. H., C. E. Leiserson, R. L. Rivest and C. Stein, *Introduction to Algorithms*, The MIT Press, Massachusetts, 2001.

24. Watts, D. J., *Small Worlds: The Dynamics of Networks between Order and Randomness (Princeton Studies in Complexity)*, Princeton University Press, NJ, 2003.

25. Dorogovtsev, S. N. and J. F. F. Mendes, "Evolutions of Networks", *Advances in Physics*, Vol.51, No.4, pp.1079-1187, 2002.

26. Albert, R. and A. L. Barabasi, "Statistical mechanics of complex networks", *Reviews of Modern Physics*, Vol.74, No.1, pp.47-97, January 2002.

27. Kleinberg, J. M., "The Small-World Phenomenon: An Algorithmic Perspective". *In Proceedings of the 32nd ACM Symposium on Theory of Computing*, Cornell University, Ithaca, NY, USA, pp.163-170, 2000.

28. Newman, M. E. J., "Models of the Small World: A Review", *Journal of Statistical Physics*, Vol.101, No.3, pp.819-841, November 2000.

29. Kleinberg, J. M., "Navigation in a small world", *Nature*, Vol.406, No.6798, August 2000.

30. Goldstein, M. L., S. A. Morris and G. G. Yen, "Problems with Fitting to the Power-Law Distribution", *The European Physical Journal B - Condensed Matter and Complex Systems*, Vol.41, No.2, pp.255-258, September 2004.

31. Barabasi, A. L. and R. Albert, "Emergence of scaling in random networks", *Science*, Vol. 286, No. 5439., pp. 509-512, October 1999.

32. Molloy, M. and B. Reed, "A critical point for random graphs with a given degree sequence", *Random Structures and Algorithms* Vol.6, pp.161-180, 1995.

33. Britton, T., M. Deijfen and A. Martin-Lof, "Generating Simple Random Graphs with Prescribed Degree Distribution", *Journal of Statistical Physics*, Vol.124, No.6, pp.1377-

1397, September 2006.

34. Milo, R., N. Kashtan, S. Itzkovitz, M. E. J. Newman and U. Alon, "On the uniform generation of random graphs with prescribed degree sequences", *ArXiv Condensed Matter e-prints*, December 2003.

35. Viger, F. and M. Latapy, "Efficient and Simple Generation of Random Simple Connected Graphs with Prescribed Degree Sequence", *Computing and Combinatorics In Computing and Combinatorics*, Vol.3595, pp.440-449, 2005.

36. Aiello, W., F. Chung and L. Lu, "A random graph model for massive graphs", *STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, Portland, Oregon, United States, pp. 171-180, 2000.

37. Gkantsidis, C., M. Mihail and E. Zegura, "The markov chain simulation method for generating connected power law random graphs", *In Proceedings of 5th Workshop on Algorithm Engineering and Experiments*, 2003.

38. Buldyrev, S. V., R. Parshani, G. Paul, H. E. Stanley and S. Havlin, "Catastrophic cascade of failures in interdependent networks", *Nature*, Vol.464, No.7291, pp. 1025-1028, April 2010.

39. Newman, M. E. J. and D. J. Watts, "Scaling and percolation in the small-world network model", *Physical Review E*, Vol.60, No.6, pp.7332-7342, December 1999.

40. D. R. Karger, "A randomized fully polynomial time approximation scheme for the all terminal network reliability problem". *Proceedings of the 27th annual ACM symposium on Theory of computing*, New York, NY, USA, pp. 11-17, 1995.

41. Harms, D. D., M. Kraetzl, C. J. Coulburn and J. S. Devitt, *Network reliability: experiments with a symbolic algebra environment*, CRC Press, Florida, 1995.

42. Ball, M. O., C. J. Coulburn and J. S. Provan, "Network reliability", *Systems Research Center*, University of Maryland, TR 92-74, June 1992.

43. Erdos, P. and T. Gallai, “Graphs with Prescribed Degrees of Vertices” [Hungarian]. *Mat. Lapok*, Vol.11, pp.264-274, 1960.

44. Dueñas-Osorio, L., J. I. Craig and B. J. Goodno, “Seismic response of critical interdependent networks”, *Earthquake Engineering and Structural Dynamics*, Vol.36, No.2, pp.285-306, 2007.

45. Albert, R., H. Jeong and A. L. Barabasi, “Error and attack tolerance of complex networks”, *Nature*, Vol.406, No.6794, pp.378-382, July 2000.

46. Holme, P., B. J. Kim, C. N. Yoon and S. K. Han, “Attack vulnerability of complex networks”, *Physical Review E*, Vol.65, No.5, pp.056109+, May 2002.

47. Zhao, J. and K. Xu, “Enhancing the robustness of scale-free networks”, *Journal of Physics A: Mathematical and Theoretical*, Vol.42, No.19, pp.5003, May 2009.

48. Gol’dshtein, V., G. A. Koganov and G. I. Surdutovich, “Vulnerability and Hierarchy of Complex Networks”, September 2004.

49. Wang, X., S. Guan, C. H. Lai, “Protecting infrastructure networks from cost-based attacks”, *New Journal of Physics*, Vol.11, No.3, pp.033006+, March 2009.

50. Latora, V. and M. Marchiori, “Vulnerability and protection of infrastructure networks”, *Physical Review E*, Vol.71, No.1, pp.015103, January 2005.

51. Gorman, S. P., L. Schintler, R. Kulkarni, R. Stough, “The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure”, *Journal of Contingencies and Crisis Management*, Vol.12, No.2, pp. 48-63, 2004.

52. Chassin, D. and C. Posse, “Evaluating North American electric grid reliability using the Barabasi-Albert network model”, *Physica A: Statistical Mechanics and its Applications*, Vol.355, No.2-4, pp. 667-677, September 2005.

53. Sole, R. V., M. Rosas-Casals, B. Corominas-Murtra and S. Valverde, “Robustness of

the European power grids under intentional attack", *Physical Review E*, Vol.77, No.2, pp.026102, February 2008.

54. Arianos, S., E. Bompard, A. Carbone and F. Xue, "Power grid vulnerability: A complex network approach", *Chaos: An Interdisciplinary Journal of Nonlinear Science*, Vol.19, No.1., pp.013119-013119-6, March 2009.

55. Albert, R., I. Albert and G. L. Nakarado, "Structural vulnerability of the North American Power Grid", *Physical Review E*, Vol.69, No.2, pp.025103, February 2004.

56. Carvalho, R., L. Buzna, F. Bono, E. Gutierrez, W. Just and D. Arrowsmith, "Robustness of Trans-European Gas Networks: The Hot Backbone", *Physical Review E*, Vol.80, No.1, pp.016106, July 2009.

57. Kaiser, M. and C. C. Hilgetag, "Edge vulnerability in neural and metabolic networks". *Biological Cybernetics*, Vol.90, No.5, pp. 311-317, May 2004.

58. Berche, B., C. von Ferber, T. Holovatch and Y. Holovatch, "Resilience of public transport networks against attacks", *The European Physical Journal B - Condensed Matter and Complex Systems*, Vol.71, No.1, pp.125-137, September 2009.

59. von Ferber, C., T. Holovatch and Y. Holovatch, "Attack Vulnerability of Public Transport Networks", *Traffic and Granular Flow*, Vol.4, pp.721-731, 2009.

60. İstanbul Karayolları Haritası, www.tkm.gov.tr, 2010.

61. İstanbul Raylı Sistemler Ağı, www.istanbululasim.com, 2010.

62. Türkiye Demiryolları Haritası, www.tcdd.gov.tr, 2010.