IDENTIFYING VULNERABILITIES AND EXTREME RISKS IN CRITICAL INFRASTRUCTURE NETWORKS

AKHILA KIZHAKKEDATH

School of Mechanical and Aerospace Engineering

A thesis submitted to Nanyang Technological University
in partial fulfillment of the requirements for
the degree of Master of Engineering

2015

ACKNOWLEDGEMENT

First of all, I would like to express my sincere thanks to Dr. Tai Kang, my research guide without whom this research as well as report would have been impossible. He was always kind hearted and approachable and gave me ample time to learn the basics of my research area. He helped me whenever I got stuck and always showed me the right direction.

I would also like to thank my friends and family, especially my husband, who always stood by me during my tough times.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS

A_0	Initial accessibility of a network
A_k	Accessibility of a network after the removal of k nodes
C	Consequence measure of $G(V, E, U)$ for some failure
$C_b(i)$	Betweenness centrality of node i
$C_c(i)$	Closeness centrality of node i
$C_{cl}(i)$	Clustering coefficient of node i
$C_d(i)$	Degree centrality of node i
C_i	Capacity of node i
CF_j	Congestion function of node j
d_{ij}	Shortest path length between nodes i and j
E_0	Initial efficiency of a network
E_k	Efficiency of a network after the removal of k nodes
e_i	Number of links that exist between the neighbors of node i
$e_{i,max}$	Max. number of links existing between the neighbors of node i
e_{max}	Maximum number of links in a network
$G(V, E)$	A generic critical infrastructure network
$G(V, E, U)$	A network with unforeseen interdependencies
G_c	Giant component of $G(V, E, U)$ for some failure
$\|G_c\|$	The number of nodes in G_c or the giant component size
g	Number of subnetworks in a network
gd_{ij}	Real geographic distance between nodes i and j

L_i	Initial load at node i
$L_{j,failed}$	Total load at node j after failure and flow redistribution
l_j	Additional load received by node j upon a failure in network
m	Number of links in a network
n	Number of nodes in a network
n^i	Number of nodes which can be reached from the i^{th} node
P	Failure probability of $G(V, E, U)$ for some failure
U	A set of unforeseen interdependencies
V	Set of all nodes in a network
α	Alpha index of a network
α'	Tolerance parameter
β	Beta index of a network
γ	Gamma index of a network
ε_{ij}	Sum of congestion functions of nodes in shortest path between i and j
μ	Cyclomatic number of a network
Γ_i	Set of neighbor nodes of node i

LIST OF PUBLICATIONS

Kizhakkedath, A., Tai, K., Sim, M.S., Tiong, R.L.K. and Lin, J. (2013) "An Agent-Based Modeling and Evolutionary Optimization Approach for Vulnerability Analysis of Critical Infrastructure Networks", in Tan, G., Yeo, G.K., Turner, S.J. and Teo, Y.M. (Eds), *AsiaSim 2013 – Proceedings of the 13th International Conference on Systems Simulation*, Singapore, 6-8 November 2013, Communications in Computer and Information Science Vol.402, Springer, pp.176-187

Tai, K., Kizhakkedath, A., Lin, J., Tiong, R.L.K. and Sim, M.S. (2013) "Identifying Extreme Risks in Critical Infrastructure Interdependencies", in *ISNGI 2013 – International Symposium for Next Generation Infrastructure*, Wollongong, Australia, 30 September - 4 October 2013.

ABSTRACT

Today's society is becoming highly dependent on the services provided by various critical infrastructure networks. The increasing complexities and interdependencies among infrastructure networks have exacerbated their susceptibility to various disruption or failure events. It is therefore crucial to understand how the failure of the components in a critical infrastructure network affects the performance and integrity of the whole network. Different types of component failures may result in different levels of failure consequence and it is interesting to investigate which type of failure results in the largest failure consequence in an infrastructure network. A review on critical infrastructure protection shows that there is a need to incorporate geographic proximities in the failure cascading process in infrastructure networks. Hence this research initially investigates the failure consequence in a critical infrastructure network resulting from different types of component removals using a proximity-based cascading model for failure propagation. The feasibility of the proposed study is tested on a real-world transportation network.

A review on critical infrastructure simulation and analysis also suggests that all the analyses and subsequent policy decisions on critical infrastructure networks have been made based on the assumption that the infrastructure interdependencies model has been constructed to a fair degree of completeness. Although such analyses that aim at the identification of weaknesses and vulnerabilities in infrastructure networks may go some way in preventing or alleviating disastrous outcomes, the failure to consider unforeseen interdependencies among critical infrastructures can result in extreme disruptions not being anticipated. The review also indicates that although approaches for vulnerability/consequence analysis have been widely studied, a complete risk assessment of infrastructure network disruptions incorporating the probabilities as well as consequences of disruption events has not been given serious attention. Therefore this research also proposes using an optimization algorithm to iteratively search for the possible unforeseen interdependencies as well as the failure points that can result in extreme risk in critical infrastructures, thereby anticipating extreme risk events. In order to illustrate the feasibility of the proposed approach, an agent based model of an infrastructure network along

with its known interdependencies has been presented, with a genetic algorithm applied to search for potential unforeseen interdependencies as well as failure modes/points that can result in extreme disruptions. The results from this study show the feasibility of anticipating extreme risk events in infrastructure networks, thereby providing valuable insights for proactive risk management of critical infrastructures.

CHAPTER 1: INTRODUCTION

1.1 Background and Motivation

Today's society is becoming increasingly dependent on services provided by various infrastructures. Here, the term "infrastructure" refers to the basic physical and operational structures needed for the functioning of a society like roads, railways, canals, pedestrian walkways, postal services, telephone networks, internet, drinking water supply, sewage collection, etc. "Critical Infrastructure" is a term that is used to refer to those infrastructures whose destruction causes crippling effects on a nation's security as well as on the well-being of its citizens [1]. Initially such critical infrastructures included only the large technical systems such as electric power grids, water and fuel supply systems, transportation and communication systems. Today's critical infrastructures also include health services, banking and finance, safety and security, government, etc. that lay the foundation of most of the activities of our society. Due to the vitality of these systems, a sudden disruption in any one of them or part thereof may result in a severe strain on human life, safety and economy of the society. Some of the examples that illustrate such major infrastructure disruptions include the WTC (World Trade Center) terrorist attacks on September 11, 2001 [2], the U.S. Blackout on August 14, 2003 [3], the Sumatra earthquake in Indonesia on December 26, 2004 [4], and the Tohoku earthquake and Tsunami in Japan on March 11, 2011 [5]. These incidents and their aftermaths prove that the risks and inherent vulnerabilities in critical infrastructures should be addressed in a proactive manner since we should not wait for these incidents to happen and only then start planning how to react to them.

One of the works that has received much attention in the context of vulnerability analysis of critical infrastructure is the study on how the failure of the components in a critical infrastructure system affects the performance and integrity of the whole system. The failure of components in infrastructure systems can be triggered in a random (e.g. natural hazards, technical failures) or

intentional manner (e.g. terrorist attack) and these different triggers of failures may result in different levels of failure consequence in infrastructure systems. It is therefore motivating to study the failure consequences in critical infrastructure systems resulting from different types of component failures (e.g. random, intentional) in order to investigate which type of component failure results in the largest failure consequence.

The failure of components in critical infrastructure systems such as transportation systems, internet, power grids, etc. may also trigger cascading failures which occur in the form of traffic congestion, blackouts, etc. In most of the models describing the failure cascading/flow redistribution process in critical infrastructure systems, it is assumed that when a failure occurs, the flow/load at the failed infrastructure component (e.g. a rail transit station) will be redistributed to neighboring components. It is also assumed that the share of flow/load received by the neighboring components depends on the initial flow/load at these components. However, the geographic proximities of the neighboring components from the failed infrastructure component also play an important role in cascading dynamics. For example, when a failure occurs at a transit station in a rail transit network, the passengers will move to those stations which are closer to the failed station. A modification in the failure cascading mechanism incorporating geographic proximities is therefore another motivation behind the current work.

In addition to the fact that each of the critical infrastructures like transportation, power supply, etc. is highly complex, interconnected and also geographically dispersed, modern infrastructures also rely heavily on the services of other infrastructures. Such dependencies within an infrastructure sector (e.g. transportation) and interdependencies between infrastructure sectors (e.g. transportation and power supply) has resulted in a global system of systems that is highly vulnerable to cascading failures initiated by technical errors, deliberate attacks, climate changes, natural disasters and so on. The WTC terrorist attack (September 11, 2001) gives an illustration of the interdependencies that exist among critical infrastructures. The fire and building collapses following the attack damaged two substations located under the World Trade Center as well as power transformers, transmission lines and other

distribution equipment which further resulted in the outage of a third substation. The collapse of twin tower building also resulted in breaks in the water-mains and this further caused flooding of rail tunnels, a commuter station, and a depository containing the most important telecommunication cables which were used to perform trades on the stock exchange [2]. This example shows how the World Trade Center attack affected power supply, water supply, transportation as well as telecommunication infrastructure systems. This example shows that identifying the risks and vulnerabilities in infrastructure systems is extremely important and must take into account the effects of failure propagation/cascade on the affected sector as well as on other interdependent sectors. Therefore, the infrastructure owners who were earlier concerned only with their own domains, now have to consider the influence from other domains. Although this has led to the great improvements in the area of multi-sector infrastructures, there are still many aspects that need attention like what models can be used, what we can do to handle the large number of failure scenarios to be studied, etc.

Although numerous methods and metrics have been developed to model interdependent critical infrastructures and to analyze their vulnerability to failures, one of the common features of all these works is that they assume that the information regarding the interdependencies among infrastructures is completely known. However, many of the interdependencies may be unforeseen due to the presence of several relations and complex feedback paths that exists among infrastructure components. Critical infrastructures often undergo many subsequent upgrades and hence the information regarding critical infrastructures may also be incomplete [6]. It has also been reported that infrastructure failures often cascade along indirect links that are mostly originated by proximity which emerge at the time of crisis [6]. Some of these unknown or unforeseen interdependencies may not be crucial because they may not result in any additional disruption consequences upon some failures in critical infrastructures. However, some of the unforeseen interdependencies may trigger cascading failure of many other components resulting in larger disruption consequences. The potential unforeseen interdependencies that can result in larger disruption consequences in infrastructures upon some failures therefore need to be unraveled. Hence, an approach incorporating the possible unforeseen

interdependencies among infrastructure components needs to be developed to anticipate extreme disruptions.

Different technical infrastructure systems are usually designed in such a way that they can withstand the frequently occurring incidents. Unfortunately, these infrastructures usually do not cope well with rare incidents that result in large scale disruptions [7]. A plot of the frequency of disruption events and consequences usually follow a power law distribution [8]. The region that concerns everyone is the distribution tail, i.e. the disruption events that has low probabilities of occurrence, but result in extreme consequences. This has raised an interesting question: "How can we anticipate these tail events or extreme risk events before they occur?"

All these concerns mentioned above motivated us to go further and develop the research objectives which will be discussed in the coming section.

1.2 Research Objectives

It has been seen from the previous section that in the vulnerability analysis of critical infrastructures, it is interesting to study the failure consequences resulting from different types of component failures (e.g. random, intentional) in order to investigate which type of component failure results in the largest failure consequence. There is also a need for some modifications in the failure cascading mechanism incorporating geographic proximities between the infrastructure components. One of the primary aims of this research is therefore to use a proximity-based failure cascading model to investigate the failure consequences resulting from different types of component failures in critical infrastructure networks. It has also been seen from the previous section that the anticipation of extreme risk events in critical infrastructures is extremely important which also needs the incorporation of the possibility of unforeseen interdependencies. Therefore, a methodology to anticipate extreme risk events in critical infrastructure networks is secondly developed by considering the possibility of unforeseen interdependencies. This can be accomplished by identifying the set of critical infrastructure components to be modeled and their basic interdependencies, and then applying optimization techniques to modify the network iteratively with unforeseen interdependency relationships and failure

points until the disruption effects are maximized. The optimization algorithm will be multi-objective and the criteria for optimization will be both probability as well as consequence of failure. This helps in formulating a risk analysis framework for critical infrastructure disruptions.

Therefore the main objectives of this research are:-

a. To investigate the failure consequences in critical infrastructures resulting from different types of component (node) failures by incorporating a proximity-based failure cascading mechanism.

b. To investigate how the extreme risk events can be anticipated by solving the problem of optimizing infrastructure interdependency models for extreme failure consequences and low probabilities.

c. To investigate how the problem of multi-objective optimization of risk can be formulated.

1.3 Scope

The scope of the formulated objectives has been discussed below:

a. The failure consequences in critical infrastructure resulting from three different types of component failures will be investigated in the current research. Appropriate metrics will be used to measure the consequences of the removal/failure of components. The proximity-based failure cascading mechanism and the failure consequences of different types of component failures will be illustrated by taking transportation infrastructure as case study.

b. The proposed approach for anticipating extreme risk events involves optimization of the infrastructure interdependencies model for extreme disruptions. This can be accomplished by integrating an analysis procedure with an optimization algorithm within a computational platform. Although other optimization approaches and analysis platforms may be applicable, this research plans to use a two-objective evolutionary algorithm for optimization and an agent-based modeling platform for analysis of network disruptions.

c. As discussed earlier, since the objectives of the evolutionary algorithm include both probabilities of failure points as well as consequences, the methodology

represents a risk analysis framework for anticipating extreme disruptions. The decision variables of the evolutionary algorithm are the unforeseen interdependencies and the failure points within the network. In order to limit the scope, this research will mainly study the effect of adding up to two unforeseen interdependencies and up to two failure points, i.e. node failures. The study of link failures will be considered in future.

1.4 Organization of the report

Chapter 2 presents a literature review on critical infrastructure modeling and simulation. The review covers various topics like complex networks, risk and vulnerability analysis in single as well as multi-sector infrastructures and so on. The investigation of the failure consequences in critical infrastructure networks resulting from different types of component failures by incorporating a proximity-based failure cascading mechanism has been reported in Chapters 3. Chapter 4 discusses on a method to anticipate extreme risks in infrastructure networks and the application of the proposed method to a case study. The report concludes with Chapter 5 which discusses on the conclusions and future work of this research.

CHAPTER 2: LITERATURE REVIEW

2.1 Perspectives on risk and vulnerability

Risk is a term that is used in day-to-day life. Humans think in terms of risk in almost every field like business, safety, engineering, investment, finance and politics. Traditional risk analysis is based on a set of triplets: the failure events that can occur, the probability of occurrence of those events and their consequences [9]. Risk analysis therefore requires the identification of all the possible events that can degrade a system, the probabilities of those events and their consequences. If the studied system is very complex, the quality of risk analysis will have to be compromised due to the poor quality of probability and consequence estimates.

Vulnerability is yet another concept that is used in many research areas, but its meaning is quite ambiguous. In many definitions, vulnerability is the overall susceptibility of a system to loss due to a failure, i.e. the magnitude of damage due to a failure [7]. Vulnerability is therefore more related to network weaknesses and consequences of a failure. The main concept of vulnerability analysis is the anticipation of weaknesses in a system, i.e. identifying locations in a system where the system failures will have the gravest consequences [10]. Vulnerability can be seen from two perspectives: the first is to assess the overall vulnerability of a system, i.e. from a global perspective and the second is to find the critical parts or components in a system [7].

The various perspectives on risk and vulnerability have been explained in a number of works [11-13]. According to Johansson [7], the major difference between the concept of risk and vulnerability is whether or not the type and likelihood of an initiating failure event is estimated. In this respect, vulnerability analysis can be considered to be a part of risk analysis and combining vulnerability with the probability of a failure event exploiting the vulnerability yields risk. However, it is not always easy to find the probabilities of initiating failure events such as weather conditions or even random component failures in a system. Therefore, vulnerability assessment is critical since it provides

information on how a system performs when exposed to failures. In this research too it is believed that vulnerability/consequence analysis is a part of risk analysis and it has to be combined with the probability of failures in order to obtain a flawless value of risk as shown in Fig. 2.1.

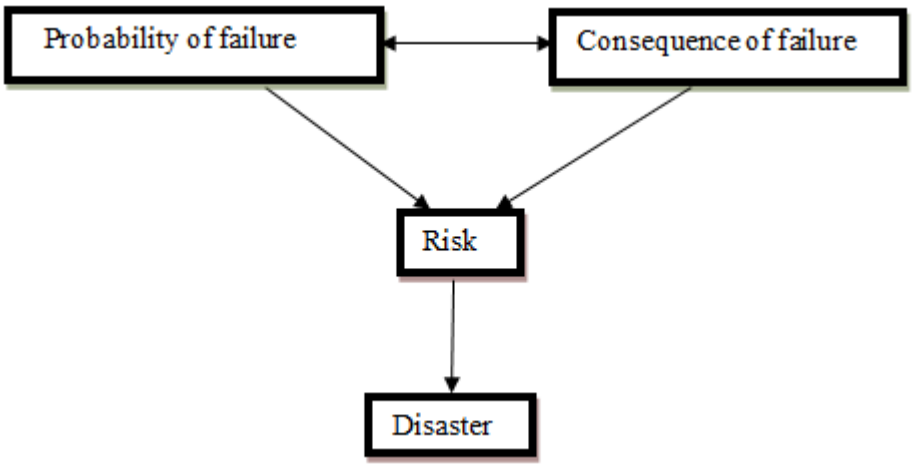

Fig. 2.1 Risk as a function of probability of failure and consequence of failure

2.2 Critical Infrastructures as Complex Networks

Conventionally, the study of networks was a branch of discrete mathematics called "Graph Theory". With the exciting works of Euler and his Konigsberg bridge problem, major developments took shape in graph theory. In addition, the concepts of social network analysis also emerged which focused on the relationship between social entities, trade between nations, communication between members of a group, etc. However, most of the studies were focused on static networks. The development of random network model was one among the pioneering works on dynamic networks [14]. In spite of the dynamic nature of random networks, it proved to be a bad model for explaining the various real world networked structures. Watts and Strogatz [15] were able to overcome these limitations by developing the small-world network model which could explain some of the characteristics of real world networks. A year later, Barabási et al. [16] came up with the scale-free nature of World Wide Web that led to a very famous model known as Barabási–Albert model. Most of the real world

networks, from the minute neuron network in the brain to the vast network of World Wide Web can be explained by these complex dynamic network models.

The various terminologies used in network theory like nodes, links, paths, loops, circuits, trees, spanning trees, degree, etc. has been explained in Appendix A.

Most of the critical infrastructures of today can be characterized as complex networks. The nodes in critical infrastructure networks abstractly represent cities, railway stations, power stations, gas stations, telephone switches, etc. and the links represent railway lines, transmission lines, pipelines, communication lines/channels, etc. Both dependencies within an infrastructure network as well as interdependencies between infrastructure networks can be modeled as links. Once modeled, both topological and functional analysis can be performed to identify the overall vulnerability as well as the critical components of these infrastructure networks. Such an analysis helps to identify the vulnerable parts of critical infrastructure networks and thereby fortification facilities can be planned to improve their robustness.

Before going into the details of vulnerability or consequence analysis of critical infrastructure networks, there is a need to understand the fundamentals of the three basic types of networks seen in real world today: random, small-world and scale-free networks. There are also three main concepts: the average path length of a network, its clustering coefficient and its distribution of degree that can be used to explain and differentiate between these networks [17].

The average path length of a network can be defined as follows [18].

Definition 2.1

The average path length of a network is defined as the mean of the shortest path lengths between all pairs of nodes in the network.

Let n refer to the number of nodes, V refer to the set of all nodes and d_{ij} refer to the shortest path length between i and j, then the average path length of a network is given by equation (2.1).

$$l = \frac{2}{n(n+1)} \sum_{i,j \in V} d_{ij} \tag{2.1}$$

Clustering coefficient can be explained using the following example. In a network, for example a network of friendship, it is not uncommon that you and a friend of your friend know each other. This property is known as clustering. Suppose that a node i in a network connects to k other nodes which are called neighbors. Then, the clustering coefficient of a node i can be defined as follows [19].

Definition 2.2

Clustering coefficient of a node can be defined as the ratio between the number of links (e_i) that actually exist between the k neighbors of node i to the maximum possible number of links ($e_{i,max}$) between them.

Clustering coefficient of node i is given by equation (2.2).

$$C_{cl}(i) = \frac{\mathrm{e}_i}{e_{i,max}} = \frac{e_i}{\frac{k\,(k\,-1)}{2}} \tag{2.2}$$

The clustering coefficient of a network is the average of the clustering coefficients of the individual nodes in the network.

According to Albert and Barabási [19], degree distribution can be explained as follows.

Definition 2.3

The spread of node degrees of a network is characterized by its degree distribution function $P(k)$, which is the probability that a randomly selected node has exactly k degrees.

With the help of these three concepts, the differences between random, scale-free and small-world networks can be explained.

2.2.1 Random Networks

Random networks do not have a particular pattern or structure. The random network model was developed by Erdös and Rényi [14]. The model consists of n nodes where any two nodes are randomly linked with a linkage probability p_l. Fig. 2.2 shows three random networks with an equal number of nodes but different probabilities p_l. The average path length scales as $\log(n)$ and the clustering coefficient is the same as p_l. Random networks are homogenous because the nodes in the network do not differ too much with respect to their degrees. These networks show similar behavior to both random and targeted attacks because of their homogenous nature.

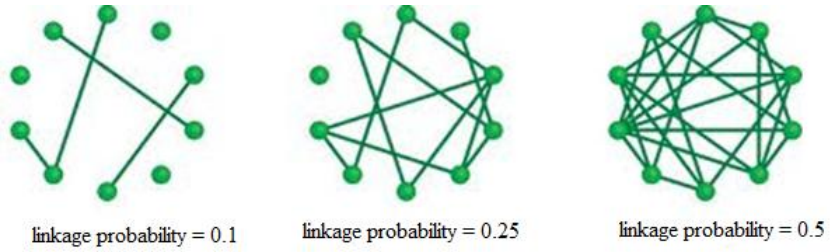

Fig. 2.2 Random networks with different linkage probabilities [20]

2.2.2 Small-World Networks

Small-world networks are those in which a majority of the network's nodes are not neighbors of each other, however most of the nodes can reach each other via a small number of links. These networks show a tendency to have cliques (i.e. subnetworks in which there are links between any two nodes) as shown in Fig. 2.3. The small-world network model was developed by Watts and Strogatz [15] in 1998. In the construction of the network model (with n nodes), initially there is a one dimensional ring lattice where every network node links with q neighbors. With a rewiring probability p_r, each link is then rewired with one end remaining fixed and the other node randomly selected, without loops. When $p_r = 0$, the network has a regular lattice structure and when $p_r = 1$, the resulting network is random as shown in Fig. 2.4. Small-world networks exhibit a high clustering coefficient for most values of p_r, but when p_r tends to 1, they act as random networks. They can also be seen as a homogenous network like random networks, but the rewiring decreases the average path length [21].

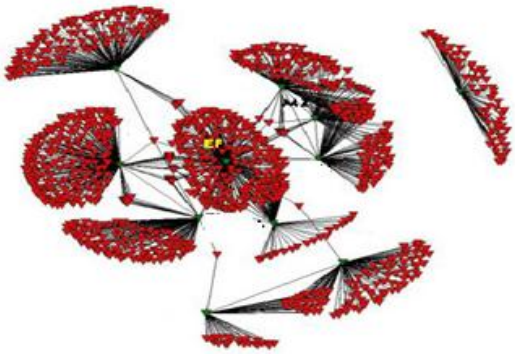

Fig. 2.3 Cliques in small-world networks [22]

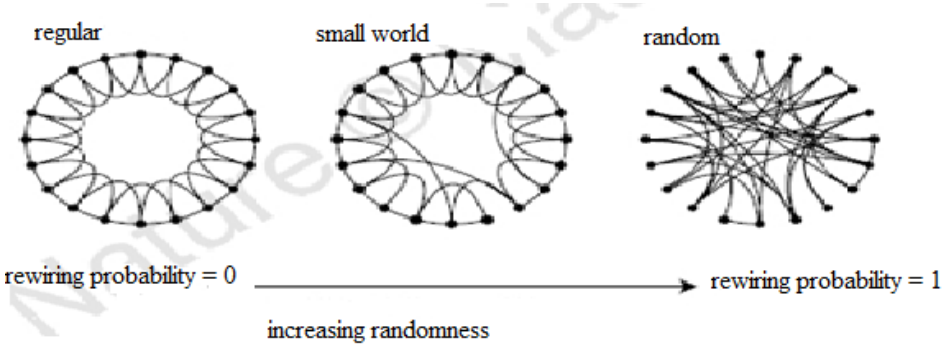

Fig. 2.4 The effect of increasing randomness on small-world networks [15]

2.2.3 Scale-free Networks

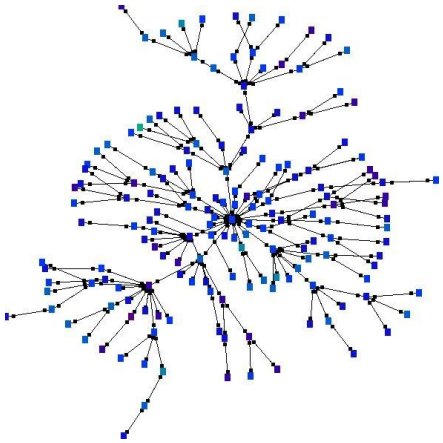

Fig. 2.5 Scale-free network [23]

Scale-free networks are those in which a few nodes have a very large number of links connected to them, but a majority of the nodes have a few number of links (Fig. 2.5). In that sense, they are non-homogeneous and follow a power law degree distribution. The reason for this phenomenon is that the new nodes that get added to the network gets preferentially linked to the existing nodes with a large number of links. In comparison with a random network (with similar number of nodes and average node degree), the average path length of scale-free networks is low and the clustering coefficient is high. The scale-free model was developed by Albert et al. [24]**.** The construction of scale-free model begins with a small number of nodes and whenever a new node gets added to the network, the links of the new node gets preferentially linked to the existing nodes with larger degrees. These networks are robust to random failures, but vulnerable to targeted attacks [24].

Most of the real world infrastructure networks like transport networks, electric power grids and World Wide Web have either random, small-world or scale-free properties. There are a multitude of papers discussing the analysis of various infrastructures as random or scale-free or small-world on the basis of their average path lengths, degree distributions, etc. Such an analysis is very helpful because it can help in understanding the hubs (hubs are the nodes with the largest degrees), flexibility or availability of alternate paths (good clustering ensures alternate paths to ensure dynamic routing upon emergencies) and also can help us to understand the survivability of networks [21]. As an example, in Sapre and Parekh [25], the Airport Network of India has been studied. The degree distribution shows its scale-free nature and therefore it is robust to random removal of nodes but breaks down on targeted attacks. The paper also mentions the benefits of such an analysis in planning during emergencies like closure of airports due to adverse weather, promoting tourism in the country and also preventing the spread of disease. The above discussion reveals that the analysis of infrastructures as random, small-world or scale-free provides us with valuable insights that can be helpful in many ways.

2.3 Impact or vulnerability analysis of single sector of infrastructure networks

There are a variety of methods available for the consequence or vulnerability analysis of single sector of infrastructure networks. The review mainly discusses on network theoretic and optimization approaches in the case of a single sector of infrastructure networks. Simulation methods like system dynamics and agent based modeling for vulnerability analysis will be discussed later in the case of multi-sector infrastructure modeling and analysis.

2.3.1 Network Theoretic Methods

There are basically two types of network theoretic approaches for assessing infrastructure network vulnerability. One type of analysis (which has been referred to as Approach 1) emphasizes on either the global or local vulnerability study by using various centrality indices and other network metrics and the second type of analysis (referred to as Approach 2) focuses on finding critical nodes using various node failure scenarios.

2.3.1.1 Approach 1

In the first type of network theoretic approach for vulnerability assessment, various measures are used to find either the global vulnerability of the entire infrastructure network or local vulnerability of the individual nodes.

Table 2.1 summarizes the important global measures and Table 2.2 summarizes the important local measures of vulnerability that are calculated for the individual nodes in a network. These tables are based on the work presented by Grubesic et al. [26]. The global measures listed in Table 2.1 were developed by Garrison and Marble [27] and Haggett and Chorley [28].

Table 2.1 Global Measures of Network Vulnerability

Metric	Formulae	Interpretations
Beta index	$\beta = \frac{m}{n}$	It is a measure of complexity: $\beta < 1$ indicates that the network has a tree structure, $\beta = 1$ indicates one more link than a tree and $\beta > 1$ indicate networks with circuits.
Cyclomatic number	$\mu = m - n + g$	A measure of the number of circuits in a network and also how many links can be removed without affecting connectivity. If the network is a spanning tree (i.e. no circuits), $\mu = 0$ and if the network has one circuit $\mu = 1$.
Alpha index	$\alpha = \frac{m - n + 1}{e_{max} - (n - 1)} * 100$	It provides a measure of connectivity. When $\alpha = 0$, the network is a spanning tree (i.e. removing any link would break the network into components) and when $\alpha = 1$, the network is maximally connected (i.e. no more links can be added).
Gamma index	$\gamma = \frac{m}{n(n-1)/2} * 100$	It is the ratio of the number of existing links in a network to the maximum possible number of links and so is a measure of relative connectivity of a network. When γ approaches a value of 1, the network is more connected and when $\gamma = 1$, the network is fully connected.

Note: m is the number of links, n is the number of nodes, g is the number of subnetworks and e_{max} is the maximum possible number of links in the network.

Table 2.2 Local Measures of Network Vulnerability

Metric	Formulae	Interpretation
Degree centrality	$C_d(i) = \sum_{j \in V} C_{ij}$	$C_d(i)$ refers to the degree centrality of a node i. If nodes i and j are connected, $C_{ij} = 1$ and V is the set of all nodes in the network. Higher degree nodes are considered to be more critical since they indicate the direct connection to many other nodes.
Betweenness centrality	$C_b(i) = \sum_{i \neq j \neq k \in V} \frac{m_{jk}(i)}{m_{jk}}$	$C_b(i)$ refers to node i's betweenness centrality, $m_{jk}(i)$ is the number of shortest paths between nodes j and k that passes through node i, m_{jk} is the total number of shortest paths between the nodes j and k and V is the set of all nodes in the network. A higher value of betweenness centrality of a node indicates that the node is a part of many shortest routes and is hence important.
Closeness centrality	$C_c(i) = \frac{1}{\sum_{j \in V} d_{ij}}$	$C_c(i)$ refers to the closeness centrality of a node i, d_{ij} is the shortest path length between nodes i and j and V is the set of all nodes in the network. A high closeness value indicates that the node is accessible to many other nodes.
Clustering coefficient	$C_{cl}(i) = \frac{e_i}{e_{i,max}}$	The clustering coefficient $C_{cl}(i)$ of a node i has already been explained in Definition 2.2 (Section 2.2). Good clustering ensures the availability of alternate paths to ensure dynamic routing upon emergencies.

To sum up, the global measures reveal the overall structure of a network and the local network centrality measures indicate individual node criticality. But it is not clear how useful these measures are in assessing which nodes if removed would be most damaging. Therefore, another trend in vulnerability assessment (Approach 2) emerged that is based on assessing the criticality of nodes by interdicting/removing them and then measuring some properties of the network that remain after disruption.

2.3.1.2 Approach 2

(a) Identification of cut nodes

A cut or articulation node is the one which when removed from the network would make the network disconnected. Therefore, if the cut nodes are found, it can be the critical nodes in a network [29].

(b) Ranking and interdiction

Here, the nodes are ranked based on their importance (for example based on centrality, etc.) and then removed on the basis of their rank. For example, Li et al. [30] have ranked the nodes based on their centrality measures like degree, closeness, etc. and then removed the nodes based on their ranks to find the critical nodes. In Gorman et al. [31] there is a mention about other indices of nodal ranking that is used to plan the node removals. They have studied the effect of various rankings like accessibility index, capacity index, global connectivity index, etc.

Apart from the different approaches for vulnerability assessment, there is a study on various measures used to indicate the failure consequence in a network. These measures mainly focus on the connectivity of the network as given below:-

(a) Diameter [18]

Definition 2.4

The diameter of a network is the length (in number of links) of the longest geodesic (shortest) path between any two nodes in the network.

If the diameter of the network that remains after removing each node is measured, it can be a fairly good indication of the loss of connectivity due to the failure of that node. Such an approach has been used by Gorman et al. [31].

(b) Giant component Size

When failures occur in a network, some nodes may get separated from the network and therefore the size or the number of nodes in the largest connected component or giant component of the network is a measure which can indicate the vulnerability of the network. When there are no failures, largest connected component of the network will include all the nodes in the network. However when failures occur, some of the nodes may get separated thereby reducing the giant component size. There are a number of papers that uses giant component size to measure the vulnerability of networks [32, 33].

(c) Spanning tree

Definition 2.5

A spanning tree of a network G *is a tree* $\subseteq G : V(T) = V(G)$ where $V(T)$ represents the set of nodes in the tree and $V(G)$ is the set of all nodes in the network.

After nodes and related links are deleted, the fewer is the number of spanning trees, the more important is the node [30].

A disadvantage with the network theoretic approaches for vulnerability assessment is that the identification of worst-case failure becomes a difficult task when the complexity of the network increases.

2.3.2 Optimization Methods

Optimization methods help to identify which combination of nodes if failed would result in the most extreme consequences. The greatest advantage of optimization-based approach is that it allows us to examine a range of disruption scenarios, both best and worst case that helps to better plan for the protection and mitigation of threats. A review on the optimization based approaches for evaluating network vulnerability is given by Murray [34], with the main approaches summarized in Table 2.3.

Table 2.3 Optimization Methods

The performance function being optimized	General problem statement	Initially proposed by
Maximal flow	Find *P* nodes/links or both in a network that upon removal would most decrease the maximum flow possible between an O-D (origin-destination) node pair.	Wollmer [35], Baran [36]
Shortest path	Find *P* nodes/links or both in a network that upon removal would most increase the shortest path possible between an O-D node pair.	Fulkerson and Harding [37], Corley and Sha [38]
Connectivity	Find *P* nodes/links or both in a network that upon removal would most decrease the connectivity of the network.	Albert et al. [24]
System flow	Find *P* node/links or both in a network that upon removal would most decrease the system flow.	Myung and Kim [39]
Access fortification	Find *P* nodes/links or both that upon fortification would most increase the level of service access in a network.	Church et al. [40]
Component attributes	Find *P* nodes/links in a network that upon removal would most decrease the total attribute impact (e.g., for attribute is population at nodes).	Grubesic and Murray [41]

2.3.3 Other approaches for vulnerability assessment

Other than the above mentioned network theoretic and optimization concepts, there have been other concepts on evaluating the vulnerability of single sector of infrastructure networks. According to Jenelius [42], links that act as alternate routes during emergencies are considered important. A link that has

small amount of flow is generally not considered very important in normal situations. However, if the link acts as a rerouting alternative for one of the heavily used links, a high priority should be given to that link. Yet another approach for vulnerability analysis in complex networks uses the concept of community detection which helps in the identification of the set/group of nodes that is vital to the connectivity of the network and its communities [43]. A community can be considered as a group of nodes that are highly connected to each other but connected to the remaining nodes with only a small number of links.

2.4 Cascading failure models of single sector of infrastructure networks

Although the behavior of an infrastructure network such as internet, transportation network, power grid, etc. largely depends on its topology, these real world networks are not only specified by their structure, but also by the dynamical properties of processes taking place in them, such as the flow of information, traffic flow, flow of electricity, etc. among the components of the network. Although previous studies have shown that node removals can have significant consequences, later, failure cascading/flow redistribution mechanisms have been studied widely [44]. Such failure cascading mechanisms triggered by the removal of nodes are common phenomena in real-life systems and can occur in many infrastructure networks including the transportation networks, internet, power grids, etc. Typical examples of cascading failures include blackouts, traffic congestion, etc. In these networks, load or flow is reassigned to bypass failed nodes leading to overloading of other nodes that are not equipped to handle this extra flow [45]. The overloading of the nodes can result in their failure resulting in further flow redistribution and this cascading process can eventually make other portions of the network also overloaded resulting in larger failure consequences. If the load/flow at a node is small, major changes will not occur with respect to the balance of loads and there are low chances of overload failures. However, a relatively large load at a node can result in a chain of overload failures thereby resulting in larger failure consequences. There are a multitude of papers that discusses on different types of dynamic models that considers such cascading or redistribution of flow/loads following failures. For

example, a cascading model proposed by Crucitti et al. [46] showed that a single node with a large load is sufficient to cause large failure consequences in a network. In Wang et al. [44], adopting the initial load/flow of a node to be a linear function of its degree, a cascading model is proposed and the cascading failures in a typical scale-free network is studied. In the load/flow redistribution process, the load at the failed node is reassigned to neighboring nodes that are linked to the failed node and the amount of additional load received by the neighboring nodes depends on the initial load at these neighboring nodes. In Mirzasoleiman et al. [47], the cascading failures following edge removals have been investigated and the flow passing through the removed edge is redistributed to its neighboring edges. This cascading model has been applied to a number of real world networks including the US airport network. Fang et al. [48] studied the cascading behavior of complex networks in the case of directed networks and tested their model on a directed random network, a directed scale-free network and an IEEE 118 network model.

In most of the cascading models studied in literature, the load/flow at a node was generally calculated as a function of its degree or betweenness centralities and after the failure cascading or flow redistribution process, the overloaded nodes fail and get separated from the network. However, in many physical networks such as Internet and transportation networks, the overloaded nodes result in only congestion or increased traveling times and are not separated or removed from the network. To incorporate this factor into cascading dynamic models, Wang et al. [49] defined a congestion function for each node to show its extent of congestion and applied this model to an Internet network. Furthermore, in many real world networks, the amount of load distributed to the neighboring nodes following failures not only depends on their initial loads but also depends on the proximities of the neighbors from the failed nodes. For example, when a failure occurs at a transit station in a rail transit network, more passengers will move to those stations which are closer to the failed station. In addition, in many infrastructures there may be nodes (e.g. railway stations) that lie in close geographic proximity with each other even though there are no physical links (i.e. railway lines) connected between them. In such cases, when a node (i.e. station) fails, its load (passenger flow) will be transferred not only to the

neighboring nodes (stations) having physical links with the failed node, but also to other nodes (stations) which lie in close proximity with the failed node (station). Therefore there is a need to incorporate geographic proximity into cascading dynamics model.

2.5 Types of Technical Infrastructure Networks

This section mainly discusses on the different types of networks to which vulnerability analyses have been applied. The vulnerability analysis has been done mainly on three types of networks: power grids, telecommunication infrastructure and transportation infrastructure. Even though there are a few works on other sectors, it is not included in the current discussion.

2.5.1 Power grids

Power grids refer to networks of high-voltage transmission lines that transport electric power over long distances both within and between countries. The nodes in a power grid correspond to generating stations and switching substations, and the links correspond to the high-voltage transmission lines.

There are a number of works that discusses on the vulnerability of power grids. For example, Arianos et al. [50] has conducted a complex network analysis of an IEEE test power network where the performance of the network to both random and targeted node removals is studied. A community detection approach has been applied to assess the vulnerability of an Italian 380 kV power system by Rocco S and Ramirez-Marquez [43]. Rocco et al. [51] explains the vulnerability assessment of Venezuelan national electric power system using an optimization approach. Different cascading models are also used to study flow redistribution mechanisms in power grids [52].

2.5.2 Telecommunication infrastructure networks

Telecommunication infrastructure that has been mainly discussed in literature includes telephone networks, computer data networks and the Internet. Murray et al. [53] has applied an optimization approach to find the critical components that would most decrease the network performance in Abilene Internet network. The network performance has been quantified with respect to both connectivity as well as flow. Gorman et al. [31] discusses about the

vulnerability analysis of computer data networks. The paper gives information on different nodal hierarchies (accessibility index, capacity hierarchy, global connectivity index and so on) and node failures based on those hierarchies. Rocco S and Ramirez-Marquez [43] has applied a community detection method for the vulnerability analysis of a telephone network in Belgium. A comparison of various global and local network theoretic metrics and optimization approaches, applied to Abilene internet network has been made by Grubesic et al. [26]. Different cascading models have also been used to study failure cascading mechanisms in Internet [47, 49].

2.5.3 Transportation infrastructure

Of all the critical infrastructure networks, transportation networks are crucial for the development of a country. The ease of transporting goods as well as people depends on the topology and geographic distribution of a transportation system. Transportation networks include airline, road, rail as well as shipping networks that aid in transportation from one place to another.

Of all modes of transportation, the road networks play a very important role in transportation. A lot of research work has been done on vulnerability analysis of road networks of different countries. For example, the concepts from complex network theory have been applied to the vulnerability analysis of the street network of Helsinki, Finland [29]. Rocco and Ramirez-Marquez [43] studied the vulnerability of a road network in an Italian province using community detection approach. In Rocco et al. [51], the vulnerability of a road network in Italy has been studied using an optimization approach.

However, with the growth of population, road transportation alone is unable to meet the travel demands of population and therefore urban metro railway systems are developed to relieve congestion in cities. Metro railway systems are rapid transit train systems with high capacity and speed, capable of providing clean, safe and reliable transit service for millions of customers daily throughout cities. There have been various works done on the vulnerability analyses of the metro rail systems of different countries. For example, the topological properties of the Shanghai subway network have been studied by Zhang et al. [54]. The study shows that the network is robust to random node removals but highly

vulnerable to targeted node removals. Deng et al. [55] have used two measures of efficiency and average path length to find the vulnerability of a metro network in China. Different cascading models are also applied to metro rail networks [47, 56].

In addition, there has also been works on vulnerability analysis of the air transportation network of different countries [57].

2.6 Multi-sector Infrastructures

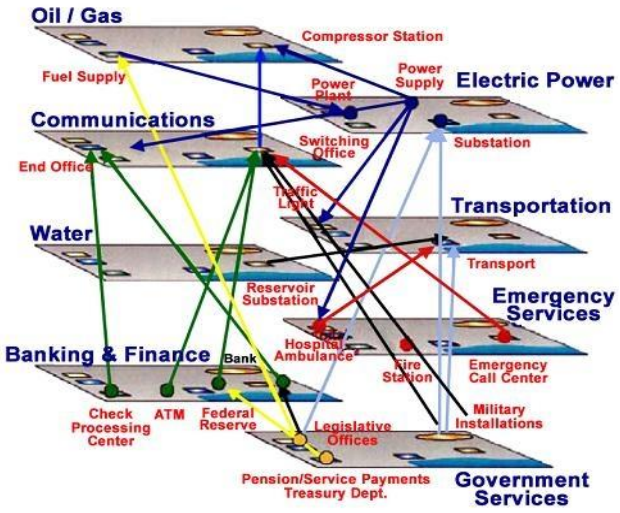

Fig. 2.6 Interdependencies in Critical Infrastructures [58]

Today's infrastructures are highly interdependent on each other (Fig. 2.6). The linking between infrastructure components of different sectors is very critical for the optimal and economic operation of various infrastructures and can improve the operation and performance of these infrastructures in many ways. However, the interconnectedness or interdependency can also introduce more weaknesses in the interdependent networks. Therefore, apart from understanding the performance of a single sector of infrastructure network, there is a need to understand the working and behavior of interdependent/interconnected infrastructures [59].

2.6.1 Types of Interdependencies

The interdependencies among infrastructure components of different sectors have been classified in many ways by various scientists. Rinaldi [60] has classified the interdependencies into four categories: physical, cyber, geographic

and logical. Dudenhoeffer et al. [61] proposed a slightly different but similar categorization of interdependencies as physical, geospatial, policy and informational. Setola et al. [62] employed the same categorization as that of Rinaldi [60], but added social interdependency as a fifth category. Table 2.4 summarizes the different types of interdependencies existing in critical infrastructures.

Table 2.4 Commonly Classified Infrastructure Interdependencies

Type of interdependency	Description
Physical	A physical or topological reliance between infrastructure components like material flow between them.
Information/Cyber	An informational or control requirement between infrastructures like SCADA.
Geographic/Geospatial	A binding that exists between the infrastructure components due to proximity.
Policy/Procedural	A binding that exists between the infrastructure components due to policy or higher level decisions: for example, government's emergency orders on a particular area due to the influence of an event.
Societal/Logical	A relationship that exists due to societal factors like public opinion, fear, cultural issues, etc.

In recent years, efforts have been made by various researchers to study the interdependencies that exist in infrastructure networks. For example, Jönsson et al. [63] modeled both physical and geographical interdependencies in a fictional electrified railway network. Both physical as well as cyber interdependencies between power grid and communication infrastructure have been modeled by Hadjsaid et al. [64]. However, Mussington [65] states that one of the shortfalls in knowledge related to critical infrastructure protection is the incomplete understanding of interdependencies among infrastructure components.

2.6.2 Modeling and Simulation of Multi-sector Infrastructures

The modeling of multi-sector infrastructures is difficult because the single infrastructures are already complex and therefore the coupling between various infrastructures adds an extra complexity to the problem. Generally, the interdependency studies and vulnerability assessment of multi-sector infrastructures has been carried out using predictive approaches or empirical approaches [66]. Predictive approaches include network theoretic models, inoperability models, system dynamic models, agent-based models, etc. On the other hand, empirical modeling aims at studying past events in order to increase our understanding of infrastructure interdependencies.

2.6.2.1 Predictive Approaches

(a) Network Theoretic Models

The main advantage of network theoretic models is that they are accurate, but their complexity increases when the system grows [67]. There are a number of works that use network theoretic models for vulnerability analysis of multi-sector infrastructure networks. For example, Johansson and Hassel [66] mentions about a network theoretic model for vulnerability analysis of a Swedish railway system which is interdependent to four other systems. In addition to constructing the topology of the systems using network theory, the flow in these networks, i.e. the functioning of these networks is also modeled using concepts from network theory. Chai et al. [3] uses various centrality measures mentioned in Table 2.2 (Section 2.3) to find the most critical infrastructure among a set of interdependent infrastructures. Yet another network theoretic framework that captures the interactions between electric power networks, telephone networks and gas supply networks has been proposed by Svendsen and Wolthusen [68]. In this model, various attack scenarios have been considered for the vulnerability analysis such as single node removal, removal of a small connected component (which can represent natural disasters like flooding), etc.

(b) Input-Output Inoperability Models (IIM)

Haimes and Jiang [69] put forward an inoperability model based on Leontief input-output model to model the interdependencies existing between infrastructures. In their approach, a system comprising 'r' interconnected

infrastructures is modeled. The input of the model includes the various failures like natural disasters, terrorist attacks, random failures, etc. and the output of the model is measured in terms of inoperability (usually measured as a continuous variable between 0 and 1 where 0 refers to the system where there are no failures and 1 refers to the condition where the system is completely inoperable), economic losses, etc. [70]. A case study on using IIM is given by Haimes et al. [71]. The study presents the application of IIM to various High-altitude Electromagnetic Pulse (HEMP) attack scenarios in United States. The impacts of the attacks are measured in terms of economic losses, inoperability, workforce earnings losses and the number affected in the workforce. Since HEMP attack has immediate effects in the power sector, the study aims to find out which sector is most affected when power infrastructure is disturbed. Yet another example is provided in Setola et al. [62] where IIM has been applied to capture the interdependencies between eleven critical infrastructure sectors in Italy where the effect of power outages are considered. The IIM is definitely a valuable tool for assessing economic losses for a system of infrastructures, but it requires the knowledge of financial data.

(c) System Dynamics

The real world complex systems have certain important properties like dynamism (they have stocks and flows), nonlinearity, feedback and time delays. System Dynamics is an approach developed by Jay Forrester [72]. In this method, a causal loop diagram is used to represent a system that takes into consideration all the components of the system along with their relationships. By capturing the relationships, the feedback loops can be found which can have either positive or negative identifier. The positive identifier indicates that a perturbation in the first component of the system causes a change in the same direction in the second component. Thus a causal loop diagram provides us with a qualitative understanding, helping us to understand the structure and behavior of a complex infrastructure system. In order to have a detailed quantitative understanding, the causal loop diagram has to be converted to a stock and flow diagram. A stock and flow diagram consists of stocks (any entity that changes, i.e. adds or decreases over time), flows (rate of change of stock), valves (controls the flows) and clouds (sources and sinks for the flows). The stock and flow

diagram can then be converted to various mathematical relationships. Conrad et al.[73] have studied the interdependencies among communication, power and emergency services using system dynamics.

A drawback of system dynamic modeling is the fixed structure of a system dynamics model: the stock levels, rates of flow, and the equations linking them have to be determined before starting the simulation [74]. Yet another feature of System Dynamics is that it does not possess spatial explicitness [75]. This means that if an attack occurs at a specific node in a networked infrastructure, the ability of the attack event to cascade depends on the behavior of the direct neighbors of the attacked node, but, in the case of system dynamic modeling the cascade can be evaluated using only the overall behavior of the network rather than the behaviors of the individual nodes. Moreover, System Dynamics supports only continuous modeling, i.e. if we need to model an attack we can only model it as a continuous process. At any time, the attack is present and what changes throughout the simulation is the proportion of nodes attacked.

(d) Agent-based simulations

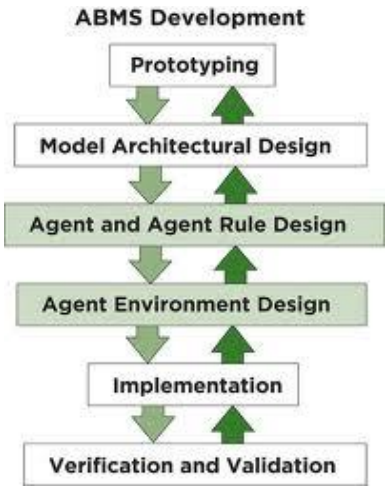

Fig. 2.7 Agent Based Model development [76]

Agent-based modeling is yet another modeling technique belonging to artificial intelligence. An agent is an autonomous computational entity and its behavior is dependent on its experience. In agent-based simulations, the agents interact with each other and also with its environment. The objectives, behavior,

and constraints of agents are modeled in the form of rules [76, 77]. The agent-based model development process is explained in Fig. 2.7.

Basically, there are two types of multi-agent approaches that are used to model the interdependencies: macro-agent and micro-agent approaches. In micro-agent based approach, every single component of an infrastructure is an agent and therefore there is a need to implement each infrastructure model from the scratch. In macro-agent approach, each infrastructure as a whole is represented as an agent and is simulated using a specific sector simulator. The detailed functions of each infrastructure agent are hidden from other infrastructure agents and only the shared functionalities between the infrastructures are exposed. Casalicchio et al. [78] used a macro-agent approach to model interdependent infrastructures.

One advantage of agent-based model compared to system dynamic models is that it can handle spatial explicitness [75]. Agent based modeling also supports both discrete as well as continuous modeling, i.e. we can model an attack as a discrete event, it can have a specific beginning and end.

2.6.2.2 Empirical approaches

Empirical approaches aim at studying past events, compiling data from those events and thus identifying general patterns of interdependencies and consequences of disruptions. As an example, McDaniels et al. [79] describes an empirical framework for multi-sector infrastructure interdependency and vulnerability assessment which includes compiling data related to the failure event, characterizing interdependencies according to their type (physical, logical, geographic, cyber), impacted systems (buildings, finance, food supply, health care), order (direct, second order, higher order), etc. as well as characterizing the consequences of the interdependencies according to their severity (minor, moderate, major), spatial extent (local, regional, national), number of people affected (few, many), etc. The authors applied the framework to examine the patterns of interdependencies that occurred in 2003 North American blackout, 1998 Quebec ice storm and 2004 Florida hurricanes. Yet another example is that of Zimmerman [80] who proposed an empirical approach in which several indicators were used to characterize the disaster data collected, like the types of

infrastructures that most frequently damaged other infrastructures, the types of infrastructures more commonly affected by other infrastructures, combinations of failures that were more frequent, the number of people affected, etc.

The two categories of approaches: empirical and predictive are complementary to each other. The empirical studies helps to provide input to predictive approaches thus aiding decision and planning.

2.6.3 Cascading failures in interconnected networks

In Section 2.4, cascading models of isolated networks had been discussed. The corresponding models for interconnected or interdependent networks are presented in this section. Interdependent networks are actually network of networks. Therefore the failures in one infrastructure network may induce failures in the other network which further results in failure of more nodes in the first network thus triggering a cascade of failures. Some of the cascading models discussed in the case of independent networks have been extended to interdependent networks as well. For example, in Tan et al. [81], the cascading failures in two interdependent scale free networks have been discussed where the load/flow at a node is estimated by its betweenness centrality. In their model, when a node is removed, the shortest paths between many other nodes are affected, thus changing the loads of other nodes resulting in the overloading of many nodes and their subsequent failures. Another example for cascading failure model in interconnected infrastructure is that of Hernandez-Fajardo and Dueñas-Osorio [82] where an enhanced betweenness centrality is used for load/flow estimation. The test networks used are a power sub-transmission system and a potable water mains network. In Wang et al. [83], the failure of edges have been studied by considering the interdependency between a power system and a gas pipeline system. The initial load at an edge is defined as a function of the product of the degrees of its end nodes and the load on a failed edge will be transferred to neighboring edges resulting in their overloading, failure and further flow redistribution.

2.7 Risk Analysis of Critical Infrastructures

It has already been stated in Section 2.1 that vulnerability analysis can be considered to be a part of risk analysis and complementing vulnerability analysis

with probability of failure gives risk. Even though there have been a large amount of work on the vulnerability analysis of critical infrastructure, there are only a few works on the risk analysis of critical infrastructure networks. As an example, Dalziell and Nicholson [84] have studied the various hazards that can close a road section in New Zealand. The hazards that have been investigated include snow, volcanic eruptions, traffic accidents, etc. and risk is quantified in terms of frequency of occurrence of the hazard events and duration of road closure (consequence). Yet another example is that of Winkler et al. [85] where risk assessment of a power grid to hurricane events is performed. The component fragility models are used to find the failure probabilities of individual power network components and transmission lines and the consequences of failures are estimated by various network topological measures.

In risk analysis, extreme risks can be defined as follows.

Definition 2.6

The risk of a failure event can be classified as an extreme risk if the failure probability of the event is very low and the consequence upon failure is high.

The term Black Swan is sometimes used to refer to these low probability, high consequence events that are quite difficult to predict. The terrorist attack of September 11, 2001, the 2004 Indonesian tsunami, etc. can be regarded as Black Swans. The term “Black Swan” was coined by Nassim Nicholas Taleb. According to Taleb [86], a Black Swan is an outlier as it lies outside the realm of regular expectations, it carries an extreme impact and in spite of its outlier status, humans concoct explanations for its occurrence after the fact, making it explainable and predictable.

The world today is ruled by power law because of the occurrence of extreme events. The distribution of frequency versus consequence of many disruption events like floods, landslides, etc. can often be approximated by power-law distributions. This is because even though a10-year flood is more frequent than a 100-year flood, the 100-year flood will be more devastating. It is the events in the heavy tail (like the 100-year flood) that creates deadly consequences and becomes an extreme risk event.

The critical infrastructures of today are extremely susceptible to extreme risk events. The anticipation of these extreme risk events is therefore very important in disaster planning and mitigation activities.

2.8 Summary of the state-of-the-art in critical infrastructure protection

Sections 2.1-2.7 of Chapter 2 provides a summary of the research work in the domain of critical infrastructure protection with respect to mainly the methods and models used for analysis and the type of networks used. The literature review shows that the challenging problem of modeling and constructing the models of critical infrastructures has motivated much work over the last decade. The review also shows that these works have emphasized on the identification of methods for describing the structure and functioning of critical infrastructure systems, with a focus on identifying the most critical infrastructure component/asset.

These identified problems show that all analyses and subsequent policy decisions in critical infrastructure protection are made based on the assumption that the infrastructure interdependencies model has been constructed to a fair degree of completeness, i.e. the set of interdependencies is completely known beforehand. They fail to assume that a significant part of the network interdependencies/links may in fact be unforeseen. Setola and De Porcellinis [6] has reported that the information regarding interdependencies may be incomplete due to the frequent upgradation of infrastructures and O'Rourke [2] has reported that since many of the networks are underground, the proximity of aging and weakened pipelines to other important facilities like high-pressure gas mains is not frequently recognized. Furthermore, Mussington [65] has stated that one of the major shortfalls in the knowledge of critical infrastructure protection is the incomplete understanding of the interdependencies among infrastructure components. This research therefore challenges the current thinking and paradigm about infrastructure modeling and analysis which is based on the assumption that the network of infrastructure interdependencies has been constructed to a fair degree of completeness. By assuming that a significant part of the network interdependencies is unforeseen, the novelty of the proposed

approach for identifying extreme risk lies in the application of an optimization algorithm to search for unforeseen interdependencies and failure points that can give rise to extreme disruptions in critical infrastructure networks.

Furthermore, most of the works discussed in literature focuses on the vulnerability or consequence analysis of infrastructure networks neglecting the probabilities of failure. However, a complete risk analysis involving the probabilities of different failure events is very crucial for anticipating extreme risk events.

The literature review also shows that investigating the failure consequences in critical infrastructures resulting from component/node removals or failures is a widely researched topic in critical infrastructure protection. Although there are numerous models describing the failure cascading mechanism following component removals/failures, there still needs to be some modifications incorporating geographic proximities between infrastructure components. This is because in real world, the amount of flow distributed from a failed node to the neighboring nodes following failures not only depends on their initial loads but also depends on the proximities of these neighbors from the failed node. In addition, in many infrastructures such as the transportation network, there may be nodes (e.g. railway stations) that lie in close proximity with each other even though there are no physical links (e.g. railway lines) connected between them. In such cases, when a node fails, its load (passenger flow) will be transferred not only to the neighboring nodes having physical links with the failed node, but also to the nodes which lie in close proximity with the failed node.

In order to close these identified gaps, this research proposes the following:

a. Using a proximity-based failure cascading mechanism to investigate the failure consequences in infrastructure networks which helps to incorporate geographic proximities into vulnerability analysis.

b. The concept of synthesizing (optimizing) the infrastructure network by the addition of unforeseen interdependencies which helps to overcome the limitation of assuming the completeness of the network model.

c. Formulating the optimization problem as multiobjective risk maximization problem which helps to incorporate both probability as well as consequence into risk analysis thereby providing a framework for anticipating extreme risk events.

The details of the proposed approaches will be discussed in the coming Chapters.

CHAPTER 3: IDENTIFYING VULNERABILITES IN CRITICAL INFRASTRUCTURE NETWORKS BY A PROXIMITY-BASED FAILURE CASCADING MODEL

Critical infrastructure networks play a crucial role in the economic development of a country and also in the well-being of its citizens. These networks are however vulnerable to failures due to natural disasters, component aging, terrorist attacks and so on and the resulting service disruptions may result in debilitating impacts on the whole society. It is therefore crucial to understand how the failure of the components in a critical infrastructure network affects the performance and integrity of the whole network. Different triggers/types of failures (e.g. random, intentional) may result in different levels of failure consequence and hence it is important to investigate which type of component failure results in the largest failure consequence in an infrastructure network. The literature review shows that there is a need to incorporate geographic proximities in the failure cascading process in infrastructure networks because the amount of load distributed to the neighboring nodes following failures not only depends on their initial loads but also depends on the proximities of the neighboring nodes from the failed node. Hence a proximity-based failure cascading model for vulnerability analysis of critical infrastructure networks is proposed and the failure consequences in these networks following random and targeted/intentional node removals will be studied. The following sections provide the details of the cascading model together with case studies on transportation infrastructure networks.

3.1 The failure cascading (flow redistribution) process

When a node loses its ability to continue functioning normally due to equipment damage, climatic conditions or intentional attacks, the load/flow at this node will be redistributed quickly to other nodes in the network. In this section, a description of how flow/load is redistributed upon node failures has been provided. We represent a generic critical infrastructure network as an undirected network $G(V, E)$ where V represents the set of all nodes in the

network, E represents the set of links and $n = |V|$ represents the number of nodes in the network. The distribution of flow/load at nodes (e.g. rail transit stations, etc.) in a critical infrastructure network depends on various factors like the topology of the network, population of the area, facilities available and so on. All these factors contribute to the usage or utilization of various nodes in a network. It is not always easy to determine the actual load at each node, or perhaps such information is not readily available to the public. Hence it is quite reasonable to assume that the load or flow at a node is dependent on the topological properties of the node. It is therefore wise enough to use topological metrics like degree of a node as a proxy/substitute for the load or flow at the node. The degree of a node indicates the number of links connected to that node. It is also known that the degree of a node has an important relationship with the geographical population density of that node [54] and hence the degree of a node is looked at as an indicator for estimating load/flow in the current work. Compared to the real physical models explaining the behaviour of critical infrastructure networks under failures, the computational demand of analyses using such proxy load metrics is also not very high. Furthermore, such analyses using proxy metrics help to understand the basic flow adjustments taking place in these networks after failures.

Following previous models addressing cascading phenomenon, each node in a critical infrastructure network also has a capacity threshold, which is the maximum load or flow the node can handle. Since the node capacity cannot be extremely large and is generally limited by cost, it is natural to assume that the capacity of a node i denoted by C_i is proportional to its initial load L_i as shown in equation (3.1). In this equation, the constant of proportionality α' denotes the tolerance parameter.

$$C_i = \alpha' L_i \quad i = 1,2,\dots,n \; and \; \alpha' \geq 1 \tag{3.1}$$

Under normal operating conditions, the load at a node will be less than the assigned capacity of the node. Under certain conditions like terrorist attacks, random technical failures, climatic conditions, etc., nodes can fail. When a node

is subjected to failure, it is assumed that the load at that node will be redistributed to neighbouring nodes. There are some nodes which are geographically very close to each other (within 1 km in this case) which are not connected by links. Apart from the physical links that represent the railway lines, roads, etc. these geographic proximities are also modeled in the current work. During load redistribution, it is assumed that the load or flow at the disrupted/failed node will be redistributed to those neighboring nodes that have either a physical link connection or geographic proximity with the disrupted node as illustrated in Fig. 3.1. The amount of load received by these neighbouring nodes depends on the initial load at these nodes as well as the geographic distance of these neighbouring nodes from the disrupted/failed node.

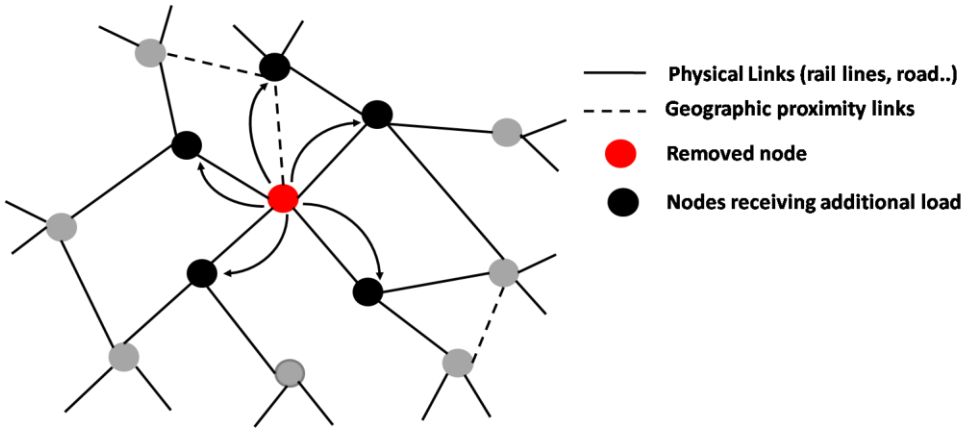

Fig. 3.1 An illustration of the failure cascading mechanism following a node removal in an infrastructure network.

The additional load l_j received by a neighbouring node j upon failure of a node i is given by equation (3.2) where L_i and L_j represents the initial loads at node i and j respectively, Γ_i represents the set of neighbour nodes of node i and gd_{ij} represents the real geographic distance between nodes i and j.

$$l_j = L_i * \frac{\frac{L_j}{gd_{ij}}}{\sum_{v \in \Gamma_i} \frac{L_v}{gd_{iv}}} \tag{3.2}$$

Hence the total load at a neighboring node j following flow redistribution becomes the sum of its initial load and the additional load as shown in equation (3.3).

$$L_{j,failed} = L_j + l_j \tag{3.3}$$

If the load at a node after flow redistribution exceeds the capacity of the node, congestion develops and the level of congestion depends on how much the load exceeds the capacity. Congestion function CF_j is used to indicate the level of congestion on node j and has been represented by equation (3.4) where C_j represents the capacity of node j and n represents the number of nodes.

$$CF_j = \begin{cases} 1 & , L_{j,failed} \leq C_j \\ 1 + \dfrac{L_{j,failed} - C_j}{C_j} * (n-1) & , C_j < L_{j,failed} \leq 2 * C_j \\ n & , L_{j,failed} > 2 * C_j \end{cases} \tag{3.4}$$

The three cases in equation (3.4) refers to normal, congested and heavily overloaded states of nodes and only the heavily overloaded nodes are assumed to be removed (like the temporarily shut down of a transit station) leading to further load flow redistribution.

3.2 The Networks used for Analysis

The proposed failure cascading model will be illustrated on transportation networks. In this work, the networks used for study are the rapid transit railway network of Singapore, the network of bus interchanges/terminals of Singapore and the combined rapid transit-bus network. Singapore is located at the southern tip of the Malay Peninsula in South East Asia. With an estimated population of 5.4 million people and a land area of only 716.1 km^2, Singapore is the third densest country in the world. Since its independence in 1965, Singapore has experienced tremendous economic development and a major part of its progress can be attributed to an efficient transportation system.

3.2.1 The Rapid Transit Rail Network of Singapore

Like other urban cities, Singapore faces the challenges of meeting the travel demands of the growing population against the constraints of physical space. The construction of a reliable rapid transit railway transport system to support the ground transportation thus became one of the crucial transport strategies of the

nation. The rapid transit railway system is the hallmark of Singapore's success, and the network is also very important to the society and economic growth of Singapore. Due to the heavy reliance of the society on the public rail transport, even simple service disruptions in the system can easily lead to unacceptable outcomes affecting a large number of commuters, thereby affecting the day-to-day activities and economic development of the nation. Large disruption events will not only cause inconvenience and travel delay for commuters; commuters can lose confidence in public transport and be encouraged to use private transport in the long run. A sequence of serious disruptions happened in the rapid transit network in 2011 and the disruptions affected over thousands of passengers and commuters. During the disruptions, traffic congestions were reported in many major areas in Singapore. For example, on 20th September 2011, a power fault disrupted train services at 16 stations. The resulting four hour delay left thousands of commuters (approx. 27,000) stranded during rush hour [87]. Similar incidents took place in Dec 2011: train service at 11 stations was disrupted for 5 hours and the commuters had to walk through the train tunnels to the nearest station in order to exit [88]. With these recent frequent breakdowns in the rail services, questions were raised about the vulnerability of the rapid transit network. Hence, the rapid transit rail network of Singapore is taken as an example to illustrate the proposed model and also to analyze its vulnerability to disruptions.

The range of public rail transport that provides services covering the entire island nation includes the Mass Rapid Transit (MRT) system and Light Rail Transit (LRT) system. The MRT system constitutes the major component of the railway system in Singapore, spanning the entire city-state. The MRT system currently includes the North South (red) Line, East West (green) Line, North East (purple) Line, Circle (yellow) Line and Downtown (blue) Line [89]. The MRT network is complimented by a small number of regional LRT network lines that link MRT stations with Housing Development Board (HDB) public housing estates. The LRT lines act as feeder services to the MRT network. The LRT system currently includes three lines, each serving a public housing estate. Apart from the MRT and LRT lines in operation, new lines also have been proposed.

In order to construct the network for study, all the MRT and LRT lines in operation has been incorporated together with a few of the new lines for which the latitude and longitude data was available. The studied railway network is generated by considering stations as nodes and involves a total of 141 nodes. Any pair of stations is considered to be connected by a physical link when there is a real railway line between both these stations. Apart from the physical link, a different kind of link based on geographic proximity has also been incorporated into the network model; two stations are connected by a geographic dependency link if the stations are separated only by a distance of maximum 1 km. In order to identify the geographic dependency links, the distance between every pair of nodes/stations was calculated. This was done by first obtaining the latitude and longitude information of the various stations [90] and then obtaining the distance between them in kilometres. There are total of 159 physical links and 84 geographic dependency links in the rail transit network. An illustration of the rapid transit network used in the current study is shown in Fig. 3.2. The stations (represented by black circles) are placed according to real geographic positions based on latitude and longitude. The red, green, yellow, purple and blue lines are shown in their respective colors and the LRT lines are shown in black. The geographic dependency links are shown by fluorescent green lines.

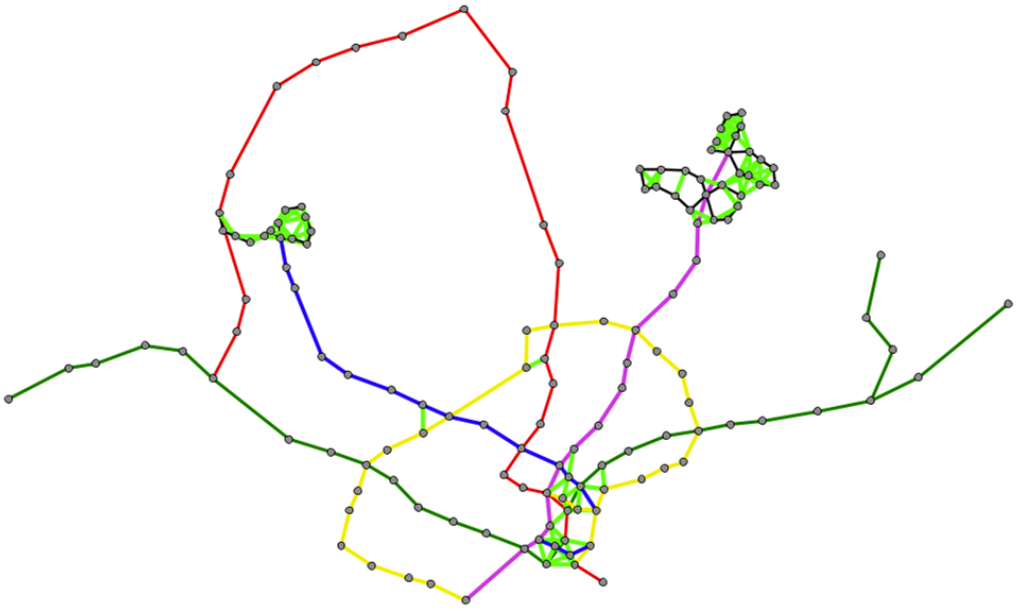

Fig. 3.2 An illustration of the rapid transit network of Singapore where geographic dependency links (fluorescent green) are also included.

3.2.2 The Bus Network

Buses form a major part of land transportation in Singapore. The bus transportation complements the Urban Rapid Transit Rail network of Singapore in transporting people to almost any corner of the city state. Buses are operated by two companies: SBS (Singapore Bus Service) Transit Limited and SMRT (Singapore Mass Rapid Transit) Corporation. There are a number of bus interchanges, terminals and bus stops in Singapore. A bus terminal is the start or end point of a bus route. Bus interchange is a bus terminal that has intersection or connection to the rapid transit rail network. For simplicity, the current work has considered only the bus interchanges and terminals. Singapore is divided into different planning regions. Each of the bus interchange/terminal is located in any one of the planning areas. Fig. 3.3 shows the distribution of the different interchanges and terminals in the different planning areas. The nodes are numbered from 142 to 182 as a continuation of the node numbering in rail transit network.

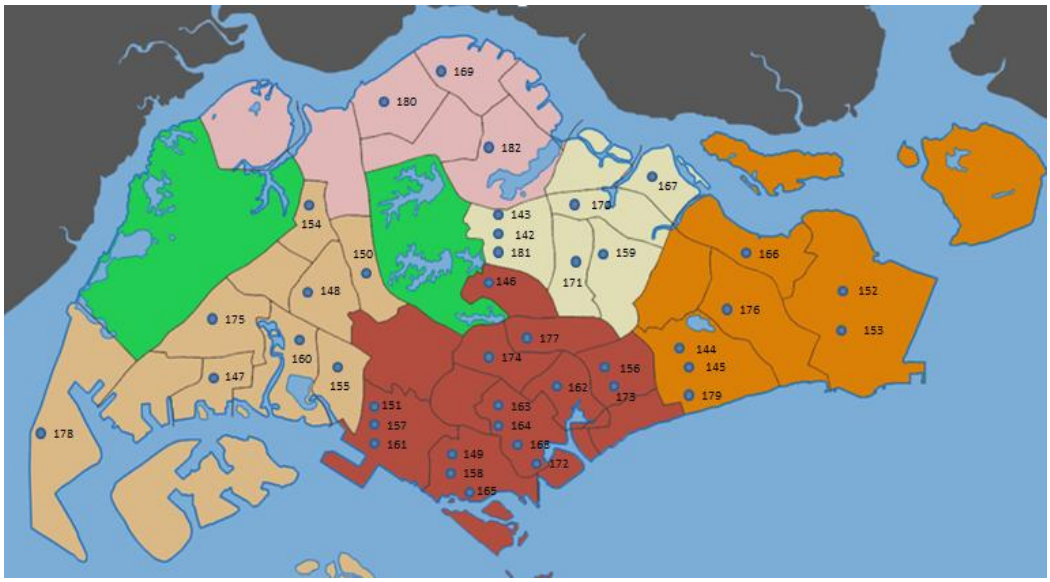

Fig. 3.3 Distribution of bus nodes (blue circles) in the different planning areas in Singapore

In order to construct a simplified bus network, it is assumed here that any two interchanges/terminals are connected by a direct bus route if they are located in adjacent planning areas as shown in Fig. 3.4. In the figure, the black circles and bold lines represent nodes and links respectively.

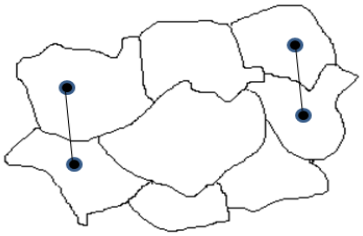

Fig. 3.4 Construction of the simplified bus network

In this way a network of bus interchanges/terminals is constructed for the case study. The constructed network has a total of 41 nodes and 181 links. Similar to the rapid transit network, the latitude and longitude information of the bus interchanges/terminals was retrieved to calculate the real distances (in kilometres) between the nodes in the bus network. There are no geographic dependency links in the constructed network. Fig. 3.5 shows an illustration of the constructed network of bus interchanges/terminals. The interchanges/terminals (blue circles) are placed according to real geographic positions based on latitude and longitude.

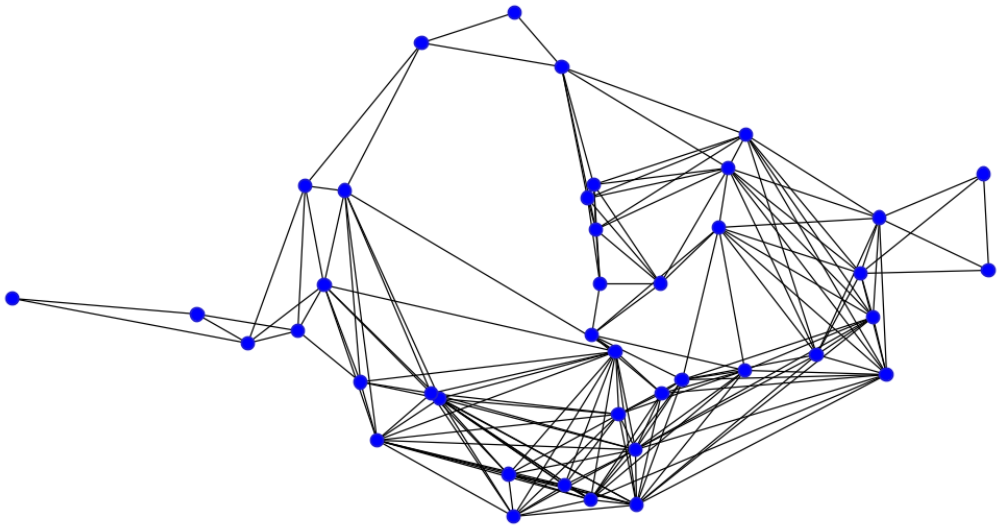

Fig. 3.5 Illustration of the bus network of Singapore

3.2.3 The Combined Rapid transit-Bus Network

In Singapore, the rapid transit rail network and the bus network works in an interconnected manner. Many of the rail transit stations are co-located with the bus interchanges. In order to construct the combined rapid transit-bus network, the geographic proximities are considered. If a node in the rapid transit network is within proximity of one kilometre with a node in the bus network, a

geographic interdependency is considered to be present between the two. These links are called geographic interdependency links rather than geographic dependency links as we called in the case of rapid transit networks because they exist between two types of networks. The geographic interdependencies are also represented by links. An illustration of the constructed combined rapid transit-bus network is shown in Fig.3.6. In the figure, the green and blue circles respectively represent the rapid transit stations and bus interchanges/terminals. The constructed network has a total of 182 nodes and 495 links. The consideration of interdependencies between the two networks is important because during a failure in the rapid transit network, the passengers will be transferred to not only other transit stations, but also to the nodes in the bus network. This can relieve some of the overloading of nodes in the rapid transit network, but at the same time can also introduce overloading of nodes in the bus network. This is a characteristic of an interdependent network: on one hand interdependency between networks is very essential for optimal and improved operation of infrastructures; on the other hand it induces more vulnerability into the system.

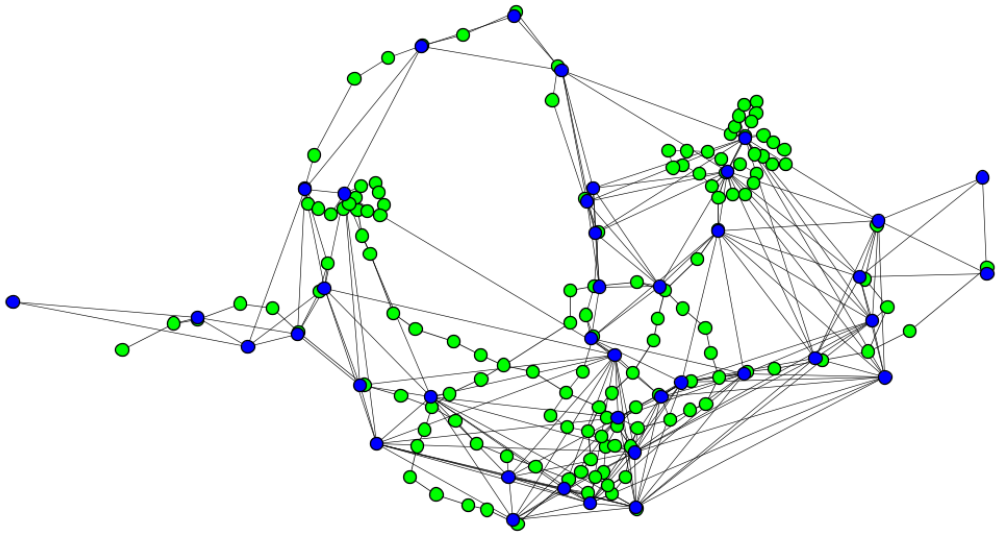

Fig. 3.6 An illustration of the combined rapid transit-bus network

3.3 Measuring the performance loss after failures

After node failures and flow/load redistribution, the failure consequence in the network has to be quantified using suitable vulnerability metrics/measures.

Since the proposed failure cascading model will be illustrated on transportation networks, two measures (efficiency and accessibility) that are suitable for measuring the vulnerability or failure consequence in transportation networks has been used.

3.3.1 Efficiency

Network efficiency is one of the measures used to describe the failure consequence of networks. If n denotes the total number of nodes in the network, d_{ij} represents the shortest path length between nodes i and j and V represents the set of all nodes in the network, efficiency is given by equation (3.5).

$$Efficiency = \frac{1}{n(n-1)} \sum_{i,j \in V} \frac{1}{d_{ij}} \tag{3.5}$$

It is assumed that the efficiency of flow/transfer between a pair of nodes is inversely proportional to the shortest path length between them. If two nodes i and j are not connected, then the shortest path length d_{ij} tends to infinity and the efficiency of flow/information transfer between those nodes tends to zero. If the efficiency of the network after a node removal is low, the removed node is critical. There are a number of papers that uses efficiency to measure the vulnerability/failure consequence of networks [46, 54, 91, 92].

Different from the normal definition of efficiency, a modified efficiency measure is used in this work in which the efficiency of load transfer or traffic flow between a pair of nodes depends on the congestion of the nodes in its path [49]. Instead of assuming that the efficiency of flow between a pair of nodes is inversely proportional to the length of the shortest path connecting them, it is assumed that the efficiency of flow is inversely proportional to the sum of congestion functions of the nodes along the shortest path. Therefore, if the nodes along the shortest path between a pair of nodes are not heavily congested the efficiency of flow will be high; else the efficiency will be low. An efficiency measure that incorporates the extent of congestion instead of shortest path length is important in evaluating the failure consequences in infrastructure networks such as transportation networks. The modified network efficiency used in this work is given by equation (3.6).

$$Efficiency = \frac{1}{n(n-1)} \sum_{i,j \in V} \frac{1}{\varepsilon_{ij}} \text{ where } \varepsilon_{ij} = \sum_{t \in P} CF_t \quad (3.6)$$

Here n refers to the number of nodes in the network during normal operation, V refers to the set of all nodes, P refers to the shortest path (with the smallest number of hops) connecting i and j and CF_t refers to the congestion of node t.

When the infrastructure network is operating normally, let the efficiency be represented by E_0 which is represented by equation (3.6). In fact the node removal changes the efficiency of the network since some of the nodes may become congested and overloaded after flow redistribution. Let the efficiency of the network remaining after the removal of k nodes be denoted by E_k. The number of nodes n in equation (3.6) is replaced by $(n-k)$and the set of nodes V is replaced by V_k which denotes the set of nodes remaining after node removal. The percentage efficiency loss after the cascading process is therefore obtained by equation (3.7).

$$Efficiency\ loss = \left(1 - \frac{E_k}{E_0}\right) * 100\ \% \quad (3.7)$$

3.3.2 Accessibility

Another vulnerability measure that has been used to measure the consequences after node removals is accessibility. The notion of accessibility in infrastructure networks such as transportation networks can be illustrated through a basic definition: accessibility is the ease with which desired destinations may be reached [93]. People who are in places that are highly accessible can reach many other destinations quickly while people in less accessible places can only reach fewer places. In certain situations where the level of service varies widely over hours of the day, this broad definition of accessibility may be modified to include factors such as time dependency [94]. In the current work, the accessibility between different nodes can be quantified as the average fraction of reachable nodes from each node [95]. If n denotes the total number of nodes under normal conditions, the passengers at each node can

reach the other $n-1$ nodes by taking one or several trains or buses. If n^idenotes the number of nodes which can be reached from the i^{th} node, then accessibility of the transportation infrastructure network can be given by equation (3.8).

$$Accessibility = \frac{1}{n}\sum_{i=1}^{n}\frac{n^i}{n-1} \tag{3.8}$$

The fraction of reachable nodes from each and every node is totalled and then divided by the number of nodes to produce the average fraction called accessibility. Under normal conditions, since the network is a single connected component, n^i is equal to $n-1$ and hence the accessibility is equal to 1.

When the infrastructure network is operating normally, let the accessibility be represented by A_0 computed by equation (3.8). After the removal of k nodes, let A_k denote the accessibility of the remaining network. The number of nodes n in equation (3.8) is replaced by $(n-k)$ which denotes the number of nodes remaining after node removal. The percentage accessibility loss after node failures and cascading process is therefore obtained as in equation (3.9).

$$Accessibility\ loss = \left(1-\frac{A_k}{A_0}\right) * 100\ \% \tag{3.9}$$

3.4 The Simulation Framework

The key purpose of understanding the dynamics of cascading failures is to control it with proper strategy. Different triggers of cascading failures may result in different levels of failure consequences in networks. The malfunctions in a critical infrastructure network can be initiated by natural hazards, technical failures, terrorism and so on. Incidents such as natural disasters, technical failures or accidents mostly occur in a random manner in these networks. Incidents like terrorist attacks target crucial nodes in the network. For a critical infrastructure network we therefore investigate the removal/failure of nodes based on different node removal strategies. Specifically, three different node removal strategies have been investigated in this work. For each strategy, different removal fractions i.e. percentages of the total number of nodes to be

removed are fixed and the required number of nodes corresponding to those fractions are removed. While removing a node, the links attached to the node are also removed. Once nodes are removed, flow/load redistribution occurs. Through these removal strategies, the current work attempts to investigate whether different removal strategies can lead to different levels of consequences following failures and load redistribution. The current work also attempts to investigate which removal strategy results in the largest failure consequence in a critical infrastructure network. The removal strategies used in this work has been explained in detail as follows [96].

3.4.1 Random removal of nodes

Random disruptions or failures represent natural hazards (floods, earthquakes), technical failures, etc. in which each node has an equal probability of being removed. Such failures can therefore be simulated by randomly choosing nodes in a critical infrastructure network corresponding to a node removal fraction and removing those nodes from the network. After nodes and their corresponding links are removed, load at the removed nodes is redistributed.

3.4.2 Removal of nodes based on node degree

In targeted failures that represent failures such as terrorist attacks, "important" or highly central nodes have more probability of failure than others. In this work, node degree (i.e. the number of links connected to a node) is used as an indicator of node importance. In order to simulate degree-based removal strategy, the nodes are selected in the decreasing order of degrees in the initial network until the number of nodes reaches the required removal fraction. The selected nodes are then removed together with their corresponding links.

3.4.3 Removal of nodes based on recalculated node degree

The degree-based removal strategy uses the information on the initial network. However when nodes are removed, the network structure changes thus leading to different distributions of node degree. Therefore in recalculated degree-based removal strategy, after the removal of a node and its corresponding links, the node degrees of all the remaining nodes are recalculated. The recalculation of node degrees and the removal of nodes with the highest degrees

continue until the required fraction or percentage of nodes is removed. This type of recalculated removal is a more natural way of removing nodes in some circumstances. As an example, consider the process of finding the critical nodes in a rapid transit rail network. The closure of any one station is likely to affect the criticality of the remaining stations and hence it justifies the use of recalculated removal strategy to study the vulnerability of critical infrastructure networks such as transportation networks.

To measure the vulnerability of critical infrastructure networks to disruptions or failures, the node removal strategies are used to remove the nodes in the network and the consequences are measured using the two measures: efficiency and accessibility. These vulnerability measures are calculated at different removal fractions starting from a minimum of 2% (of the total number of nodes) up to a maximum of 50%. For each removal fraction, about 10 realizations or runs are averaged. In the simulations, the tolerance parameter α' is set to 1.1. This means that the network nodes (i.e. the rail stations, etc.) are operating at a capacity that is 110% of their initial loads. NetLogo, an integrated modelling environment is used to perform the simulations [97]. It is particularly well suited for modelling complex systems. For simulating node removals in NetLogo, the nodes are assumed as autonomous agents that can leave the network randomly or through removal in a targeted way. The information regarding links between the nodes can be provided to NetLogo using external files. The entire procedure has been illustrated in Fig. 3.7.

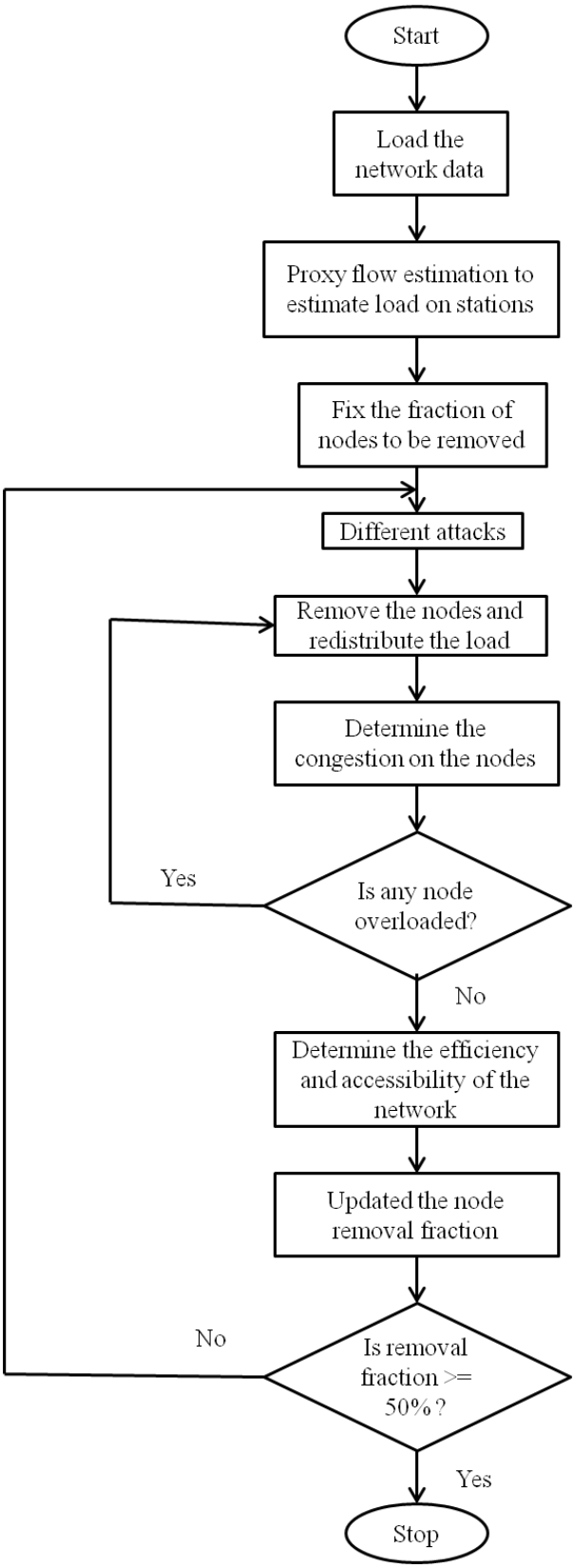

Fig. 3.7 Illustration of the simulation framework used in the current study

3.5 Simulation Results

In the current work, the vulnerability of three different transportation networks (Singapore's rapid transit rail network, bus network and rapid transit-bus combined network) to three node removal strategies has been investigated based on the proposed flow redistribution/cascading mechanism. The vulnerability indicators: efficiency and accessibility are measured at different removal fractions for each node removal strategy.

3.5.1 Analysis of Rapid Transit Rail Network

3.5.1.1 Results on Rapid Transit Rail Network Efficiency

Network efficiency is an important indicator measuring the vulnerability or failure consequence of a network. Fig. 3.8 shows how efficiency of the studied rapid transit rail network decreases under different node removal strategies as a function of the fraction or percentage of nodes removed and Table 3.1 shows the percentage efficiency loss of the network under different removal strategies and removal fractions.

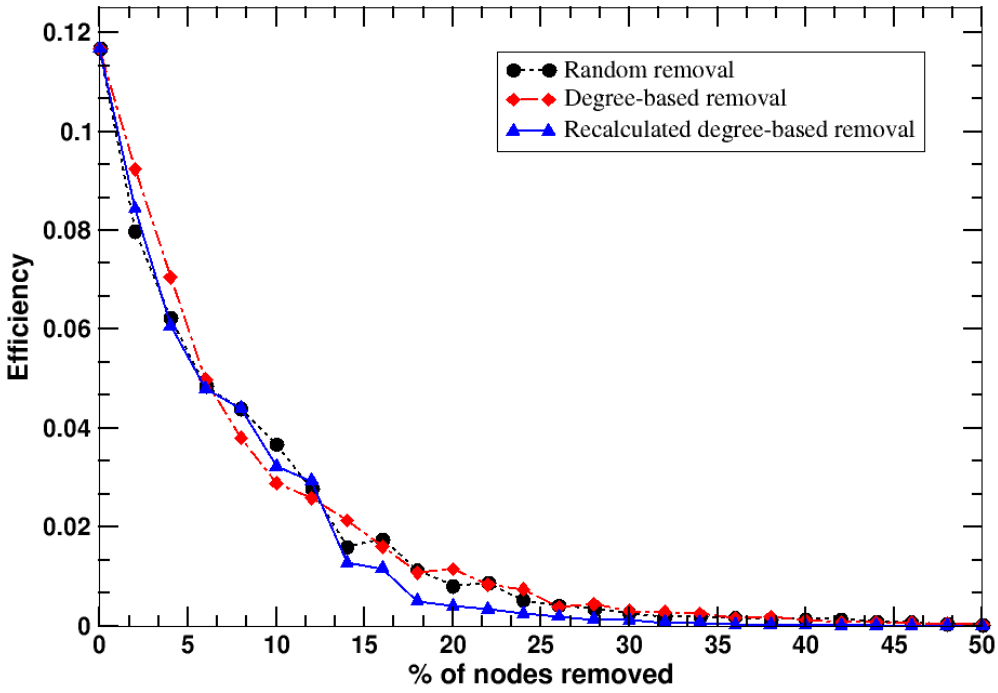

Fig. 3.8 The plot showing the efficiency degradation with different percentages of node removals in the rapid transit network

Table 3.1 The efficiency as well as % efficiency loss under the three node removal strategies in rapid transit rail network

% of node rem-oved	Random removal		Degree-based removal		Recalculated degree-based removal	
	Efficiency	Efficiency loss (%)	Efficiency	Eficiency loss (%)	Efficiency	Efficiency loss (%)
0	0.116819	0	0.116819	0	0.116819	0
2	0.07994	31.56938	0.092406	20.89803	0.084423	27.73203
4	0.062333	46.64151	0.070532	39.6228	0.060702	48.03769
6	0.048601	58.39615	0.049878	57.30358	0.048038	58.87859
8	0.043963	62.36685	0.038045	67.43277	0.043968	62.36259
10	0.036641	68.63414	0.028897	75.26319	0.032281	72.36644
12	0.027728	76.26388	0.025896	77.8324	0.029346	74.87914
14	0.016	86.30365	0.021345	81.72811	0.012735	89.09881
16	0.017572	84.95756	0.016048	86.26223	0.011589	90.07953
18	0.011323	90.30731	0.010803	90.75212	0.005012	95.71001
20	0.008134	93.03693	0.011512	90.14541	0.004034	96.54661
22	0.008736	92.52193	0.008386	92.82156	0.003362	97.12206
24	0.005236	95.51793	0.007401	93.66444	0.002448	97.90436
26	0.00406	96.52471	0.003814	96.73517	0.001935	98.34397
28	0.003537	96.97206	0.00441	96.22488	0.001291	98.89516
30	0.002636	97.74367	0.003045	97.39349	0.001146	99.01872
32	0.001966	98.31731	0.002827	97.57961	0.000657	99.43757
34	0.001914	98.3614	0.002498	97.86136	0.000662	99.43307
36	0.0017	98.54439	0.001606	98.62507	0.000346	99.7037
38	0.001377	98.82116	0.001791	98.46706	0.000236	99.79834
40	0.001391	98.8091	0.001192	98.97982	0.000173	99.85192
42	0.00136	98.83608	0.000831	99.28838	5.91E-05	99.94944
44	0.0009	99.22948	0.000682	99.41627	2.33E-05	99.98009
46	0.000816	99.30114	0.000658	99.43672	1.46E-05	99.98752
48	0.000416	99.6439	0.0004	99.65764	1.11E-05	99.99051
50	0.000291	99.75122	0.000344	99.70527	7.18E-06	99.99385

It can be seen from Fig. 3.8 that the efficiency decreases in a similar manner for random, degree-based and recalculated node removal strategies. This is an indication that the studied rapid transit network is a random network. Therefore, the removal of a node, no matter randomly or intentionally does not result in

much variation on the performance of the whole network. That is the reason why the efficiency curves are close to each other in all the removal strategies. As an example, Table 3.1 shows that after 10% of nodes are removed, there is a loss of 68.63 % and 72.36 % of network efficiency in the case of random and recalculated removal strategies respectively. Fig. 3.8 also shows that the drop in efficiency is fast for all the removal strategies which is further validated by Table 3.1 which shows that by about 16-18 % of node removal, approximately 90% efficiency has been lost.

3.5.1.2 Results on Rapid Transit Rail Network Accessibility

Accessibility is yet another vulnerability indicator and the accessibility of any network under normal conditions is 1. When nodes are removed, the network's accessibility worsens since failures make it increasingly difficult for different stations to be reachable from each other. Fig. 3.9 shows the plot of accessibility and Table 3.2 lists the accessibility loss of the network under different node removals.

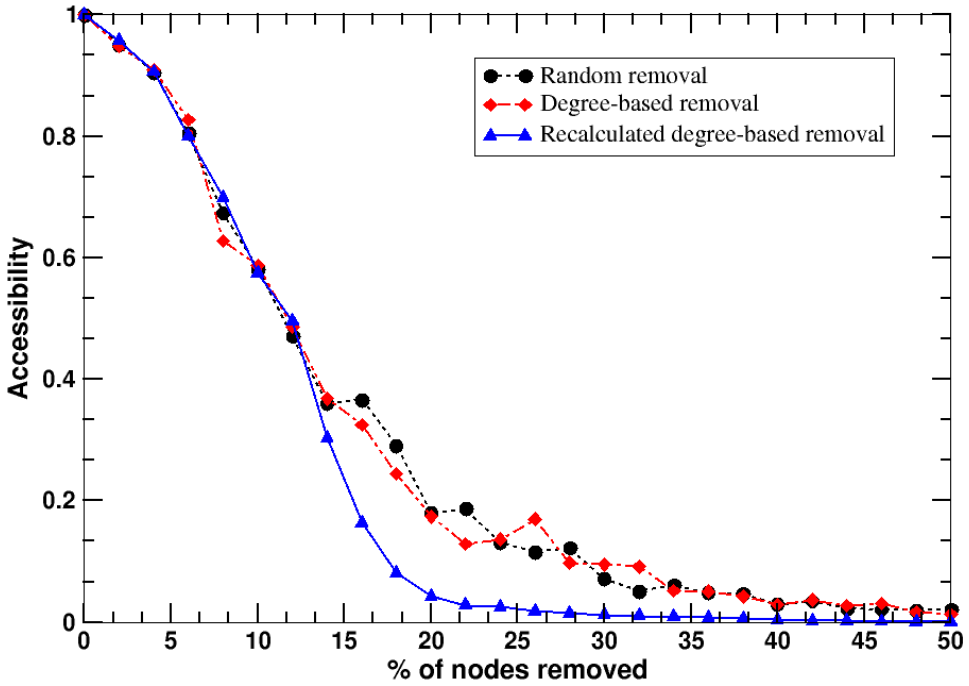

Fig. 3.9 The plot showing the reduction in accessibility with different fraction of node removals in the rapid transit network

Table 3.2 The accessibility as well as % accessibility loss under the three node removal strategies in rapid transit rail network

% of nodes removed	Random removal		Degree-based removal		Recalculated degree-based removal	
	Accessibility	Accessibility loss %	Accessibility	Accessibility loss %	Accessibility	Accessibility loss %
0	1	0	1	0	1	0
2	0.950871	4.912867	0.948217	5.178318	0.957751	4.224924
4	0.905714	9.428571	0.909625	9.037487	0.906413	9.35867
6	0.805309	19.4691	0.827062	17.29382	0.800679	19.93212
8	0.673121	32.68794	0.627629	37.23708	0.699534	30.04661
10	0.581783	41.82168	0.587163	41.28369	0.574357	42.56434
12	0.46997	53.00304	0.486272	51.37285	0.49613	50.38703
14	0.36074	63.92604	0.367882	63.21175	0.303982	69.60182
16	0.366261	63.37386	0.324843	67.5157	0.163941	83.60588
18	0.290952	70.90476	0.244144	75.58561	0.081064	91.89362
20	0.18003	81.99696	0.173931	82.60689	0.042705	95.72948
22	0.187112	81.28875	0.128886	87.11145	0.028146	97.18541
24	0.131337	86.86626	0.136282	86.37183	0.024813	97.51874
26	0.115937	88.40628	0.169858	83.01418	0.018116	98.18845
28	0.121743	87.82573	0.097822	90.21783	0.014498	98.55015
30	0.071773	92.8227	0.095076	90.4924	0.012421	98.75785
32	0.051236	94.87639	0.091388	90.8612	0.010294	98.97062
34	0.060892	93.91084	0.051641	94.83587	0.008622	99.13779
36	0.048784	95.12158	0.050598	94.94022	0.007528	99.24721
38	0.046586	95.34144	0.042594	95.74063	0.005765	99.42351
40	0.029807	97.01925	0.028723	97.12766	0.004154	99.5846
42	0.034245	96.57548	0.036555	96.34448	0.002847	99.7153
44	0.023333	97.66667	0.02768	97.23202	0.002209	99.77913
46	0.020284	97.97163	0.030922	96.9078	0.001459	99.8541
48	0.019797	98.02026	0.015947	98.40527	0.001155	99.8845
50	0.019949	98.00507	0.012695	98.7305	0.000932	99.90679

It can be seen from Fig. 3.9 that similar to the case of efficiency, the accessibility decreases in a similar manner for random and degree-based removal strategies. The decrease in efficiency under recalculated degree-based removal strategy is similar to the other two node removals up to about 13-14% of node

removal after which the accessibility decreases slightly more in the case of recalculated strategy than the other two strategies. For example in the case of random removal, at about 18 % of node removal the accessibility loss of the rapid transit network is 70.90476 % whereas the accessibility loss in the case of recalculated removal is 91.89362 %. This may be because the importance of a node may change after node removals. After removals, the nodes which were previously trivial due to low degrees now become the nodes with highest degrees.

Figs. 3.10, 3.11 and 3.12 shows the fragmentation of the studied rapid transit network after nodes are removed based on random, degree-based and recalculated degree-based removal strategies respectively. The removal fraction chosen is 18% since it is at this fraction that the difference between the accessibilities of random, degree-based and recalculated removals is the highest. A comparison of the figures shows that the network becomes just slightly more fragmented in the case of recalculated removal when compared to random and degree-based removals.

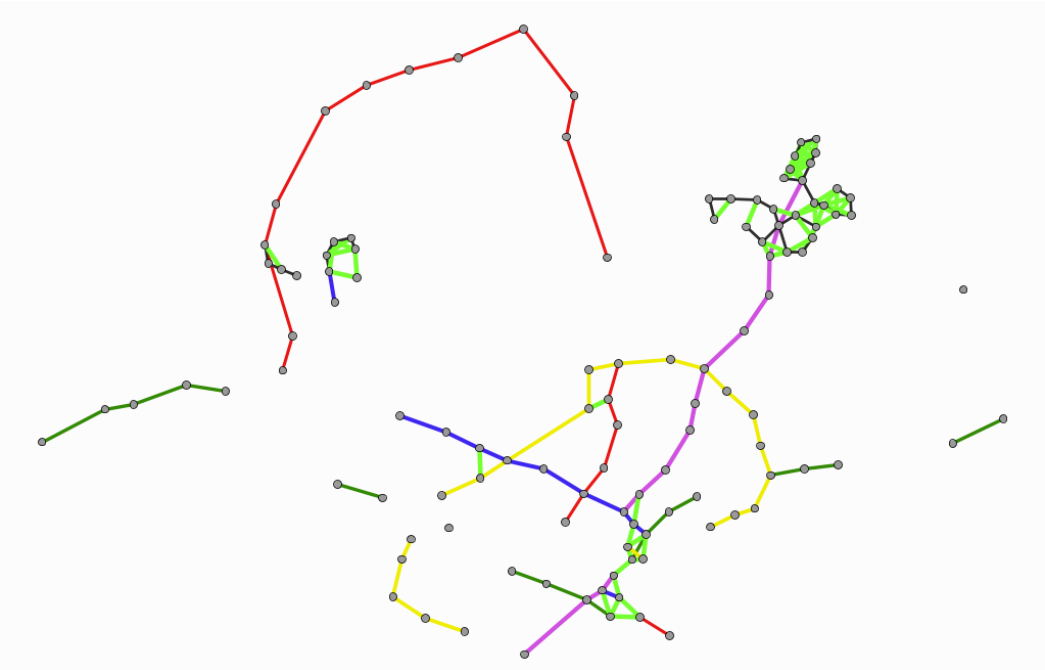

Fig. 3.10 The figure showing the network fragmentation in the rapid transit network when 18% of nodes are removed randomly

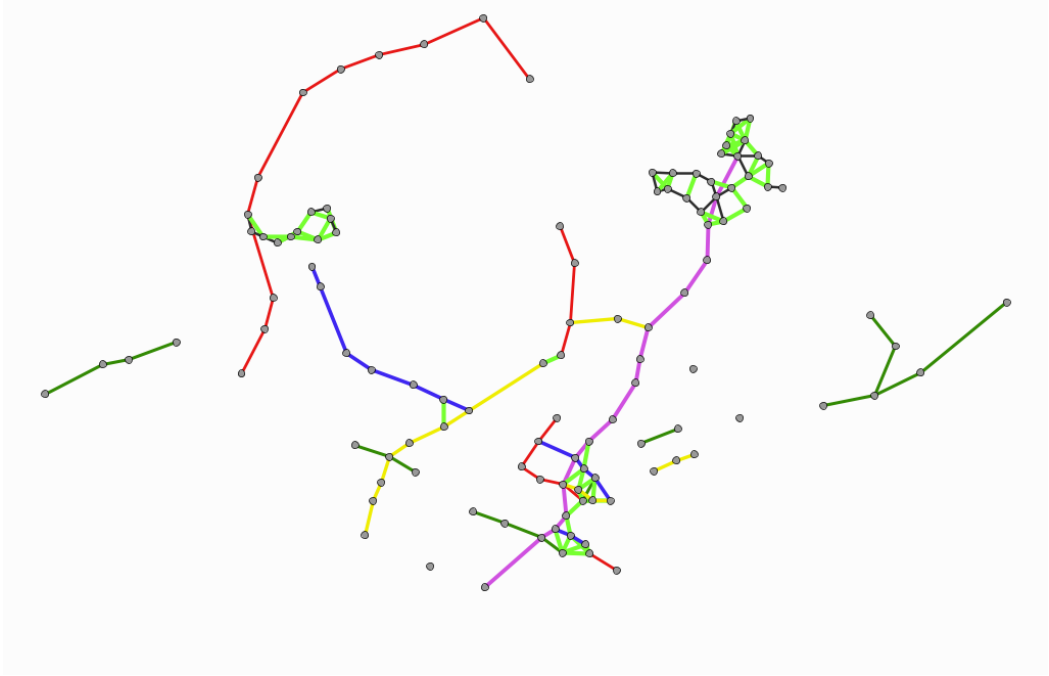

Fig. 3.11 The figure showing the network fragmentation in the rapid transit network when 18% of nodes are removed based on degree

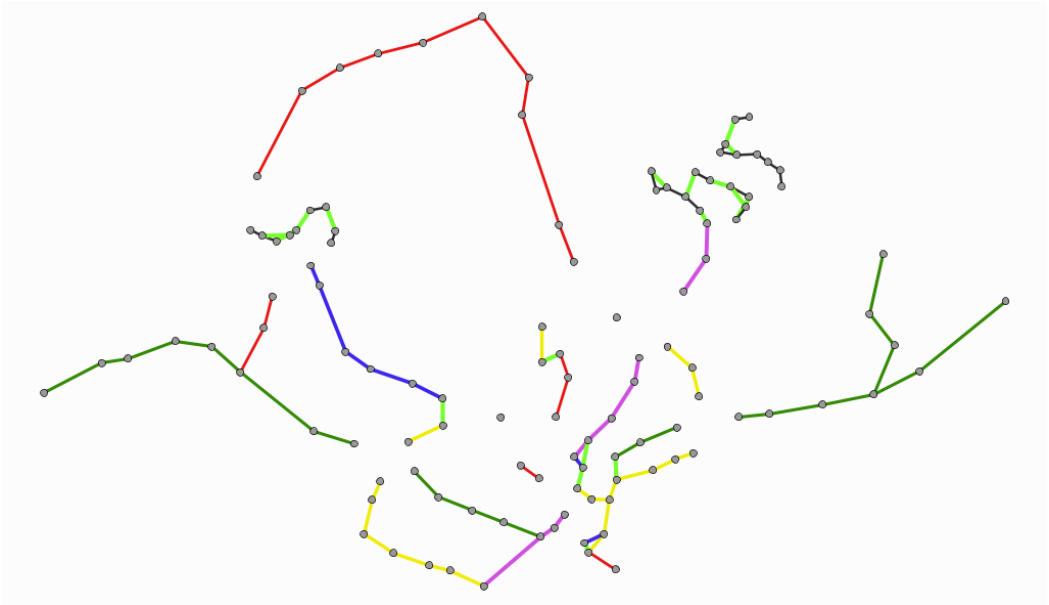

Fig. 3.12 The figure showing the network fragmentation in the case of recalculated degree-based removals when 18% of nodes are removed in the rapid transit network.

In general, the studied rapid transit network shows the behaviour of a random network since the network behaves in a similar manner to random as well as degree-based node removals. The network behaves in a similar manner to all the removal strategies with respect to efficiency. The recalculated strategy results in only slightly more damage to the network for higher removal fractions with respect to accessibility.

3.5.2 The Analysis of Bus Network

3.5.2.1 Results on Bus Network Efficiency

Fig. 3.13 shows how efficiency of the studied bus network decreases under different removal strategies as a function of the fraction or percentage of nodes removed and Table 3.3 shows the percentage efficiency loss of the network under different removal strategies and removal fractions.

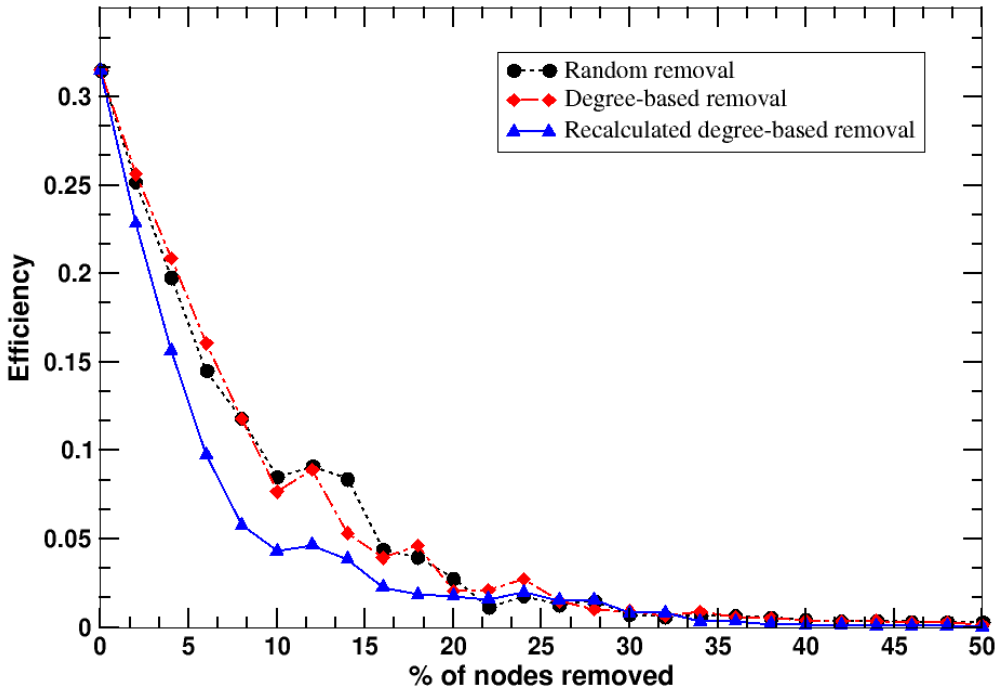

Fig. 3.13 The plot showing the reduction in efficiency with different fraction of node removals in the bus network

Table 3.3 The efficiency and % efficiency loss under the three node removals in the bus network

% of node removed	Random removal		Degree-based removal		Recalculated degree-based removal	
	Efficiency	Efficiency loss (%)	Efficiency	Efficiency loss (%)	Efficiency	Efficiency loss (%)
0	0.315032	0	0.315032	0	0.315032	0
2	0.251517	20.1623	0.256347	18.62813	0.228401	27.49913
4	0.197824	37.20637	0.208776	33.7285	0.156218	50.41196
6	0.145032	53.96472	0.16072	48.98292	0.097553	69.03387
8	0.118133	62.50378	0.118087	62.51576	0.05779	81.65589
10	0.085016	73.01627	0.07679	75.62475	0.043122	86.31172
12	0.091156	71.06732	0.089162	71.69756	0.046531	85.22963
14	0.084151	73.29093	0.053231	83.10293	0.038601	87.74705
16	0.043785	86.10455	0.039414	87.48896	0.022596	92.82737
18	0.0398	87.36973	0.046302	85.30251	0.018512	94.1239
20	0.027689	91.21426	0.020517	93.48741	0.017747	94.36673
22	0.01159	96.32453	0.021122	93.29534	0.01588	94.95916
24	0.017526	94.44029	0.027325	91.32629	0.01972	93.74026
26	0.012959	95.89006	0.01479	95.30514	0.015337	95.13146
28	0.014913	95.26979	0.010108	96.79151	0.015482	95.0855
30	0.007276	97.69418	0.009251	97.06342	0.008365	97.3446
32	0.006348	97.98882	0.006485	97.94154	0.008287	97.36953
34	0.006738	97.86477	0.00896	97.1559	0.003471	98.89805
36	0.006627	97.90012	0.005826	98.15057	0.003553	98.87202
38	0.005584	98.23112	0.004988	98.41676	0.001899	99.39722
40	0.004187	98.67462	0.003755	98.80805	0.001566	99.50277
42	0.003547	98.87799	0.003393	98.92282	0.001274	99.5955
44	0.003742	98.81605	0.003643	98.84359	0.00104	99.66992
46	0.003252	98.97141	0.002742	99.12955	0.000883	99.71974
48	0.00278	99.12122	0.002688	99.14681	0.00093	99.70469
50	0.002942	99.06984	0.001618	99.48643	0.000326	99.89659

It can be seen from Fig. 3.13 that the efficiency decreases in a similar manner for random as well as degree-based node removal strategies. However, the efficiency of the bus network under recalculated degree-based removals is slightly lower compared to random or degree-based removals. As an example, Table 3.3 shows

that under random node removal strategy, after 10% of nodes are removed, the efficiency loss is 73.01627 % whereas under recalculated degree-based removal strategy the efficiency loss is 86.31172 %. The above analysis shows that the degradation of the efficiency of the bus network subjected to recalculated degree-based removals is only slightly more severe than that of random or degree-based node removals. Towards higher removal fractions, the three removal strategies perform almost in a similar manner. Fig. 3.13 also shows that the efficiency curve is very steep in the case of all the removal strategies, i.e. the efficiency decreases very fast initially, after which the curve becomes flat.

3.5.2.2 Results on Bus Network Accessibility

Fig. 3.14 shows the plot of accessibility under different percentages of node removals. The accessibility loss of the bus network under different removals has been listed in Table 3.4.

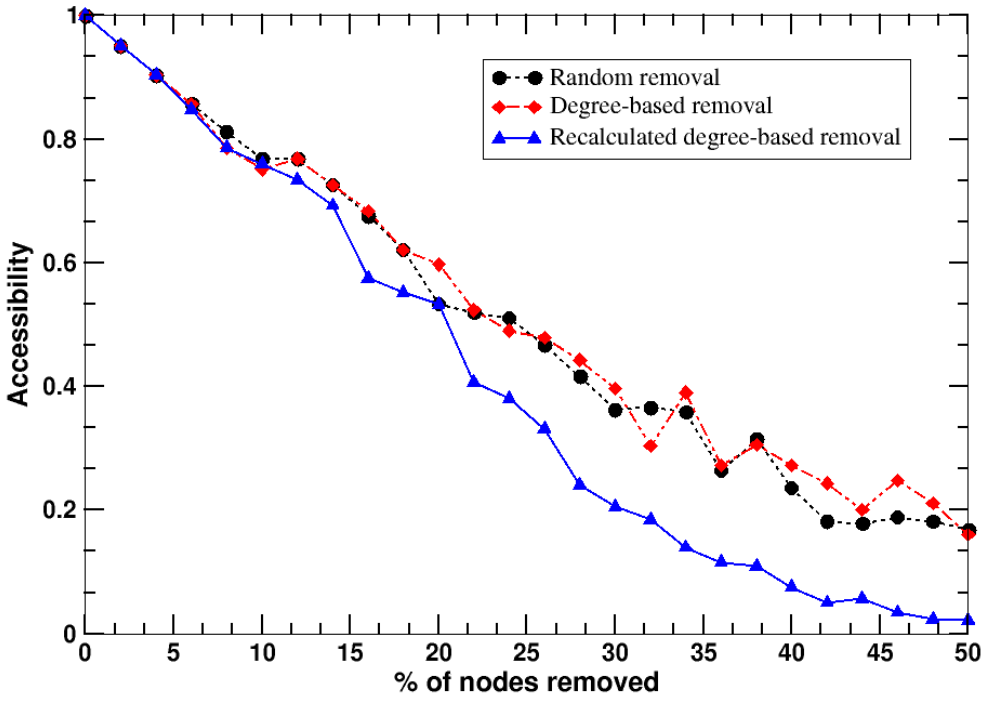

Fig. 3.14 The plot showing the accessibility degradation with different fraction of node removals in the bus network

Table 3.4 The accessibility as well as % accessibility loss under the three node removal strategies in the bus network

% of node removed	Random removal		Degree-based removal		Recalculated degree-based removal	
	Accessibility	Accessibility loss (%)	Accessibility	Accessibility loss (%)	Accessibility	Accessibility loss (%)
0	1	0	1	0	1	0
2	0.95122	4.878049	0.95122	4.878049	0.95122	4.878049
4	0.903659	9.634146	0.903659	9.634146	0.903659	9.634146
6	0.857317	14.26829	0.857317	14.26829	0.848293	15.17073
8	0.812195	18.78049	0.786098	21.39024	0.785854	21.41463
10	0.768293	23.17073	0.751463	24.85366	0.759756	24.02439
12	0.768293	23.17073	0.768293	23.17073	0.73439	26.56098
14	0.72561	27.43902	0.72561	27.43902	0.692927	30.70732
16	0.676098	32.39024	0.684146	31.58537	0.574878	42.5122
18	0.620732	37.92683	0.620732	37.92683	0.552683	44.73171
20	0.532927	46.70732	0.597317	40.26829	0.532982	46.7018
22	0.519512	48.04878	0.523902	47.60976	0.407317	59.26829
24	0.510488	48.95122	0.49	51.000	0.38098	61.902
26	0.467317	53.26829	0.47878	52.12195	0.330922	66.9078
28	0.416829	58.31707	0.442683	55.73171	0.240244	75.97561
30	0.362683	63.73171	0.396829	60.31707	0.205366	79.46341
32	0.366341	63.36585	0.303659	69.63415	0.184645	81.5355
34	0.358537	64.14634	0.390488	60.95122	0.139744	86.0256
36	0.263415	73.65854	0.272195	72.78049	0.11561	88.43902
38	0.314878	68.5122	0.30561	69.43902	0.10878	89.12195
40	0.235854	76.41463	0.272195	72.78049	0.075122	92.4878
42	0.181951	81.80488	0.243171	75.68293	0.050488	94.95122
44	0.178049	82.19512	0.200732	79.92683	0.05678	94.322
46	0.188537	81.14634	0.248049	75.19512	0.03465	96.535
48	0.18122	81.87805	0.210976	78.90244	0.02389	97.611
50	0.168537	83.14634	0.160732	83.92683	0.021345	97.8655

It can be seen from the Fig.3.14 that similar to the case of efficiency, accessibility decreases in a similar manner for random and degree-based node removal strategies. Accessibility under recalculated strategy is almost similar to

random or degree-based strategies for initial node removals, however when the percentage of node removals increase, accessibility under recalculated removal is lower than the other two strategies. As an example under random removal strategy, after 10% of nodes are removed, the accessibility loss is 23.17073% and for the recalculated strategy the accessibility loss is 24.02439 %. However when the percentage of removal increases to say, 40% under random removal, the accessibility loss is 76.41463% and under recalculated removal the accessibility loss is 92.4878%. However, in general, the damage on the accessibility of the bus network subjected to recalculated degree-based node removal is higher than that of random or degree-based node removals.

Figs. 3.15, 3.16 and 3.17 illustrate the topology of the bus network under the three removal strategies when 30% nodes are removed. The figures show that even at 30% node removals, the network remains as a single connected component indicating that the bus network is more robust than the rapid transit rail network.

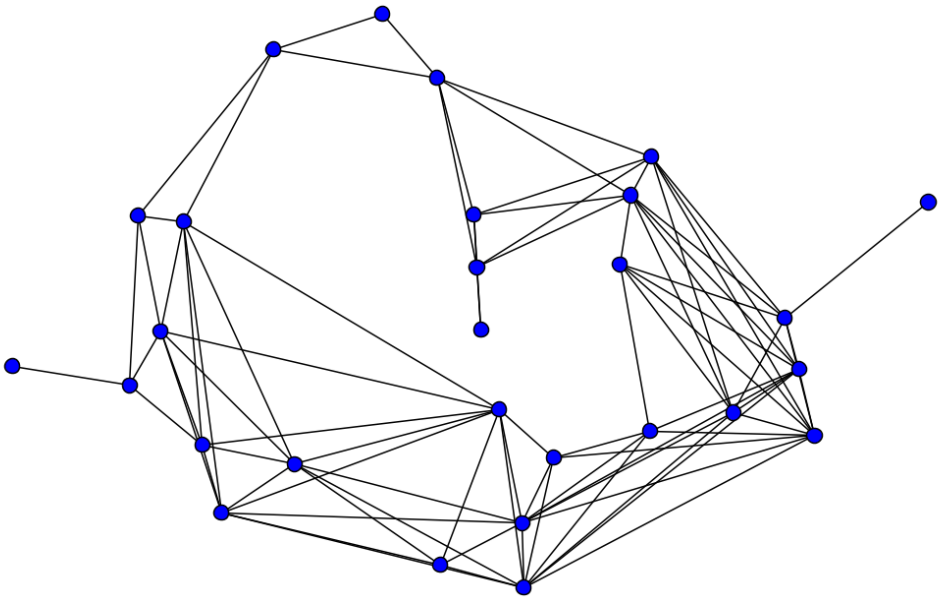

Fig. 3.15 The topology of the bus network when 30% nodes are removed randomly

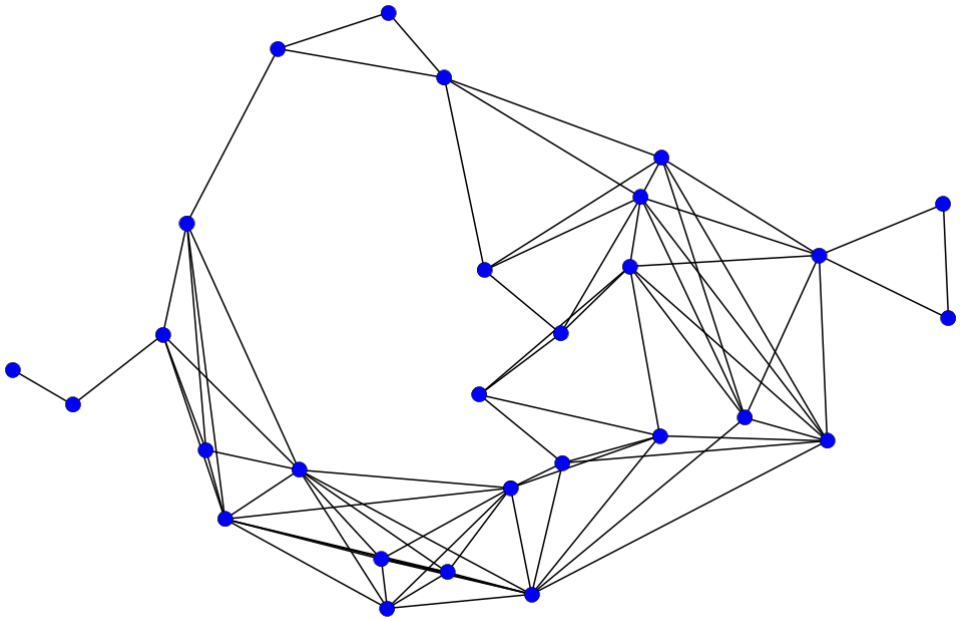

Fig. 3.16 The topology of the bus network when 30% nodes are removed based on degree

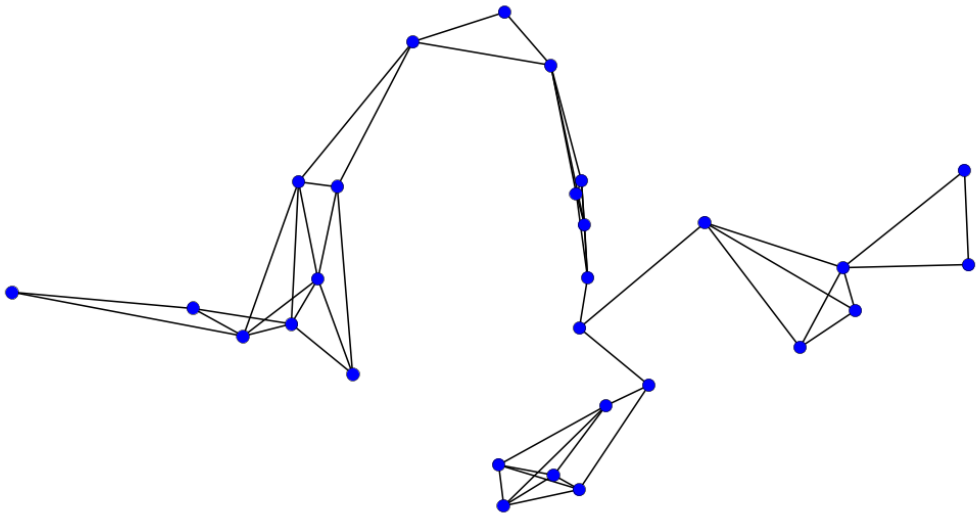

Fig. 3.17 The topology of the bus network when 30% of nodes are removed in the case of recalculated degree-based removal

3.5.3 The Analysis of the Combined Rapid Transit-Bus network

3.5.3.1 Results on Combined Network Efficiency

Fig. 3.18 shows how efficiency of the combined network decreases under different removal strategies as a function of the percentage of nodes removed. Table 3.5 shows the percentage efficiency loss of the network under different removal strategies and removal fractions. It can be seen from the figure that the efficiency decreases in a similar manner for random as well as degree-based node removal strategies. However, the efficiency under recalculated degree-based node removals is lower compared to random or degree-based removals. As an example the table shows that under random node removal strategy, after 6% of nodes are removed, the loss of efficiency is 45.94 %. Under recalculated degree-based removal strategy, the efficiency loss is 84.20% when 6% nodes are removed. Fig. 3.18 also shows that the efficiency curve is very steep in the case of recalculated removal strategy, i.e. the efficiency decreases very fast initially, after which the curve becomes flat.

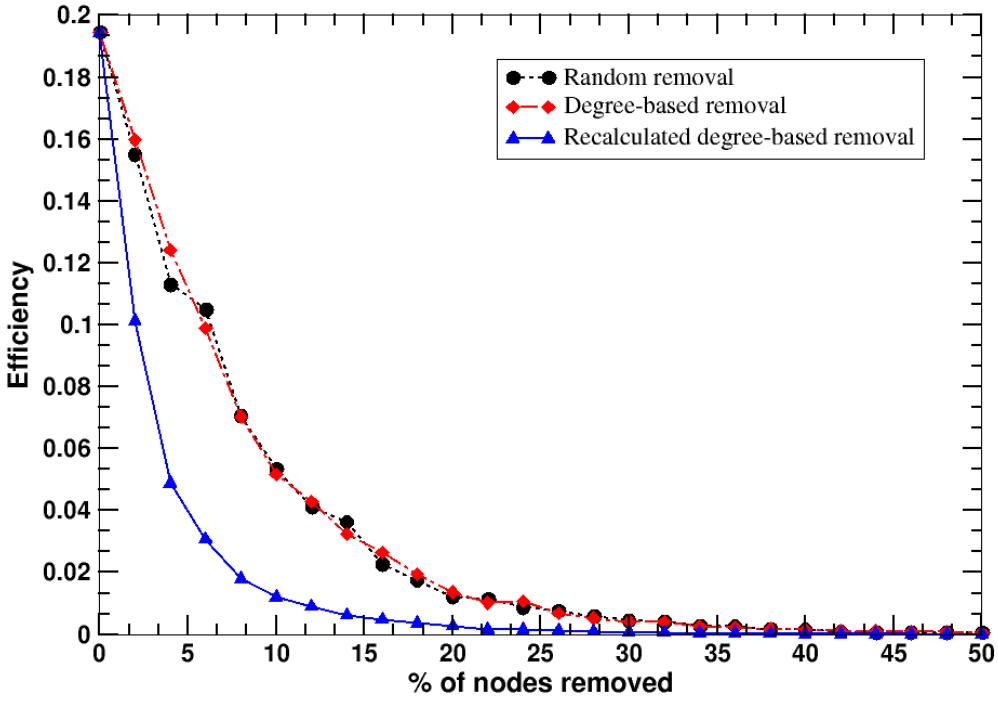

Fig. 3.18 The plot showing the efficiency degradation with different fraction of node removals in the combined network

Table 3.5 The efficiency as well as % efficiency loss under the three node removal strategies in the combined network

% of node removed	Random removal		Degree-based removal		Recalculated degree-based removal	
	Efficiency	Efficiency loss (%)	Efficiency	Efficiency loss (%)	Efficiency	Efficiency loss (%)
0	0.19452	0	0.19452	0	0.19452	0
2	0.15515	20.239382	0.159784	17.857058	0.101141	48.004668
4	0.113166	41.82310825	0.124126	36.18863751	0.048835	74.89470057
6	0.105156	45.94065013	0.098941	49.13600558	0.03073	84.2021754
8	0.070733	63.63706407	0.070335	63.84189289	0.017992	90.7506374
10	0.053408	72.54365866	0.051715	73.41429646	0.011999	93.83136553
12	0.0413	78.76825037	0.042901	77.94508206	0.009032	95.35679613
14	0.03628	81.3487268	0.032488	83.29844269	0.006231	96.79649401
16	0.022744	88.30739649	0.026412	86.42221318	0.004834	97.51496128
18	0.017402	91.05386916	0.019534	89.9576172	0.003663	98.11676236
20	0.01227	93.69203668	0.01367	92.97267599	0.002722	98.60060497
22	0.011486	94.0951447	0.010199	94.75663946	0.0015	99.22880649
24	0.008868	95.44113305	0.010755	94.47115302	0.001449	99.25527626
26	0.007578	96.10442081	0.006891	96.45722538	0.001293	99.33547097
28	0.005898	96.96795775	0.005253	97.2995266	0.000975	99.49860081
30	0.004606	97.63217522	0.004156	97.86340131	0.000697	99.64189838
32	0.00414	97.87163217	0.004003	97.94204486	0.000639	99.67153229
34	0.002877	98.52110696	0.002614	98.65633205	0.000338	99.82598579
36	0.002606	98.66039936	0.002298	98.81874657	0.000436	99.77587055
38	0.001758	99.09615226	0.001769	99.09057904	0.000269	99.86146901
40	0.001586	99.18458199	0.001455	99.25215486	0.000212	99.89121458
42	0.000979	99.49649111	0.001225	99.37032884	0.000154	99.92067066
44	0.000724	99.6275575	0.001028	99.47133851	0.000106	99.94557917
46	0.000729	99.62514345	0.000738	99.62077673	3.51E-05	99.98197114
48	0.000788	99.59475025	0.000791	99.59341189	2.87E-05	99.98526814
50	0.000579	99.70255918	0.000573	99.70542743	1.25E-05	99.99358367

3.5.3.2 Results on Combined Network Accessibility

Fig. 3.19 shows the reduction in accessibility for various removal fractions in the combined network and Table 3.6 show the accessibility loss for different removal fractions and removal strategies. The figure shows that the recalculated-degree based removal strategy results in a higher reduction in accessibility of the whole system when compared to the other two strategies. For example at 14% of node removals, the random removal of nodes results in an accessibility loss of 33.3301% whereas at the same removal fraction, the recalculated removal results in 71.37514% accessibility loss.

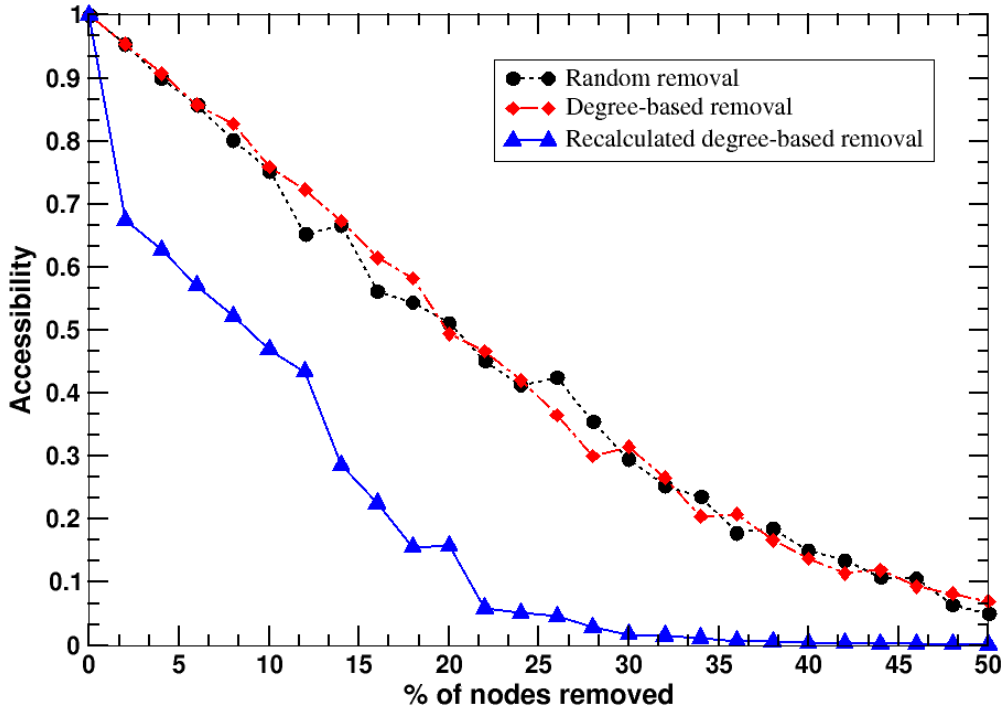

Fig. 3.19 The plot showing the reduction in accessibility with different fraction of node removals in the combined network

Table 3.6 The accessibility as well as % accessibility loss under the three node removal strategies in the combined network

%of node removed	Random removal		Degree-based removal		Recalculated degree-based removal	
	Accessibility	Accessibility loss (%)	Accessibility	Accessibility loss (%)	Accessibility	Accessibility loss (%)
0	1	0	1	0	1	0
2	0.954259	4.5741	0.954259	4.5741	0.674458	32.55419
4	0.899338	10.06618	0.907486	9.251412	0.627321	37.26793
6	0.857932	14.20679	0.857823	14.21772	0.570894	42.91057
8	0.801979	19.80208	0.827491	17.25093	0.522883	47.71174
10	0.753348	24.66517	0.75897	24.10297	0.469225	53.07753
12	0.652857	34.71435	0.722943	27.70566	0.434193	56.58066
14	0.666699	33.3301	0.67345	32.65497	0.286249	71.37514
16	0.561095	43.89047	0.615057	38.49432	0.225475	77.45249
18	0.543574	45.64264	0.581993	41.80074	0.155898	84.41018
20	0.511651	48.83492	0.494141	50.58588	0.158375	84.16247
22	0.451351	54.86491	0.466517	53.34831	0.058989	94.10115
24	0.412507	58.74932	0.420557	57.94427	0.051569	94.84306
26	0.424455	57.55449	0.365406	63.45941	0.045838	95.41619
28	0.354453	64.55467	0.300322	69.96782	0.029118	97.08822
30	0.295817	70.41831	0.315172	68.48279	0.017291	98.2709
32	0.253658	74.63421	0.266177	73.38231	0.015397	98.46032
34	0.235651	76.43495	0.204748	79.52523	0.011851	98.81489
36	0.178836	82.11645	0.20833	79.16702	0.006715	99.32852
38	0.185478	81.45225	0.166924	83.30763	0.005573	99.44266
40	0.150301	84.96995	0.137539	86.24613	0.004031	99.59687
42	0.135134	86.48655	0.114261	88.57386	0.003278	99.67215
44	0.107474	89.25263	0.119398	88.06023	0.002817	99.71829
46	0.106344	89.36555	0.093012	90.6988	0.002307	99.76929
48	0.064356	93.56445	0.081987	91.80135	0.001469	99.85308
50	0.049979	95.00212	0.069893	93.01075	0.00119	99.881

Figs. 3.20, 3.21 and 3.22 give an illustration of fragmentation of the combined network when 30% nodes are removed based on random, degree-based and recalculated degree-based removal strategies.

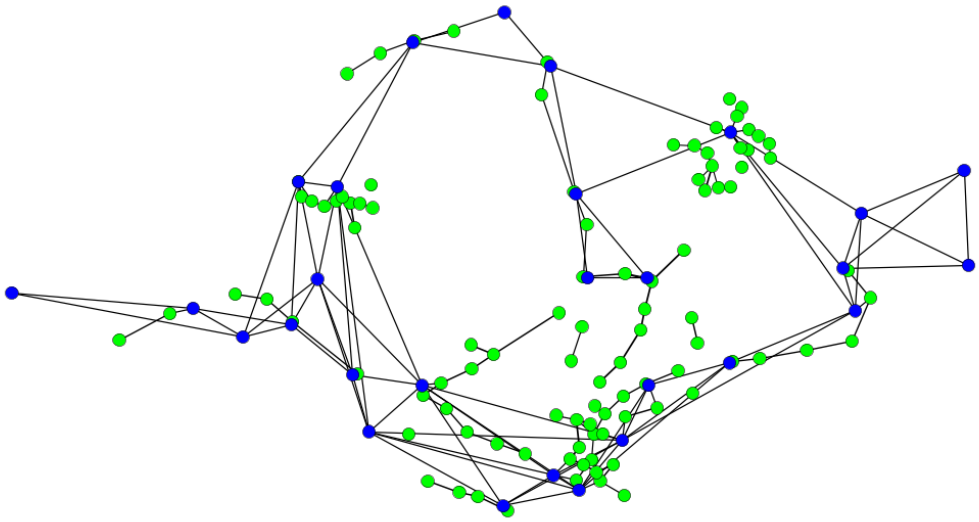

Fig. 3.20 The network fragmentation of the combined network when 30% of nodes are removed randomly.

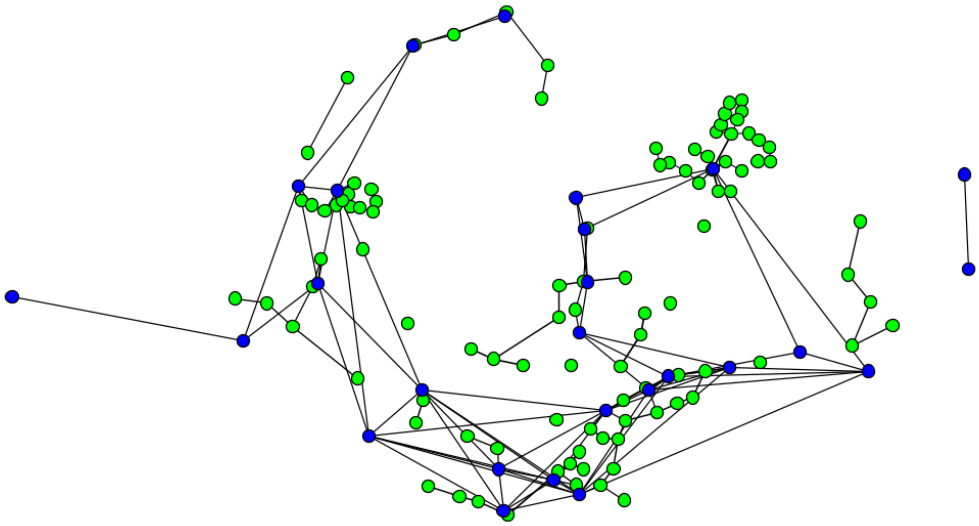

Fig. 3.21 The network fragmentation of the combined network when 30% of nodes are removed based on degree.

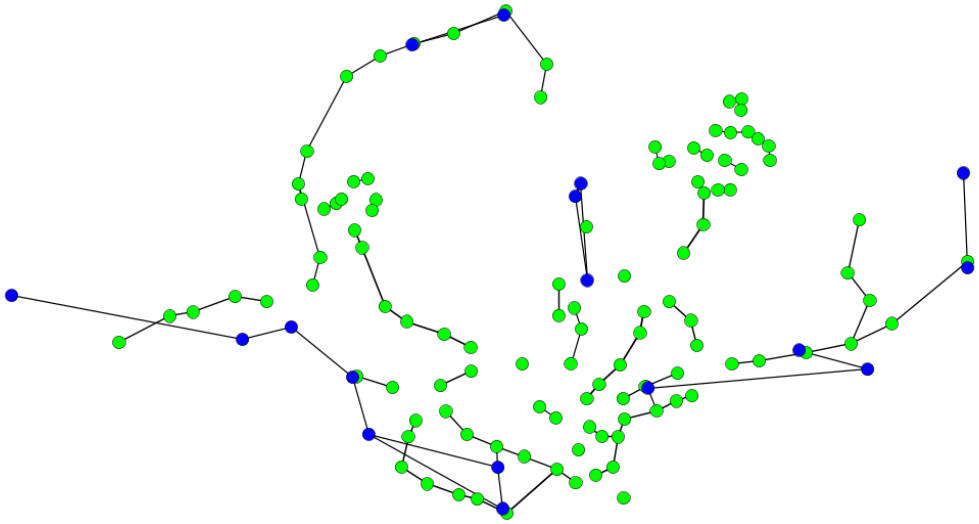

Fig. 3.22 The network fragmentation of the combined network when 30% of nodes are removed based on recalculated degree.

Figs. 3.20, 3.21 and 3.22 show that recalculated strategy results in more fragments than the random or degree-based removal. Furthermore, the figures also show that for recalculated removal more nodes are removed from the bus network than the transit network. It may be because the nodes in the bus network have higher degree compared to the nodes in the rail network.

3.5.4 Comparison of rapid transit, bus and combined networks

In general, the studied networks show the behaviour of a random network since the networks behave in a similar manner to random as well as degree-based node removals. However, recalculated node removal strategies are more effective in reducing the efficiency and accessibility than non-recalculated removal strategies in all the three networks. This may be because the importance of a node may change significantly after one or multiple node removals. For instance, a transit station which was not important in an urban transit network could become important after one or more stations are closed. In the studied model, once nodes are removed, the other nodes which were previously trivial due to low degrees now become the nodes with highest degrees. Therefore recalculated node removal strategies are more effective in diminishing the efficiency and accessibility values than the other node removal strategies because the recalculated strategies select nodes with the largest degree at each step.

3.5.4.1 Comparison of efficiency loss of the three networks

Fig. 3.23 shows the percentage efficiency loss of the three studied networks at different percentages of node removals under the random node removal strategy. The figure shows that the three networks perform in an almost similar manner, i.e. the interdependency of rapid transit network to the bus network does not result in an increase in the efficiency loss in the combined rapid transit-bus network when the nodes are removed randomly.

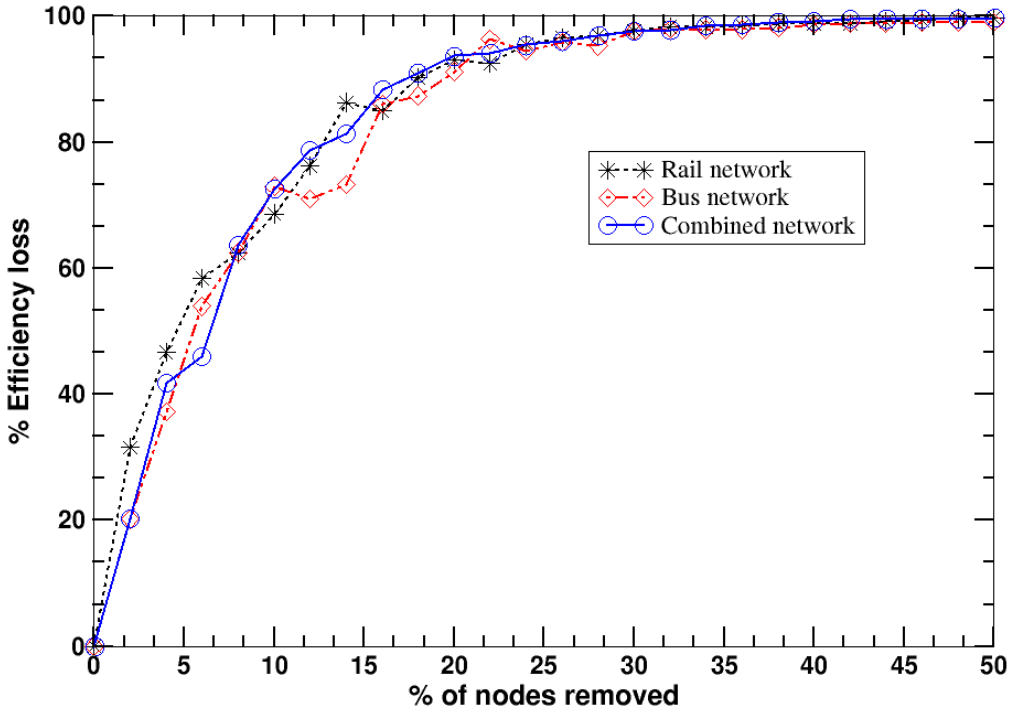

Fig. 3.23 A plot showing the efficiency loss of the three networks when different percentages of nodes are removed randomly

Fig. 3.24 shows the percentage efficiency loss of the three studied networks at different percentages of node removals under the degree-based node removal strategy. The figure shows that similar to the random removal strategy, the three networks perform in an almost similar manner. This means that the interdependency of rapid transit network to the bus network does not result in an increase in the efficiency loss in the combined rapid transit-bus network when the nodes are removed based on degree.

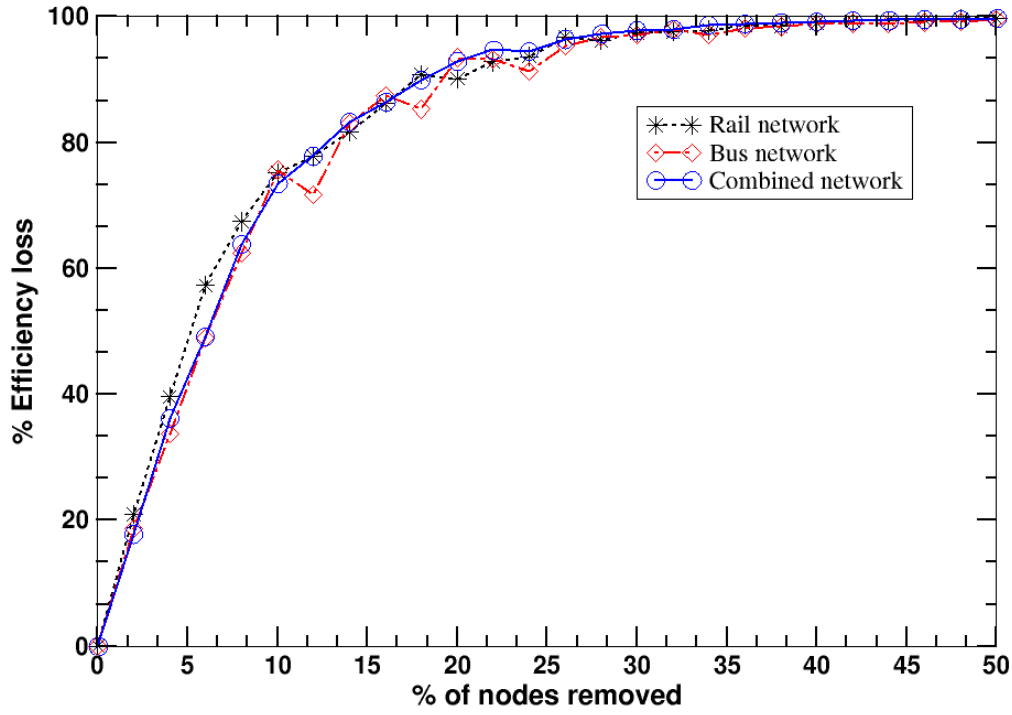

Fig. 3.24 A plot showing the efficiency loss of the three networks when different percentages of nodes are removed based on degree

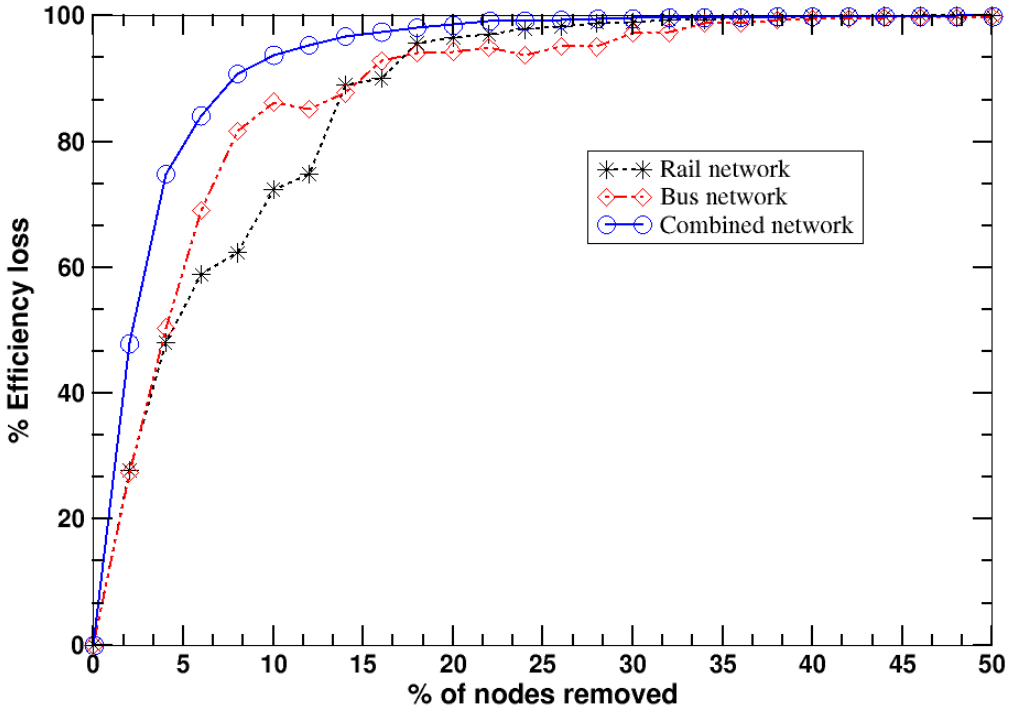

Fig. 3.25 A plot that shows the efficiency loss of the three networks when different percentages of nodes are removed based on recalculated degree

Fig. 3.25 illustrates the percentage efficiency loss of the three studied networks at different percentages of node removals under the recalculated node removal strategy. The figure shows that there is an increased efficiency loss in the combined rapid transit-bus network when compared to the independent rapid transit and bus networks. This shows that the presence of interdependent links between the two independent networks make the combined network more vulnerable under recalculated removals, resulting in an increased efficiency loss.

3.5.4.2 Comparison of accessibility loss of the three networks

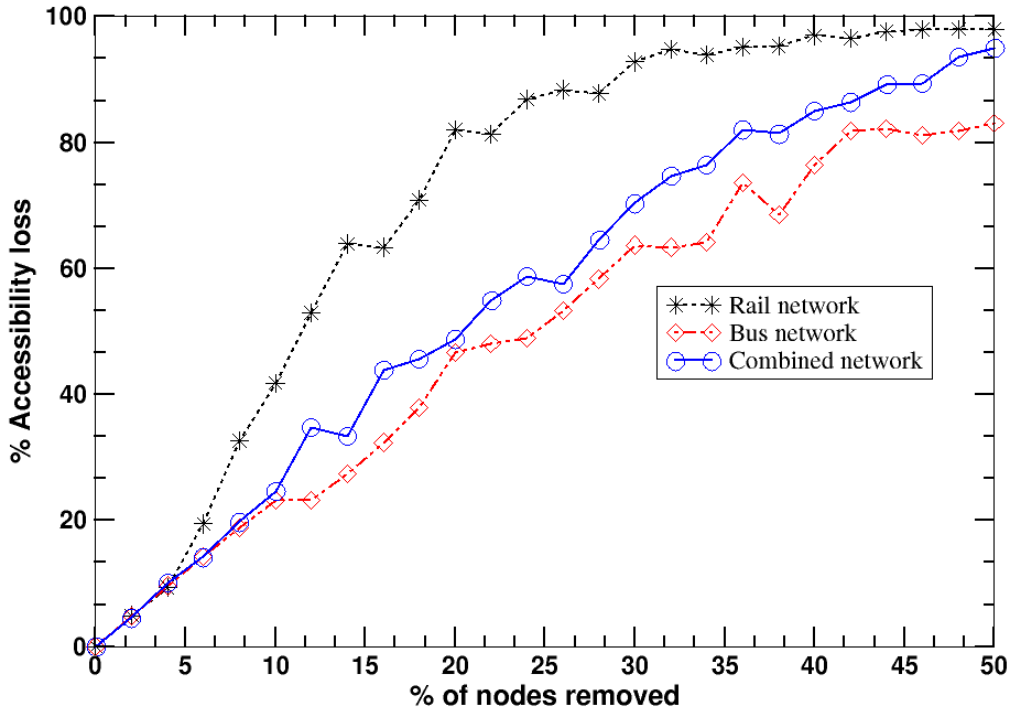

Fig. 3.26 A plot showing the accessibility loss of the three networks when different percentages of nodes are removed randomly

A plot showing the accessibility loss of the three networks when different percentages of nodes are removed randomly is illustrated in Fig. 3.26. The accessibility loss of the combined network is more when compared to the bus network, but less when compared to the rapid transit network. This shows that the presence of interdependency links can result in an improved operation but at the same time can also make the network more vulnerable. To make it more clear, for the bus network, when an interdependent layer of rapid transit network

is added, the accessibility loss in the whole combined rapid transit-bus network increased when compared to the accessibility loss in the independent bus network. However for the rapid transit network when an interdependent layer of bus network is added, the whole combined rapid transit-bus network performance improved, i.e. the accessibility loss decreased when compared to the independent rapid transit network.

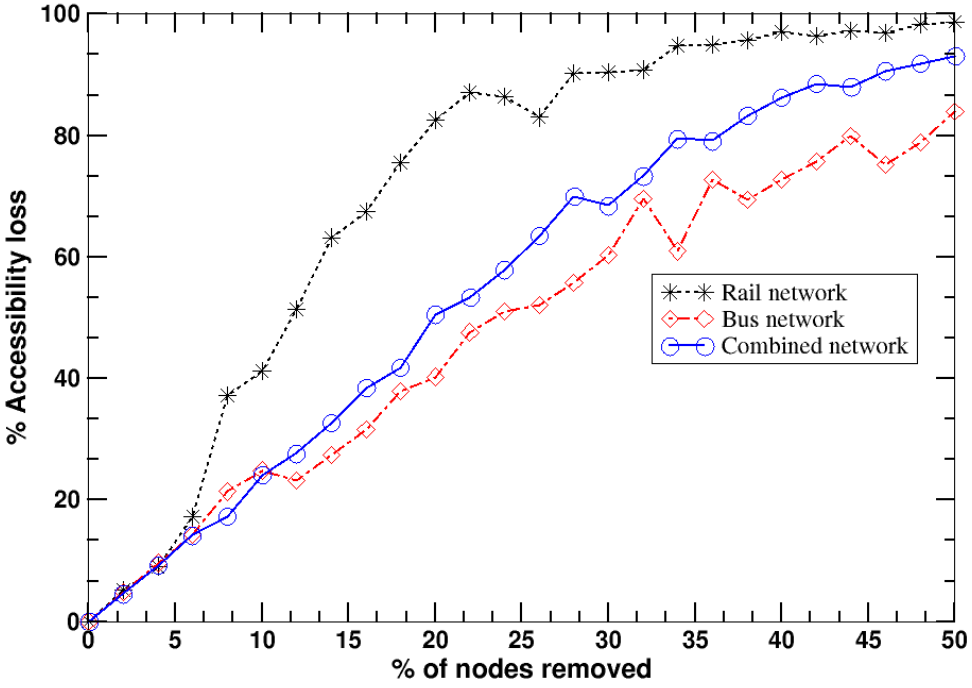

Fig. 3.27 A plot showing the accessibility loss of the three networks when different percentages of nodes are removed based on degree

A plot showing the accessibility loss of the three networks when different percentages of nodes are removed based on degree is illustrated in Fig. 3.27. Similar to random removal, the accessibility loss of the combined network is more when compared to the bus network, but less when compared to the rapid transit network. When an interdependent layer of rapid transit network is added to the bus network, the accessibility loss in the whole combined rapid transit-bus network increased when compared to the accessibility loss in the independent bus network. For the rapid transit network when an interdependent layer of bus network is added, the whole combined rapid transit-bus network performance

improved, i.e. the accessibility loss decreased when compared to the independent rapid transit network.

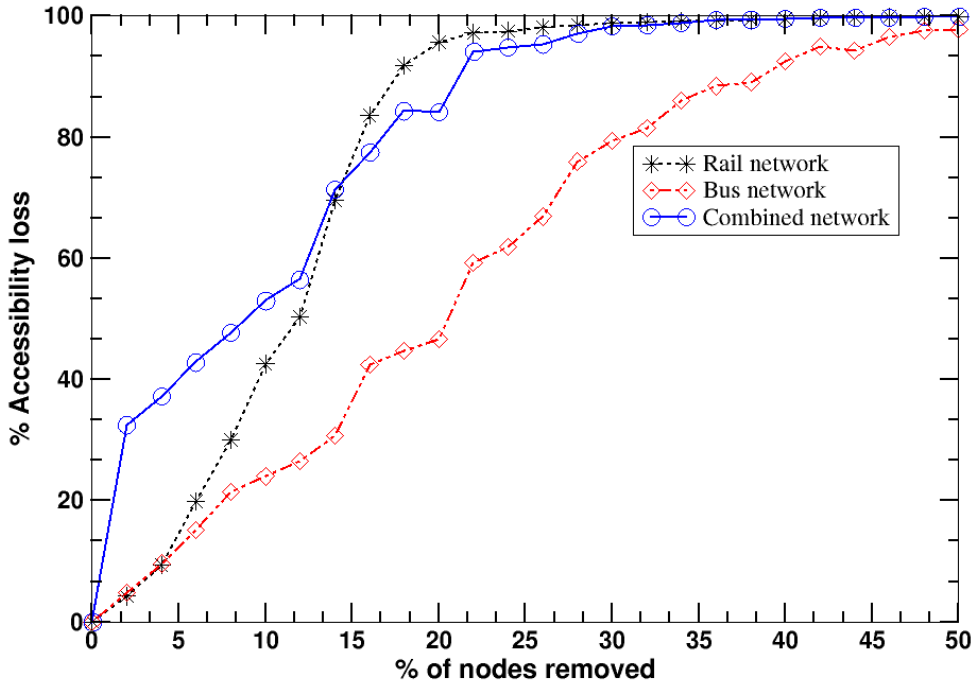

Fig. 3.28 A plot showing the accessibility loss of the three networks when different percentages of nodes are removed based on recalculated degree.

Yet another plot that shows the accessibility loss under recalculated removals is shown in Fig. 3.28. The plot shows that the accessibility loss of the combined rapid transit-bus network is more compared to the independent bus network. The plot also shows that for lower removal fractions in the recalculated strategy, the accessibility loss of the combined network is more compared to the independent rapid transit network and for higher removal fractions, the accessibility loss is less.

3.6 Summary

This chapter mainly discusses on the investigation of vulnerability/failure consequence in a critical infrastructure network resulting from three different node removal strategies using a proximity-based failure cascading model. The investigation was applied to study the behaviour of three transportation

networks: a rapid transit rail network, a bus network and a combined rapid transit-bus network. The study mainly shows that recalculated removal strategies result in more failure consequences in the studied networks when compared to the other two removal strategies. The study also shows that the presence of interdependencies can have both positive as well as negative consequences. On one hand interdependencies can improve the operation (e.g. accessibility) of the combined rapid transit-bus network; on the other hand, the interdependencies can make the combined network more vulnerable leading to larger network performance degradation or larger failure consequences (e.g. efficiency). However, those interdependencies that make the system more vulnerable, i.e. the ones that increase the failure consequences in the combined network are of great concern and should be further studied.

CHAPTER 4: ANTICIPATING EXTREME RISKS IN INFRASTRUCTURE NETWORKS BY EVOLUTIONARY OPTIMIZATION

Although a variety of models and methods have been developed by various researchers to model and analyze infrastructure networks and their interdependencies, most of them are based on the assumption that the infrastructure interdependencies model has been constructed to a fair degree of completeness. As an example, in the previous chapter the interdependencies between networks were constructed based on geographic proximities between the two networks and the network model was assumed to be complete. However, some of the interdependencies that exist among infrastructures may be unforeseen due to the presence of complex feedback paths, frequent upgradation of infrastructures and so on and they may be revealed only after the occurrence of some disaster or disruption. Some of these unknown or unforeseen interdependencies may not be critical because they may not result in any additional disruption effects. However, some of the unforeseen interdependencies may be crucial because they may result in the cascading failure of many other components resulting in larger disruption effects and they have to be unraveled. Since the network models are incomplete, it is futile to perform the required analyzes on them since they may underestimate the disruption effects of extreme events. Hence, instead of analyzing a given infrastructure network to determine the disruption effects of any failure, the network that will result in the most extreme disruption due to some failure is synthesized in order to anticipate extreme risk events. This can be accomplished by identifying the set of critical infrastructure components to be modeled and their basic interdependencies, and then applying optimization methods to modify the network iteratively with unforeseen interdependencies (additional links) and failure points (nodes) until the disruption effects are maximized. The disruption effect is measured using risk which is a function of the probability of failure events as well as consequence. Since risk has two components the optimization problem is multiobjective, the objectives being maximization of failure

probability and maximization of failure consequence. However, in reality, the failure events that have high frequencies of occurrence may not result in extremely high consequences, while the ones that occur very rarely like a 100-year flood event may result in disastrous consequences. Since the two objectives of probability and consequence are often conflicting in nature, the multiobjective optimization procedure would generate a set of trade-off solutions rather than a single optimal solution. The decision variables of the optimization procedure would be the unforeseen interdependencies as well as failure points (node failures) within the network. Towards the end of optimization, the multiobjective optimization procedure would generate a set of solutions (networks with corresponding failure points) converging towards Pareto-optimality. Of all the solutions, the ones with maximum failure consequences can be examined to determine the unforeseen interdependencies as well as failure points (node failures) that may lead to the realization of extreme risk events.

4.1 The steps involved in extreme risk identification

4.1.1 Identification of the relevant infrastructure components and interdependencies

The key building blocks of the network model would be the infrastructure nodes and the known interdependencies or relationships which are represented by links. Firstly, all the relevant components/nodes of various infrastructure sectors and their characteristics have to be identified. Secondly, the different types of known interdependencies (physical, cyber, geographic, policy and societal) among the components of various sectors have to be established. Concepts from agent-based modeling are used to construct the network. Agent-based models are well suited for studying cascading behaviors in infrastructure networks. Agents can be anything from simple software entities without much intelligence to smart agents with intelligence. In the current work, agents are simple software agents that are used to represent nodes with their characteristics and the interactions between the agents are represented as links. The construction of network model has been illustrated in Fig. 4.1.

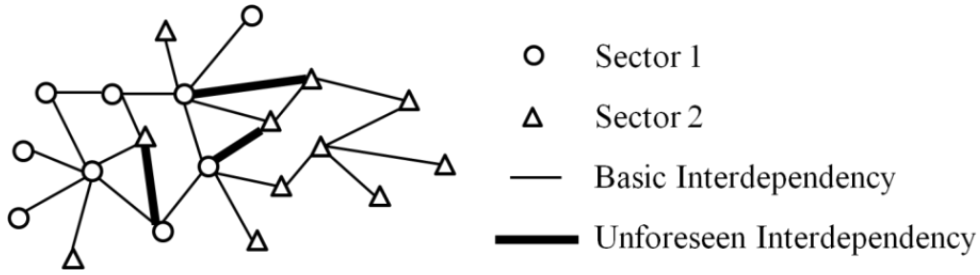

Fig. 4.1 Building the network of infrastructure interdependencies

4.1.2 Analysis of Network Disruptions

In this report, the failure events studied include only node failures. The infrastructure network will be analyzed based on risk which is considered to be a function of failure probability and failure consequence as shown in equation (4.1).

$$Risk = function\,(probability, consequence) \tag{4.1}$$

In order to analyze network risk, probabilities of node failures as well as consequences have to be calculated. A methodology to calculate the node failure probabilities is yet to be investigated and therefore for the purpose of case study, probabilities are randomly assigned. The consequence of failure will be quantified using a suitable measure from network theory. In this work, failure consequence has been quantified by measuring the giant component size of the network after node failures. When a node fails, the failure cascades through the network and additional nodes may fail due to overloading and the network may disintegrate into several components. According to Percolation theory, the functional nodes would be the one in the largest/giant component and the other nodes will be non-functional [98]. Therefore, the size (number of nodes) of the giant component formed or the giant component size $|G_c|$ is used as an indicator of network failure consequence. Since smaller giant component sizes are indicators of catastrophic failures, giant component size has to be minimized to obtain the maximum failure consequence.

4.1.3 Optimization of network models

The proposed methodology for anticipating extreme risk involves using an optimization algorithm to synthesize infrastructure networks for maximum risk. The objectives of the optimization procedure include maximization of failure probability and minimization of giant component size (since the smaller the giant component size, the worse the consequence). The decision variables include unforeseen interdependencies as well as node failures. The optimal solutions (the resulting networks) are then analyzed to find the unforeseen interdependencies and node failures that can lead to extreme risk.

4.1.3.1 Formulation of the optimization problem

Before formulating the optimization problem, there is a need to provide a formal definition of unforeseen interdependency. An unforeseen interdependency can be defined as follows:

Definition 4.1

An unforeseen interdependency in a critical infrastructure network can be considered to be an interdependency/link that is not a part of the defined or known set of interdependencies/links E.

The proposed optimization problem can now be stated as follows:

Given a set of nodes V, a set of known interdependencies E and a set of unforeseen interdependencies U, construct a set of networks $G(V, E, U)$ that maximizes risk due to some failure.

Let x_1 and x_2 represent two unforeseen interdependencies and x_3 represent a node to be failed. The consequence C of network failure is measured by calculating the giant component size $|G_c|$ of the network that arises when x_1 and x_2 are added to the network and x_3 is made to fail. The probability P of failure is a property of the node to be failed x_3. The problem can be formulated as follows:

Minimize $C(x_1,\ x_2,\ x_3\ ) = |G_c|$

Maximize $P(x_3)$

Decision variables: $x_1 \in U,\ x_2 \in U, x_3 \in V$

4.1.3.2 The optimization process using genetic algorithms

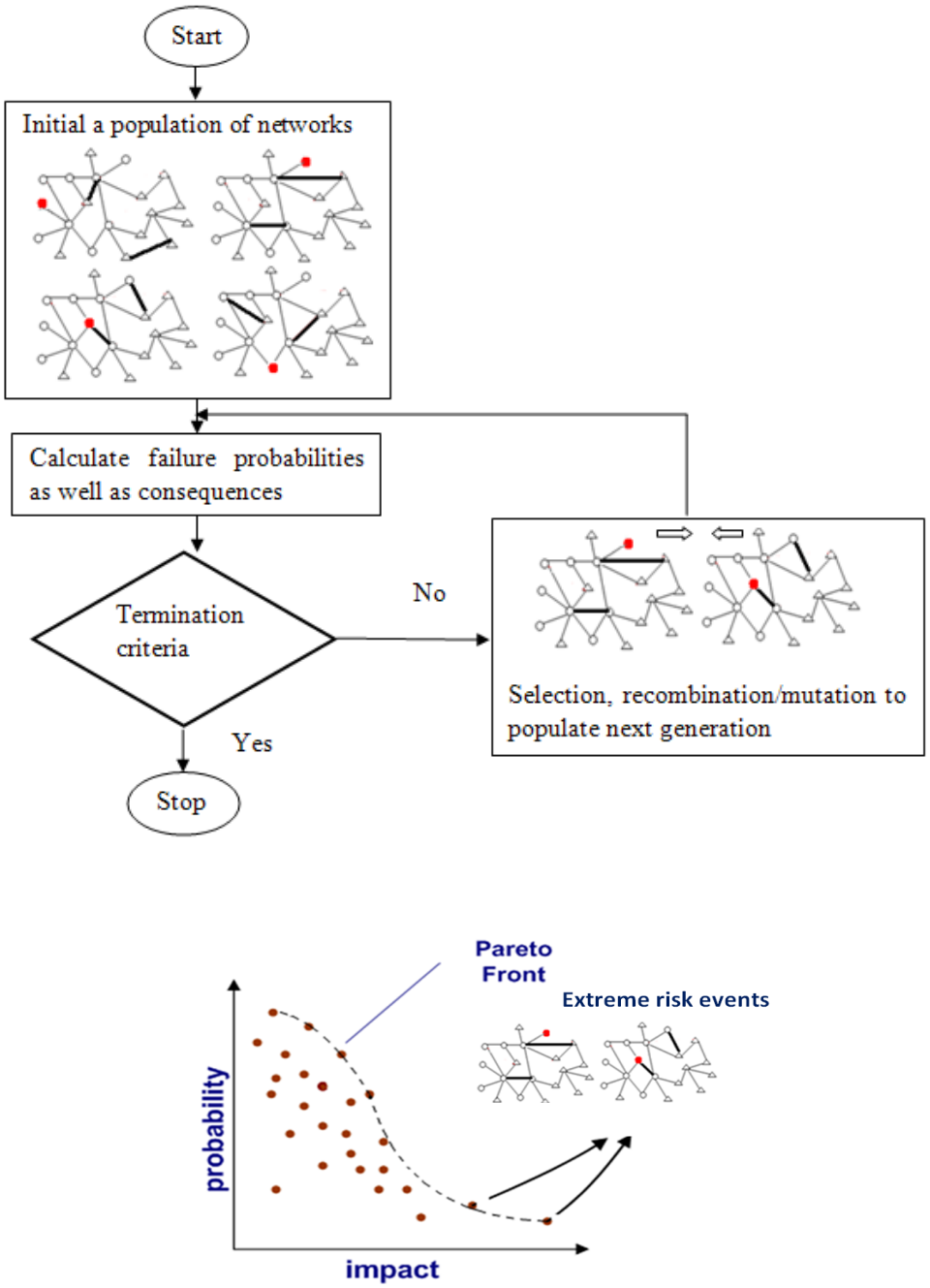

Fig. 4.2 A plot of Pareto optimal solutions obtained from evolutionary optimization, with network solutions of extreme disruption representing extreme risk events.

The multiobjective nature of the optimization problem together with the discrete nature of the problem explains the suitability of evolutionary optimization algorithms like genetic algorithms for performing the optimization. Genetic

algorithm (GA) is a heuristic algorithm based on the theory of evolution by Darwin [99, 100]. In genetic algorithms, the solutions or individuals are characterized by their chromosomes which are usually represented in binary form as strings of 0's and 1's, but other encodings like integer are also possible. The chromosomes represent the decision variables (unforeseen interdependencies and node failures) of optimization. The objective/fitness functions are maximization of failure probability and minimization of giant component size. The whole optimization process using GA is illustrated in Fig. 4.2. In the figure, the nodes in red represent the ones to be failed and the lines in bold represent unforeseen interdependencies. The details of GA (both simple and multiobjective) are provided in the subsequent sections.

(a) The working of a simple genetic algorithm

In a simple genetic algorithm, a population of individuals (network models) is initially generated in a random manner and the algorithm continues for generations. There is only one objective to be optimized in a simple genetic algorithm and therefore the fitness of each individual is calculated as the value of the objective/fitness function for that individual. In each generation, every individual's fitness is calculated and several individuals will be selected based on their objective/fitness values which then crossover and get mutated to generate next generation individuals. The termination criteria is usually the number of generations or the fitness level of individuals [99, 100]. The three basic operators in a genetic algorithm: selection, mutation and crossover are explained below.

Selection

In the theory of evolution, only the best individuals (with respect to fitness values) survive and generate new offspring individuals. There are many methods for selecting the best individuals like roulette wheel selection, tournament selection, rank selection, etc.

Crossover

In crossover, two individuals are combined or mated to generate offspring individuals. The offspring individuals may take the best characteristics from

parents and produce individuals better than their parents. Crossover occurs based on a user-defined crossover probability.

Mutation

In mutation, one or more genes in the chromosome of an individual are modified and these new genes may drive GA to reach the optimal solutions. Mutation is very important since it prevents GA from reaching local optimal solutions. Mutation occurs based on a user-defined mutation probability.

(b) Multiobjective genetic algorithms

Most of the real world problems have multiple objectives. There are generally two ways to solve a multiobjective optimization problem. In one of the ways, the individual objective/fitness functions are combined to form a weighted objective function in which the selection of weights is often an issue. In the second way, a set of Pareto optimal or trade-off solutions are determined. A Pareto optimal set is a set of solutions that are nondominated with respect to each other. A solution x_1 in a multiobjective optimization problem is said to dominate another solution x_2 if both of the following conditions are satisfied:

a. The solution x_1 is no worse than x_2 in all the objectives.

b. The solution x_1 is strictly better than x_2 in at least one objective.

Pareto optimal sets have the advantage that the obtained solution is always a trade-off [101]. In this research, a multiobjective optimization algorithm called Nondominated Sorting Genetic Algorithm II [100] will be used for optimizing the two objectives of probability and consequence of failures.

The Nondominated Sorting Genetic Algorithm II (NSGA II) algorithm

In NSGA II, a population of individuals of size N is randomly generated at the beginning. This forms the initial parent population which is then sorted based on nondomination concept into different fronts or levels. The first front includes the individuals in the entire population that are nondominated with respect to each other, but dominates all other individuals in the population. The second front/level includes all the individuals that are dominated only by the individuals

in the first front and the sorting is continued until every individual in the population belongs to their respective front. The individuals in the population are assigned a rank based on the front they belong to. An offspring population of size N is then generated from the parent population by applying genetic operators (selection, crossover and mutation). The selection process is based on the assigned rank. Thus, the first phase of NSGA II, i.e. generating the initial parent population as well as the initial offspring population is completed.

After this phase, the NSGA II algorithm works a bit differently. The initial parent and offspring populations are combined to generate a merged population. The parent population of the next generation is formed by selecting the best N individuals from the merged population, based on nondomination criteria. In addition to rank, crowding distance is calculated for every individual. Crowding distance shows the closeness of an individual to its neighbor individuals. If the mean crowding distance of a population is high, the diversity of the population is better. The offspring individuals of this generation are then produced by applying genetic operators to the newly formed parent population. The selection is now based on rank as well as crowding distance. Among individuals with the same rank, the ones in the less crowded region are considered better. The new parent and offspring populations are combined to produce the new merged population and the process is repeated until the number of generations reaches a predefined value.

A number of overlapping solutions may exist when NSGA II is applied for combinatorial optimization. Two strategies to remove overlapping individuals have been explained by Nojima et al. [102]. The removal strategies works in such a manner that no two individuals with either the same objective values/decision variables exist in each generation. The random generation process to produce the initial set of parent individuals has been repeated several times until N individuals differing in either objective values/decision variables are generated. The generation mechanism of the offspring population is not modified. However, once the merged population has been formed, the individuals with the same objective values/decision variables are removed except for a single remaining individual. The individuals after the merging process are

evaluated in a similar way as that of NSGA II to select the *N* best individuals from the merged population.

4.2 The network used for modeling

Fig. 4.3 shows an illustration of the infrastructure network used for case studies which is adapted from Lam et al. [103].

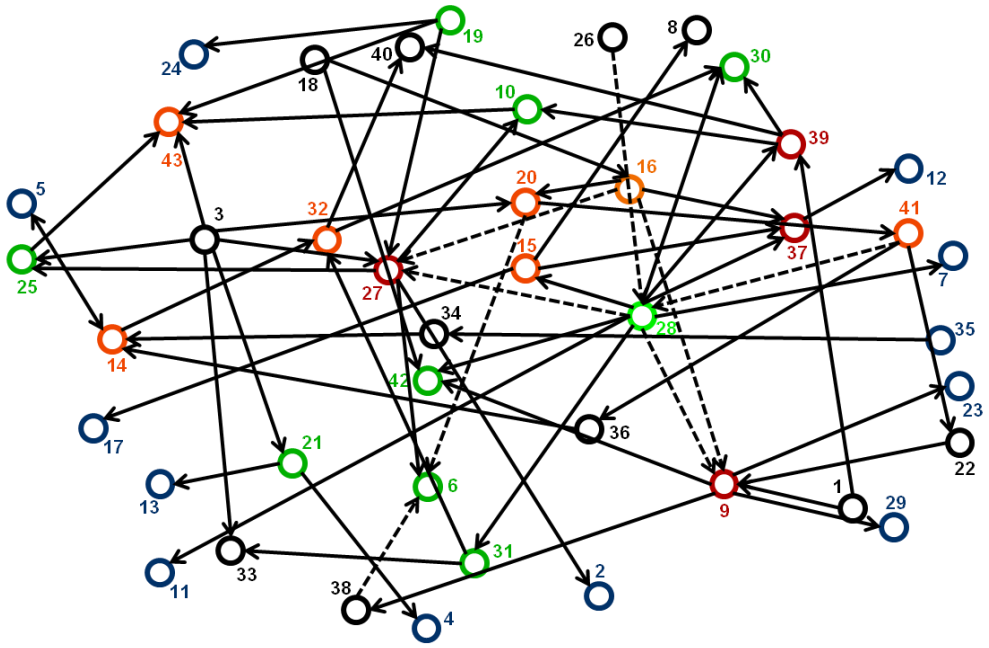

Fig. 4.3 The infrastructure network used for case studies.

In the figure, the nodes are represented as circles and labelled with their respective numbers. The solid and dashed lines respectively represent primary and secondary interdependencies. The components of various infrastructure sectors are represented as nodes and the interdependencies between them are represented as directed links. There are a total of 43 nodes and 64 links (56 primary and 8 secondary interdependencies). Some general properties of nodes and links are identified for modelling. The characteristics identified for the nodes include buffer and recovery. Links are also identified to be of any of the two types: primary or secondary.

4.2.1 Node characteristics

(a) Buffer

Infrastructure networks like oil and gas, food supply, etc. exhibit buffering properties since excess resources may be stored at their nodes (fuel filling

stations, food storages, etc.) thereby allowing their continued operation even during failures when resources have become unavailable. The availability of buffer at a node allows it to remain operational even after the resources from all other infrastructure nodes get depleted. Buffering time refers to the time period for which the node is able to continue its operation without support/input from other nodes.

(b) Recovery

The recovery capacity of a node enables it to restore its operation within an appropriate time period and recovery time refers to the corresponding time period.

4.2.2 Interdependency characteristics

(a) Primary Interdependencies

They constitute the various interdependencies/reliance between nodes of various infrastructures like the supply of materials, geographic proximities, etc.

(b) Secondary Interdependencies (Redundancies)

They come into action only when all the inputs to a node are unavailable and all the buffer has been used up. When these interdependencies come into operation, the node becomes functional and hence they act as redundancies to the node.

These two types of interdependencies, i.e. primary and secondary form the basic interdependencies or the known set of interdependencies.

4.3 The simulation framework

4.3.1 Building the network model

Fig. 4.4 shows the infrastructure network used for study created using the NetLogo platform [97]. In the figure, the nodes are laid out as a circle for clarity; primary and secondary links are shown in black and blue color respectively. In NetLogo, each node is represented as an agent. The information regarding primary and secondary link connections between the nodes/agents is provided to the NetLogo program using external text files (see Appendix B). The buffering and recovery times as well as failure probabilities of nodes are randomly

assigned to the different nodes in this study since they are mainly for illustration purposes (see Appendix B for their values inputted). These values are also stored in external text files which are then read by the program as input files. Since buffer and recovery are incorporated as time delays, a time factor has to be taken into consideration during modeling. In Netlogo, time can be modeled using a function called "tick". The concept of tick is very generic and it can represent a second, an hour or a day, depending on the application.

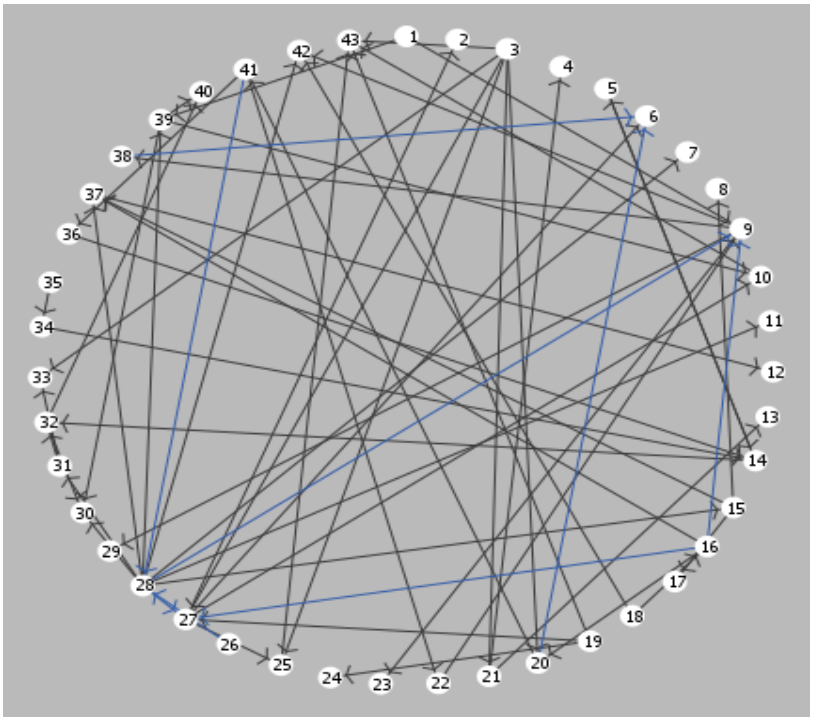

Fig. 4.4 The model built using NetLogo.

4.3.2 Implementing node failures in NetLogo

Node failures can result from different factors like random errors, intentional attacks, natural hazards, etc. When a node is made to fail, it is assumed that it is completely destroyed. There may be many nodes that depend on the failed node for resources or input and these nodes will be affected. These dependent/affected nodes however will not fail instantly since they exhibit buffering and recovery properties and also may have secondary interdependencies. Those dependent nodes that have buffer would start using their buffers and when the entire buffer is used up, the existence of secondary interdependencies will be looked for. If these dependent nodes have secondary interdependencies, they would become in normal operating state and if not, the affected or dependent nodes will be

checked for recovery. Those dependent/affected nodes with recovery property can restore their operation and the ones without recovery property would fail. When an additional node fails, checks for buffers, secondary interdependencies and recovery will be continued until all the infrastructure nodes enter their steady states, i.e. normal or failed condition. The entire cascading process has been illustrated in Fig. 4.5. After all nodes have reached their steady states, the consequences of failure can be quantified by measuring the size or the number of nodes in the largest connected component or the giant component of the network. The giant component size can be calculated using Depth First Search algorithm from network theory [104]. Another component of risk, i.e. the failure probabilities are already randomly assigned to the nodes.

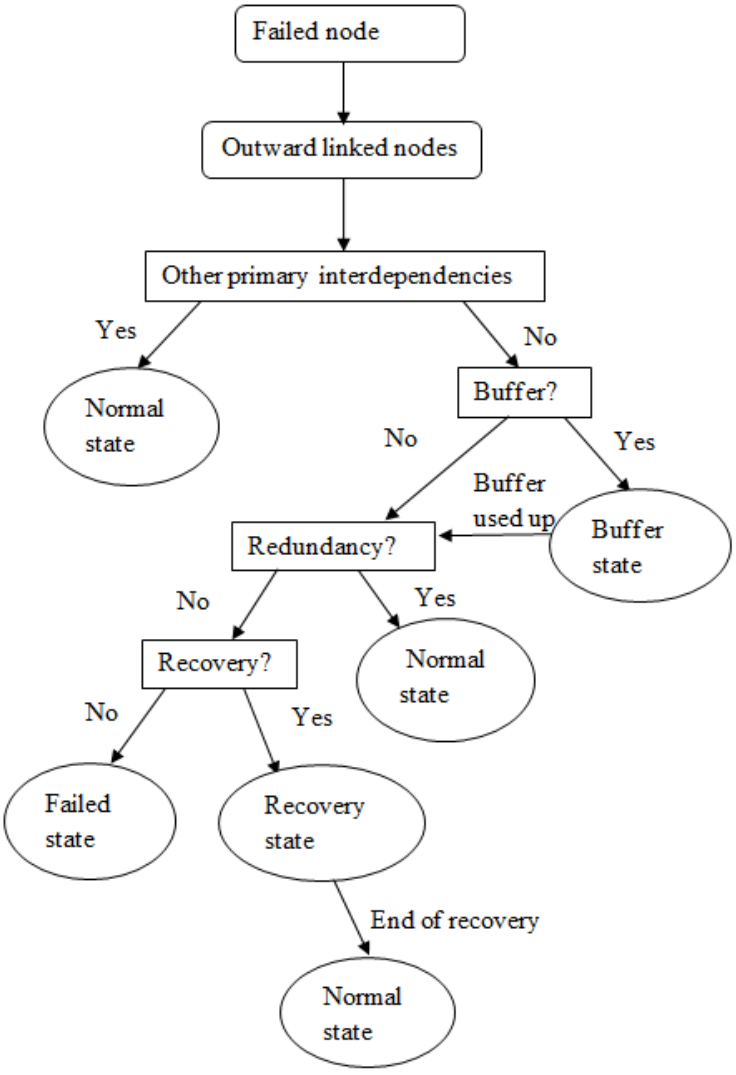

Fig. 4.5 Algorithm illustrating node failure and failure propagation in an infrastructure network

4.3.3 Implementing the genetic algorithm for optimization

4.3.3.1 Single objective optimization: minimization of giant component size

In order to investigate whether unforeseen interdependencies can cause an exacerbation of disruption consequence, i.e. a reduction in the giant component size, different single objective optimization experiments were performed using a simple genetic algorithm. For all the experiments, the objective/fitness function is minimizing of giant component size, but there is a variation in the number of decision variables depending on the number of unforeseen interdependencies added to the network model. The parameter settings of the genetic algorithm (GA) experiments are listed in Table 4.1.

Table 4.1 Parameter settings of single objective optimization experiments

Index	Parameter	Setting
1	Population size	50
2	Number of generations	50
3	Crossover rate	0.10 – 1.00
4	Mutation Rate	0.01 – 0.10

a. Single Objective Optimization Experiment 1: In this experiment, single node failures are studied and the addition of unforeseen interdependencies is not considered. Each individual in GA represents an integer that encodes the node number of the node to be failed. The effect of this failure is propagated through the network model until all the nodes reach their steady states. The node whose failure results in the least giant component size is obtained by the optimization process in which single nodes will be failed iteratively in the network.

b. Single Objective Optimization Experiment 2: In this experiment, single node failures and addition of a single unforeseen interdependency is studied. A GA individual in this experiment is encoded as linear sequence of three integers (Fig.4.6). During optimization, a single unforeseen interdependency will be added to the network and single nodes will be failed iteratively until the network with the least giant component size is obtained.

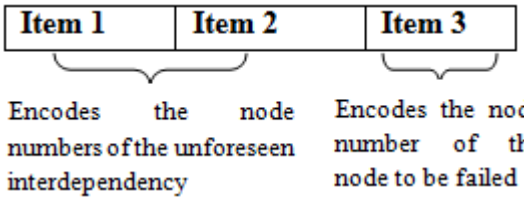

Fig. 4.6 Encoding of GA individuals in Single Objective Optimization Experiment 2

c. Single Objective Optimization Experiment 3: In this experiment, the addition of two unforeseen interdependencies together with single node failures is studied. A GA individual in this experiment can be encoded as a linear sequence of five integers (Fig. 4.7). During optimization, two unforeseen interdependencies are added iteratively to the network model and one node is failed until the network with the least giant component size is obtained.

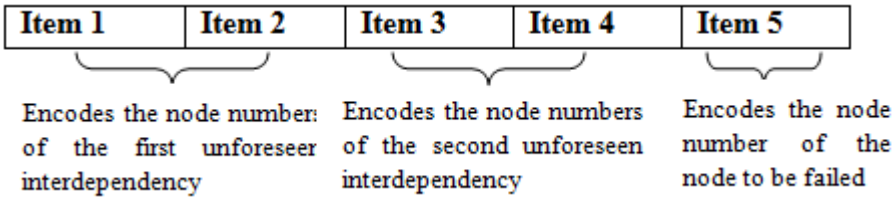

Fig. 4.7 Encoding of GA individuals in Single Objective Optimization Experiment 3

4.3.3.2 Multiobjective optimization: minimization of giant component size and maximization of probability

The aim of multiobjective optimization is to find the Pareto-optimal solutions (networks with corresponding failures) corresponding to maximum risk in order to anticipate extreme risk events. The well-known multiobjective evolutionary algorithm, NSGA II is used for optimization. Two different multiobjective optimization experiments are performed corresponding to single and two node failures. Table 4.2 lists the parameter settings of NSGA II.

Table 4.2 Parameter settings of NSGA II used for multiobjective optimization

Index	Parameter	Setting
1	Population size	100
2	Number of generations	100
3	Crossover rate	0.10 – 1.00
4	Mutation Rate	0.01 – 0.10

a. Multiobjective optimization experiment 1: An NSGA II individual in this experiment is formulated as a linear sequence of five integers as in Fig 4.7. For each individual in NSGA II, the two unforeseen interdependencies represented by the individual are added to the network model and then the node specified is made to fail. The effect of this failure is propagated through the network model until all the nodes reach their steady states. The failure consequence of each individual is then calculated by measuring the giant component size. The probability of each individual is the same as the failure probability of the node to be failed.

b. Multiobjective optimization experiment 2: An NSGA II individual in this experiment is formulated as a linear sequence of six integers (Fig 4.8). Similar to the previous experiment, for each NSGA II individual, the two unforeseen interdependencies represented by the individual are added to the network model and the two nodes specified are made to fail. The failure consequence of each individual is then calculated by measuring the giant component size and the probability of each individual is calculated as the product of the individual failure probabilities of the two nodes represented by the individual**.**

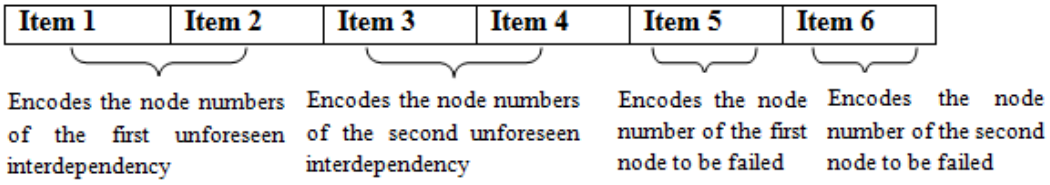

Fig. 4.8 Encoding of the NSGA II individual in multiobjective optimization experiment 2

For both experiments, a set of Pareto-optimal solutions (networks with corresponding failures) corresponding to maximum risk will be generated

towards the end of optimization. Among them, the solutions with minimum giant component sizes can be analyzed to determine the unforeseen interdependencies as well as the node failures that may lead to extreme risks in infrastructure networks.

4.4 Simulation Results

The total number of single node failures to be investigated in the infrastructure network is 43 since the network has 43 nodes. The number of ways in which a directed link can be added to the network is given by $P\ (43, 2)$ which refers to the permutation of 43 elements by taking 2 elements at a time as given by equation (4.2).

$$P\ (43, 2)\ =\ 43 * 42\ \ =\ 1806 \tag{4.2}$$

Assume that the set of unforeseen interdependencies has not been specified, i.e. they can be added between any two infrastructure nodes in the network which does not already have an existing interdependency between them. There are 64 known interdependencies in the network and therefore a single unforeseen interdependency can be added in 1742, i.e. $1806 - 64$ ways. A combination of 1742 elements taking two elements at a time provides information on how many ways in which two unforeseen links can be added as shown in equation (4.3).

$$C\ (1742, 2)\ =\ \frac{1742 * 1741}{2!}\ \ =\ 1516411 \tag{4.3}$$

The total number of cases in which single node failures and addition of two unforeseen interdependencies are studied becomes $1516411 * 43 = 65205673$. For the case where two node failures need to be studied, the search space becomes even larger. The total number of cases to be investigated increases exponentially with the number of interdependencies and node failures. This makes it difficult for using exhaustive search methods like brute-force for solving this particular optimization problem and also justifies the use of GA for solving the problem.

4.4.1 Simulation results of single objective optimization experiments

Multiple runs (about 25) of the single objective optimization experiments were performed by varying the mutation and crossover probabilities and the experiments showed that GA could effectively search from large scenario space to find the optimal solutions with reasonable running times (approx. 114 sec). Fig. 4.9 shows how the giant component size reduces with the number of generations in single objective GA experiments 2 and 3. The optimal solution was found in the case of single objective experiment 2 by 17th generation and in the case of experiment 3 by the 40th generation.

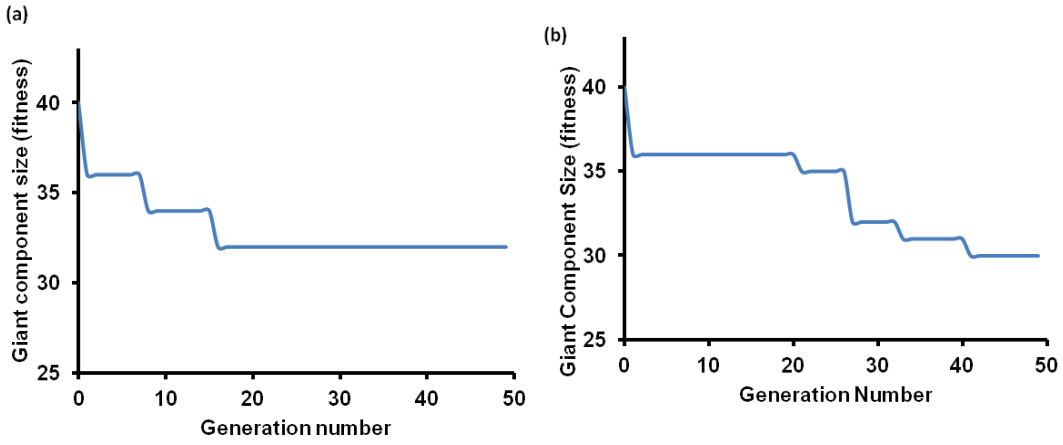

Fig. 4.9 Plot showing the improvement of fitness over successive generations in (a) Single objective GA Experiment 2 and (b) Single objective GA Experiment 3

4.4.1.1 Identifying Node Failure that results in the smallest giant component size

All the single objective GA experiments showed that the failure of node 28 results in the smallest giant component size. This may be because node 28 has interdependencies to many other nodes. In other words, many of the nodes in the infrastructure network rely on node 28 for input. Therefore, the failure of node 28 triggers cascading failure of many other nodes resulting in a greater reduction of giant component size when compared to other node failures.

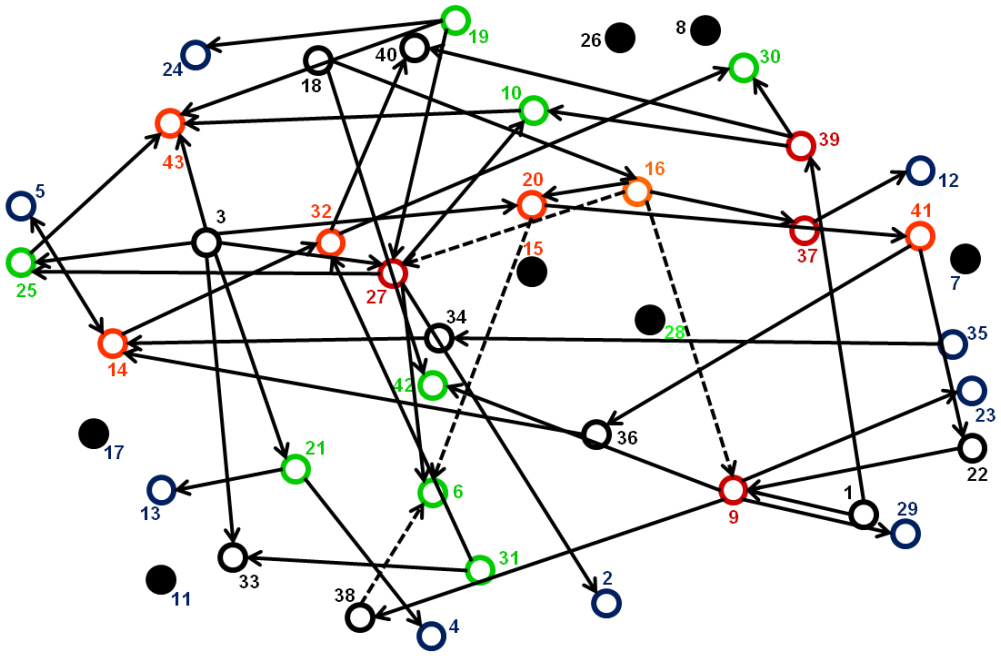

Fig. 4.10 A figure illustrating the disintegration of the studied infrastructure network when node 28 fails in GA Experiment 1.

Fig 4.10 shows the disintegration of the infrastructure network when node 28 is failed in GA Experiment 1. In the figure, the black nodes refer to the failed nodes that separate from the network's largest component thus reducing the giant component size to 36.

4.4.1.2 Identifying Crucial Unforeseen Interdependencies

Apart from the investigation of the crucial node failures that result in the least giant component size, there is a need to study the effect of adding unforeseen interdependencies on giant component size and also a need to identify the crucial unforeseen interdependencies in the network. Table 4.3 records the values of the giant component sizes obtained when node 28 fails and different number of unforeseen interdependencies are added to the infrastructure network. The table shows that adding more number of interdependencies results in greater reduction of giant component size. This implies that additional (unforeseen) interdependencies can indeed exacerbate the failure consequences.

Table 4.3 The effect of adding potential unforeseen interdependencies on giant component size after the failure of node 28

Experiment Number	No. of unforeseen interdependencies added	Unforeseen Interdependency added by GA in optimal solutions	Worst Giant comp. size
1	0	Nil	36
2	1	One of (7→3, 8→3, 11→3, 15→3, 17→3, 28→3, 31→3)	32
3	2	One of (7→3, 8→3, 11→3, 15→3, 17→3, 28→3, 31→3) and one of (3→19, 4→19, 13→19, 15→19, 21→19, 28→19)	30

A summary of the important unforeseen interdependencies obtained in the optimal solutions of the different GA experiments has also been provided in Table 4.3. An arrow is used to refer to a directed interdependency/link in the table, i.e. 7→3 refer to an unforeseen interdependency from node 7 to 3. The results from Table 4.3 show that the presence of an unforeseen interdependency to node 3 is the most crucial single unforeseen interdependency and the interdependencies to node 3 and 19 are the most crucial combination of two unforeseen interdependencies. One of the features common to node 3 and node 19 is that they are supply nodes and many nodes in the network depend on them for input. When some other nodes fail in the network, these supply nodes 3 and 19 also fail as a result of the unforeseen interdependencies added to them which further results in the failure of nodes dependent on them. This chain of failures reduces the giant component size to 30 which indicates a 30.23% reduction of giant component size.

4.4.2 Results of multiobjective optimization experiments

4.4.2.1 Results of multiobjective optimization experiment 1

The multiobjective optimization experiment 1 was run 15 times by varying the crossover and mutation probabilities. A plot of probability vs. giant component size of the individuals in the final generation of one of the runs has been shown in Fig.4.11. In the figure, the Pareto-optimal solutions corresponding to maximum risk are joined by a dashed line. The giant component sizes and probability values of the Pareto-optimal solutions obtained from all the 15 runs are listed in Table 4.4.

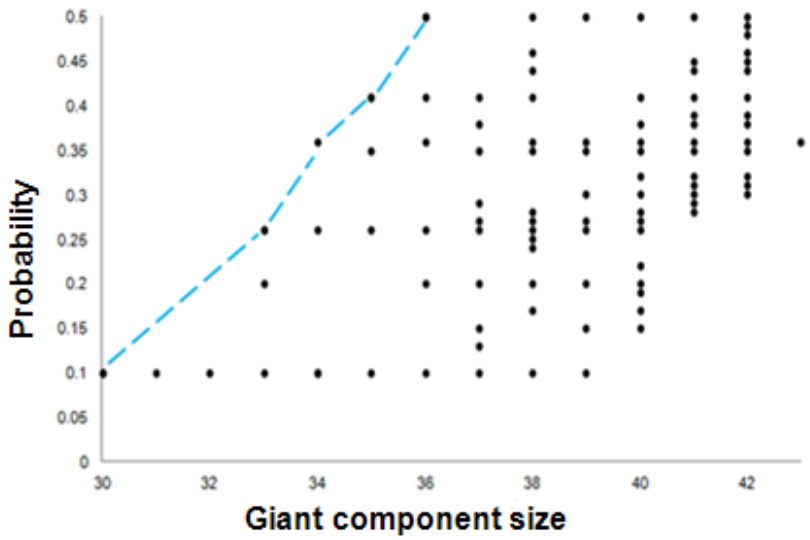

Fig. 4.11 A plot of probability vs. giant component size of individuals in multiobjective optimization experiment 1.

Table 4.4 Probabilities and giant component sizes of the Pareto-optimal solutions of multiobjective optimization experiment 1

Failed Node	Probability	Giant comp. size
28	0.1	30
9	0.26	33
15	0.36	34
31	0.41	35
1, 5, 12, 43	0.5	36

In order to investigate which node failure as well as unforeseen interdependencies can result in the maximum consequence, the Pareto-optimal solutions with the smallest giant component size of 30 obtained in the different runs of the experiment were observed in detail. One of the Pareto-optimal solutions corresponding to the smallest giant component size is shown in Fig 4.12.

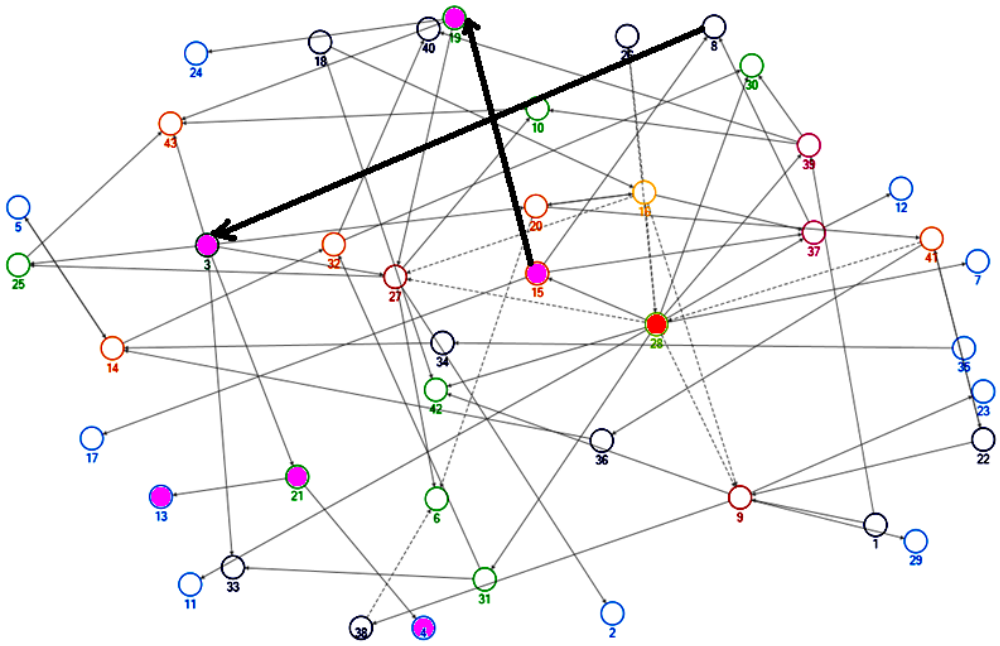

Fig. 4.12 One of the Pareto-optimal solutions corresponding to minimum giant component size in multiobjective optimization experiment 1

In Fig. 4.12, node failed is shown in red, the nodes that failed due to failure propagation are shown in purple and the unforeseen interdependencies are shown by bold lines. An observation of these Pareto-optimal solutions or networks identified the failure of node 28 as a potential extreme risk event. The failure probability of node 28 is 0.1. An analysis of the Pareto-optimal solutions also showed that the most crucial unforeseen interdependencies are the ones added to node 3 and node 19. These crucial interdependencies can be interpreted by experts in the case of real world networks.

4.4.2.2 Results of multiobjective optimization experiment 2

The multiobjective optimization experiment 2 was run 15 times by varying the crossover and mutation probabilities. A plot of probability vs. giant component size of the individuals in the final generation of one of the runs has been shown in Fig.4.13. In the figure, the Pareto-optimal solutions are joined by a dashed line.

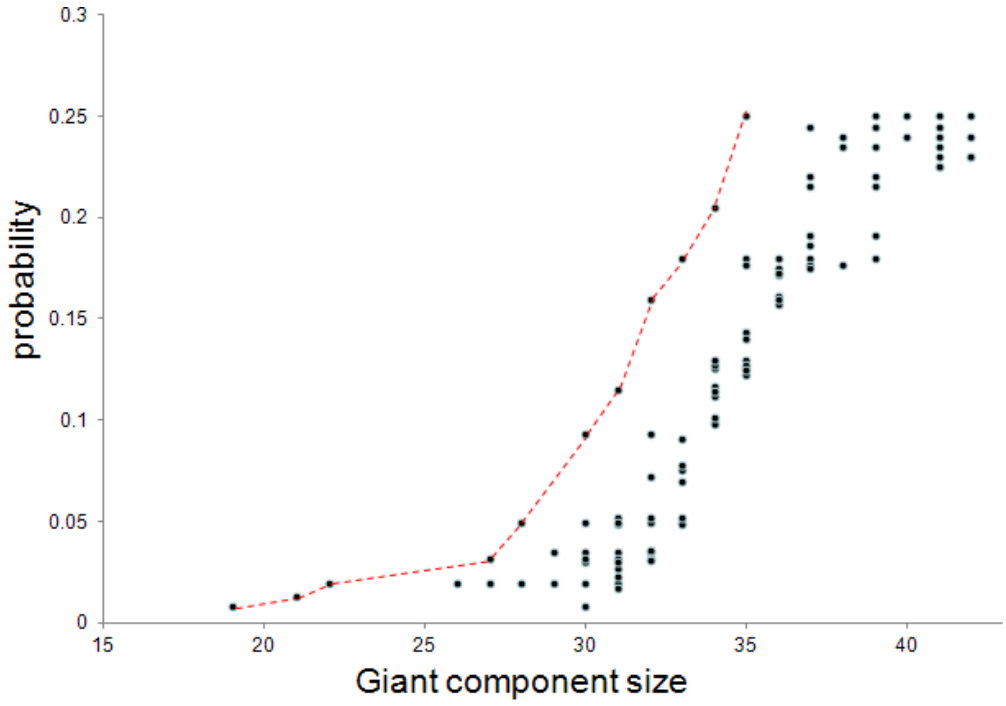

Fig. 4.13 A plot of probability vs. giant component size of individuals in multiobjective experiment 2

The giant component sizes and probability values of the Pareto-optimal solutions obtained from all the 15 runs are listed in Table 4.5. In order to investigate which combination of node failures as well as which unforeseen interdependencies can result in the maximum consequence or the smallest giant component size, the Pareto-optimal solutions with the smallest giant component size of 19 obtained in the different runs of the experiment were observed in detail. One of the Pareto-optimal solutions corresponding to the smallest giant component size is shown in Fig 4.14. In the figure, the two nodes failed are shown in red, the nodes that failed due to failure propagation are shown in purple and the unforeseen interdependencies are shown by bold lines. An observation of

these Pareto-optimal solutions identified the failure of node 28 together with the failure of node 41 as a potential extreme risk event. The probability of this failure event is calculated as the product of the individual node failure probabilities of 41 and 28 (assuming failure independence) and was found to be 0.008. The crucial unforeseen interdependencies were found to be added to nodes 1 and 3.

Table 4.5 Probabilities and giant component sizes of the Pareto-optimal solutions of multiobjective optimization experiment 2

Failed Nodes	Probability	Giant comp. size
28, 41	0.0080	19
28, 36	0.0130	21
28, 14	0.0200	22
28, 16	0.0320	27
28, 1	0.0500	28
9, 15	0.0936	30
27, 15	0.1152	31
27, 43	0.1600	32
(1,15),(5,15),(12,15),(43,15)	0.1800	33
(1,31),(5,31),(12,31),(43,31)	0.2050	34
(12,43),(1,12),(1,5),(1,43), (5,43),(5,12)	0.2500	35

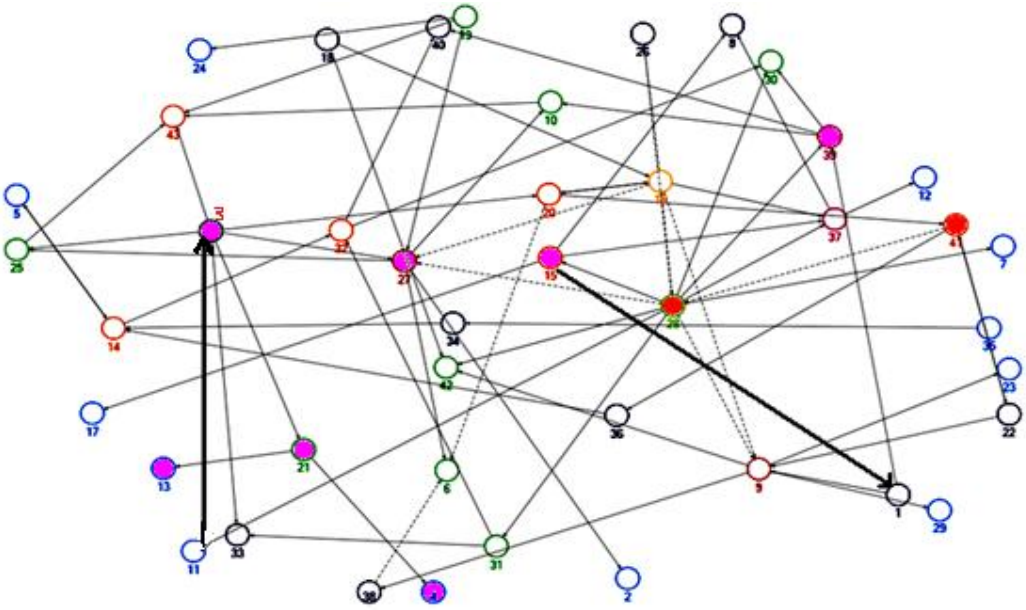

Fig. 4.14 One of the Pareto-optimal solutions corresponding to minimum giant component size in multiobjective experiment 2.

4.5 Summary

This chapter mainly discusses on a framework to anticipate extreme risk events in critical infrastructure networks where risk is considered to be function of failure probability and consequence. The proposed approach starts from a set of infrastructure components/nodes with their known interdependencies and applies a genetic algorithm to search for potential failure events and unforeseen interdependencies that can maximize risk. The approach was applied to an infrastructure network model and the results showed the potential of the proposed approach in unraveling the crucial nodes and unforeseen interdependencies in the network. It was also found from the study that the presence of additional/unforeseen interdependencies can increase the vulnerability of infrastructure networks thereby exacerbating the failure consequences.

CHAPTER 5: CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

The modeling and simulation of critical infrastructure network failures is challenging, but is extremely important for disruption prevention, protection as well as for recovery planning. The research in both single sector infrastructure as well as multi-sector infrastructures is important because the improvements made in single sector of infrastructure networks may influence the performance of other interdependent infrastructure networks.

Since the research on critical infrastructure is relatively new, the literature on them is not very well organized. There are a variety of modeling methods being developed like network theory, agent based modeling, system dynamics, etc. and also a variety of metrics for quantifying infrastructure failure consequences. Therefore the primary requirement was to understand the area and to properly organize the literature. The detailed literature review presented in Chapter 2 shows the current research trends in critical infrastructure protection and the motivation behind the research objectives.

Chapter 3 has presented an investigation of the failure consequences in critical infrastructure networks resulting from different node removal strategies using a proximity-based failure cascading model. The study investigates the removal/failure of nodes based on random, degree-based and recalculated degree-based node removal strategies. Through these removal strategies, the proposed study attempts to investigate which removal strategy results in the largest failure consequence in an infrastructure network. The failure consequences are measured using two metrics: accessibility and efficiency. Three networks: Singapore's rapid transit rail network, a network of bus interchanges/terminals and a combined rapid transit-bus network have been used for case studies. It was found from the results that in general, the studied networks show the behaviour of a random network since the networks behave in a similar manner to random as well as degree-based node removals. This means

that the failure consequence (reduction in both efficiency and accessibility) following node failures is similar for both random and degree-based removal strategies. However, recalculated node removal strategies result in more failure consequences when compared to non-recalculated removal strategies in all the three networks. The results also illustrate how the combined rapid transit-bus network behaves upon failures in comparison to the independent rapid transit and bus networks. The study shows that the presence of interdependencies can have both positive as well as negative consequences. On one hand interdependencies can improve the operation (in this case reduce the accessibility loss) of the combined network; on the other hand, the interdependencies can make the network more vulnerable leading to larger failure consequences (in this case the increase of efficiency loss).

Chapter 4 has presented a methodology to anticipate extreme risk events in critical infrastructure networks where risk is considered to be function of failure probability and consequence. On the assumption that a significant part of the network interdependencies is in fact unknown or unforeseen, the proposed approach starts from a set of infrastructure components/nodes with their known interdependencies and applies a genetic algorithm to search for potential failure points (node failures) and unforeseen interdependencies that can maximize risk in infrastructure networks. The approach was applied to an infrastructure network model. The failure consequence in the infrastructure network has been quantified using a metric called giant component size and the failure probabilities have been randomly assigned to the nodes for the purpose of case study. The results from the study mainly unraveled the single node failure as well as combination of two node failures that can maximize risk in the studied network. It was also found from the results that the presence of additional/unforeseen interdependencies can increase the vulnerability of infrastructure networks thereby exacerbating the failure consequences. The results also investigate those potential unforeseen interdependencies that can increase disruption consequences in these networks.

5.2 Original Contributions Arising from Work

The contributions at the end of this research are summarized below:-

1. The proposed study for vulnerability/consequence analysis of critical infrastructure networks has been applied to Singapore's transportation network. To the best of the author's knowledge, there are no works studying the vulnerability or failure consequence of Singapore's transportation networks to random and intentional component failures.

2. As seen in the literature, all the previous works on critical infrastructure protection have been based on the assumption that the knowledge about the interdependent infrastructure network is complete. This research is based on the assumption that the knowledge about the network interdependencies is in fact incomplete. For the first time, the current trends and thinking about critical infrastructure protection has been challenged and an optimization algorithm has been used to search for the unforeseen interdependencies as well as failure points (node failures) resulting in extreme disruptions, thereby anticipating extreme risk events.

3. Another highlight is that the methodology to anticipate extreme risk event complements the vulnerability or consequence analysis of networked infrastructures with node failure probabilities. A risk analysis approach has been given to the problem since both the consequence of failures and their probabilities of occurrence are computed as the criteria for optimization. The multiobjective maximization of risk is also a novel problem.

5.3 Future Work

The recommended future work of this research is summarized below:-

1. The load/traffic at various nodes in transportation networks has been assumed to be a function of its topological property called degree. However, in reality, the load or passenger traffic flow at each station has to be estimated through electronic tap-in and tap-out data available with the Land Transport Authority.

2. In the current research, only the node failure scenarios were investigated. There is a need to look at the effect of failure of links or interdependencies. For

this, new ways to implement cascading failures upon failure of links should be incorporated.

3. The decision variables/vector of genetic algorithm incorporated unforeseen interdependencies as well as node failures within the network. There is a need to extend the decision vector to incorporate the concept of failure mode (the different ways in which a node may fail such as intentional attack, random failure, failure due to a natural disaster, etc). There is also a need to implement cascading failures depending on the failure mode.

4. The failure probabilities of nodes were randomly assigned for the purpose of case study. There is a need for further investigation on how to use information like failure statistics, technical data, and expert opinion in order to calculate the failure probabilities of different nodes.

5. The approach to anticipate extreme risk events has to be further validated on more real world interdependent networks. The combined rapid transit-bus network can be further extended by adding more sectors and the proposed approach will be applied to study the critical nodes and unforeseen interdependencies in the interdependent network.

REFERENCES

[1] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *Control Systems, IEEE*, vol. 21, pp. 11-25, 2001.

[2] T. D. O'Rourke, "Critical infrastructure, interdependencies, and resilience," *BRIDGE-WASHINGTON-NATIONAL ACADEMY OF ENGINEERING-*, vol. 37, p. 22, 2007.

[3] C. L. Chai, X. Liu, W. Zhang, and Z. Baber, "Application of social network theory to prioritizing Oil & Gas industries protection in a networked critical infrastructure system," *Journal of Loss Prevention in the Process Industries*, vol. 24, pp. 688-694, 2011.

[4] J. K. Levy and C. Gopalakrishnan, "Promoting disaster-resilient communities: the Great Sumatra–Andaman earthquake of 26 December 2004 and the resulting Indian Ocean tsunami," *Water Resources Development*, vol. 21, pp. 543-559, 2005.

[5] E. Lekkas, E. Andreadakis, V. Alexoudi, E. Kapourani, and I. Kostaki, "The Mw= 9.0 Tohoku Japan earthquake (March 11, 2011) tsunami impact on structures and infrastructure," in *Environmental Geosciences and Engineering Survey for Territory Protection and Population Safety (EngeoPro) International conference, Moscow*, 2011, pp. 97-103.

[6] R. Setola and S. De Porcellinis, "Complex networks and critical infrastructures," in *Modelling, Estimation and Control of Networked Complex Systems*, ed: Springer, 2009, pp. 91-106.

[7] J. Johansson, "Risk and vulnerability analysis of interdependent technical infrastructures," *PhD avhandling, Universitetet i Lund*, 2010.

[8] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," *International Journal of Electrical Power & Energy Systems*, vol. 28, pp. 627-633, 2006.

[9] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," *Risk analysis*, vol. 1, pp. 11-27, 1981.

[10] M. A. Taylor and G. M. D'Este, Transport network vulnerability: a method for diagnosis of critical locations in transport infrastructure systems: *In Critical Infrastructure: Reliability and Vulnerability*, Edited by Murray, A, Springer, pp. 9-30, 2007.

[11] Å. Holmgren, "Vulnerability analysis of electric power delivery networks. ," *Ph.D Thesis*, Royal Institute of Technology, Stockholm, Sweden., 2004.

[12] Y. Y. Haimes, "On the definition of vulnerabilities in measuring risks to infrastructures," *Risk analysis*, vol. 26, pp. 293-296, 2006.

[13] P. Buckle, G. Mars, and S. Smale, "New approaches to assessing vulnerability and resilience," *Australian Journal of Emergency Management*, vol. 15, pp. 8-14, 2000.

[14] P. Erdös and A. Rényi, "On random graphs, I," *Publicationes Mathematicae (Debrecen)*, vol. 6, pp. 290-297, 1959.

[15] D. Watts and S. Strogatz, "The small world problem," *Collective Dynamics of Small-World Networks*, vol. 393, pp. 440-442, 1998.

[16] A.-L. Barabási, R. Albert, and H. Jeong, "Scale-free characteristics of random networks: the topology of the world-wide web," *Physica A: Statistical Mechanics and its Applications,* vol. 281, pp. 69-77, 2000.
[17] X. F. Wang and G. Chen, "Complex networks: small-world, scale-free and beyond," *Circuits and Systems Magazine, IEEE,* vol. 3, pp. 6-20, 2003.
[18] M. E. Newman, "The structure and function of complex networks," *SIAM review,* vol. 45, pp. 167-256, 2003.
[19] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of modern physics,* vol. 74, p. 47, 2002.
[20] S. Perseguers, M. Lewenstein, A. Acín, and J. I. Cirac, "Quantum random networks," *Nature Physics,* vol. 6, pp. 539-543, 2010.
[21] H. Thadakamaila, U. N. Raghavan, S. Kumara, and R. Albert, "Survivability of multiagent-based supply networks: a topological perspect," *Intelligent Systems, IEEE,* vol. 19, pp. 24-31, 2004.
[22] M. Sharma, "Unraveling the Dynamics of Digital Library Community: A Social Network Analysis Approach," *Bulletin of IEEE Technical Committee on Digital Libraries,* vol. 6, pp. 1937-7266, 2010.
[23] A. O. I. Hoffmann, W. Jager, and J. Von Eije, "Social simulation of stock markets: Taking it to the next level," *Journal of Artificial Societies and Social Simulation,* vol. 10, p. 7, 2007.
[24] R. Albert, H. Jeong, and A. L. Barabási, "Error and attack tolerance of complex networks," *Nature,* vol. 406, pp. 378-382, 2000.
[25] M. Sapre and N. Parekh, "Analysis of Centrality Measures of Airport Network of India," *Lecture Notes in Computer Science,* Vol.6744, pp.376-381, 2010.
[26] T. H. Grubesic, T. C. Matisziw, A. T. Murray, and D. Snediker, "Comparative approaches for assessing network vulnerability," *International Regional Science Review,* vol. 31, pp. 88-112, 2008.
[27] W. L. Garrison and D. F. Marble, The structure of transportation networks: *U.S. Army Transportation Command Technical Report 62-II,*1962.
[28] P. HAGGETT and R. J. CHORLEY, *Network analysis in geography*: St. Martin's Press, 1970.
[29] U. Demšar, O. Špatenková, and K. Virrantaus, "Identifying critical locations in a spatial network with graph theory," *Transactions in GIS,* vol. 12, pp. 61-82, 2008.
[30] F. Li, Y. Cao, and G. Li, "A Node Importance Assessment Method of Complex Networks Based on Reliability Measure," *Future Intelligent Information Systems,* pp. 271-278, 2011.
[31] S. P. Gorman, L. Schintler, R. Kulkarni, and R. Stough, "The revenge of distance: Vulnerability analysis of critical information infrastructure," *Journal of Contingencies and Crisis Management,* vol. 12, pp. 48-63, 2004.
[32] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Physica A: Statistical Mechanics and its Applications,* vol. 357, pp. 593-612, 2005.
[33] A. Nair and J. M. Vidal, "Supply network topology and robustness against disruptions–an investigation using multi-agent model,"

International Journal of Production Research, vol. 49, pp. 1391-1404, 2011.

[34] A. T. Murray, "An overview of network vulnerability modeling approaches," *GeoJournal,* pp. 1-13, 2011.

[35] R. Wollmer, "Removing arcs from a network," *Operations Research,* vol. 12, pp. 934-940, 1964.

[36] P. Baran, "On distributed communications networks," *IEEE Transactions on Communications Systems,* vol. 12, pp. 1-9, 1964.

[37] D. R. Fulkerson and G. C. Harding, "Maximizing the minimum source-sink path subject to a budget constraint," *Mathematical Programming,* vol. 13, pp. 116-118, 1977.

[38] H. Corley and D. Y. Sha, "Most vital links and nodes in weighted networks," *Operations Research Letters,* vol. 1, pp. 157-160, 1982.

[39] Y.-S. Myung and H.-j. Kim, "A cutting plane algorithm for computing k-edge survivability of a network," *European Journal of Operational Research,* vol. 156, pp. 579-589, 2004.

[40] R. L. Church, M. P. Scaparra, and R. S. Middleton, "Identifying critical infrastructure: the median and covering facility interdiction problems," *Annals of the Association of American Geographers,* vol. 94, pp. 491-502, 2004.

[41] T. H. Grubesic and A. T. Murray, "Vital nodes, interconnected infrastructures, and the geographies of network survivability," *Annals of the Association of American Geographers,* vol. 96, pp. 64-83, 2006.

[42] E. Jenelius, "Redundancy importance: Links as rerouting alternatives during road network disruptions," *Procedia Engineering,* vol. 3, pp. 129-137, 2010.

[43] C. M. Rocco S and J. E. Ramirez-Marquez, "Vulnerability metrics and analysis for communities in complex networks," *Reliability Engineering & System Safety,* 2011.

[44] J. Wang, L. Rong, L. Zhang, and Z. Zhang, "Attack vulnerability of scale-free networks due to cascading failures," *Physica A: Statistical Mechanics and its Applications,* vol. 387, pp. 6671-6678, 2008.

[45] J. Wu, H. Sun, and Z. Gao, "Capacity assignment model to defense cascading failures," *International Journal of Modern Physics C,* vol. 20, pp. 991-999, 2009.

[46] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Physical Review E,* vol. 69, p. 045104, 2004.

[47] B. Mirzasoleiman, M. Babaei, M. Jalili, and M. Safari, "Cascaded failures in weighted networks," *Physical Review E,* vol. 84, p. 046114, 2011.

[48] X. Fang, Q. Yang, and W. Yan, "Modeling and analysis of cascading failure in directed complex networks," *Safety Science,* vol. 65, pp. 1-9, 2014.

[49] J. Wang, Y.-H. Liu, Y. Jiao, and H.-Y. Hu, "Cascading dynamics in congested complex networks," *The European Physical Journal B-Condensed Matter and Complex Systems,* vol. 67, pp. 95-100, 2009.

[50] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grids vulnerability: a complex network approach," *Chaos,* vol. 19, p. Article Number 013119, 2008.

[51] C. Rocco, J. Ramirez-Marquez, D. Salazar, and I. Hernandez, "Implementation of multi-objective optimization for vulnerability analysis of complex networks," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability,* vol. 224, pp. 87-95, 2010.

[52] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the North American power grid," *The European Physical Journal B-Condensed Matter and Complex Systems,* vol. 46, pp. 101-107, 2005.

[53] A. T. Murray, T. C. Matisziw, and T. H. Grubesic, "Critical network infrastructure analysis: interdiction and system flow," *Journal of Geographical Systems,* vol. 9, pp. 103-117, 2007.

[54] J. Zhang, X. Xu, L. Hong, S. Wang, and Q. Fei, "Networked analysis of the Shanghai subway network, in China," *Physica A: Statistical Mechanics and its Applications,* vol. 390, pp. 4562-4570, 2011.

[55] Y. Deng, Q. Li, Y. Lu, and J. Yuan, "Topology Vulnerability Analysis and Measure of Urban Metro Network: The case of Nanjing," *Journal of Networks,* vol. 8, pp. 1350-1356, 2013.

[56] C. Shi-Ming, P. Shao-Peng, and Z. Xiao-Qun, "An LCOR model for suppressing cascading failure in weighted complex networks," *Chinese Physics B,* vol. 22, p. 058901, 2013.

[57] G. Bagler, "Analysis of the airport network of India as a complex weighted network," *Physica A: Statistical Mechanics and its Applications,* vol. 387, pp. 2972-2980, 2008.

[58] J. S. Foster, E. Gjelde, W. R. Graham, R. J. Hermann, H. M. Kluepfel, R. L. Lawson, *et al.*, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP)Attack," in *Executive Report*, 2004.

[59] A. Vespignani, "The fragility of interdependency," *Nature,* vol. 464, p. 15, 2010.

[60] S. M. Rinaldi, "Modeling and simulating critical infrastructures and their interdependencies," *Proceedings of the Annual Hawaii International Conference on System Sciences*, Vol.37 , art. no. CSRRC01 , pp.873-880, 2004.

[61] D. D. Dudenhoeffer, M. R. Permann, and M. Manic, "CIMS: A framework for infrastructure interdependency modeling and analysis," *Winter Simulation Conference*, pp. 478-485, 2004.

[62] R. Setola, S. De Porcellinis, and M. Sforna, "Critical infrastructure dependency assessment using the input-output inoperability model," *International Journal of Critical Infrastructure Protection,* vol. 2, pp. 170-178, 2009.

[63] H. Jönsson, J. Johansson, and H. Johansson, "Identifying critical components in technical infrastructure networks," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability,* vol. 222, pp. 235-243, 2008.

[64] N. Hadjsaid, C. Tranchita, B. Rozel, M. Viziteu, and R. Caire, "Modeling cyber and physical interdependencies-Application in ICT and power grids," in *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES*, 2009, pp. 1-6.

[65] B. D. Mussington, Concepts for Enhancing Critical Infrastructure Protection: *Rand Corporation. Santa Monica, California*,2002.

[66] J. Johansson and H. Hassel, "An approach for modelling interdependent infrastructures in the context of vulnerability analysis," *Reliability Engineering & System Safety,* vol. 95, pp. 1335-1344, 2010.

[67] E. Solano, "Methods for Assessing Vulnerability of Critical Infrastructure," *Institute for Homeland Security Solutions (IHSS),* March 2010.

[68] N. K. Svendsen and S. D. Wolthusen, "Connectivity models of interdependency in mixed-type critical infrastructure networks," *Information Security Technical Report,* vol. 12, pp. 44-55, 2007.

[69] Y. Y. Haimes and P. Jiang, "Leontief-based model of risk in complex interconnected infrastructures," *Journal of Infrastructure Systems,* vol. 7, p. 1, 2001.

[70] Y. Y. Haimes, B. M. Horowitz, J. H. Lambert, J. R. Santos, C. Lian, and K. G. Crowther, "Inoperability input-output model for interdependent infrastructure sectors. I: Theory and methodology," *Journal of Infrastructure Systems,* vol. 11, pp. 67-79, 2005.

[71] Y. Y. Haimes, B. M. Horowitz, J. H. Lambert, J. Santos, K. Crowther, and C. Lian, "Inoperability input-output model for interdependent infrastructure sectors. II: case studies," *Journal of Infrastructure Systems,* vol. 11, p. 80, 2005.

[72] J. W. Forrester, *World dynamics*: Wright-Allen Press, 1971.

[73] S. H. Conrad, R. J. LeClaire, G. P. O'Reilly, and H. Uzunalioglu, "Critical national infrastructure reliability modeling and analysis," *Bell Labs Technical Journal,* vol. 11, pp. 57-71, 2006.

[74] N. Schieritz, "Integrating system dynamics and agent-based modeling," in *Proceedings of the 20th International Conference of the System Dynamics Society*, 2002.

[75] N. Schieritz and P. M. Milling, "Modeling the forest or modeling the trees," in *Proceedings of the 21st International Conference of the System Dynamics Society*, 2003, pp. 20-24.

[76] C. M. Macal and M. J. North, "Tutorial on agent-based modelling and simulation," *Journal of Simulation,* vol. 4, pp. 151-162, 2010.

[77] P. Zhang, S. Peeta, and T. Friesz, "Dynamic game theoretic model of multi-layer infrastructure networks," *Networks and Spatial Economics,* vol. 5, pp. 147-178, 2005.

[78] E. Casalicchio, E. Galli, and S. Tucci, "Modeling and simulation of Complex Interdependent Systems: a federated agent-based approach," in *Critical information infrastructure security*, ed: Springer, 2009, pp. 72-83.

[79] T. McDaniels, S. Chang, K. Peterson, J. Mikawoz, and D. Reed, "Empirical framework for characterizing infrastructure failure interdependencies," *Journal of Infrastructure Systems,* vol. 13, p. 175, 2007.

[80] R. Zimmerman, "Decision-making and the vulnerability of interdependent critical infrastructure," *IEEE International Conference on Systems, Man and Cybernetics*, pp. 4059-4063 vol. 5, 2004.

[81] F. Tan, Y. Xia, W. Zhang, and X. Jin, "Cascading failures of loads in interconnected networks under intentional attack," *EPL (Europhysics Letters)*, vol. 102, p. 28009, 2013.
[82] I. Hernandez-Fajardo and L. Dueñas-Osorio, "Probabilistic study of cascading failures in complex interdependent lifeline systems," *Reliability Engineering & System Safety*, vol. 111, pp. 260-272, 2013.
[83] S. Wang, L. Hong, M. Ouyang, J. Zhang, and X. Chen, "Vulnerability analysis of interdependent infrastructure systems under edge attack strategies," *Safety science*, vol. 51, pp. 328-337, 2013.
[84] E. Dalziell and A. Nicholson, "Risk and impact of natural hazards on a road network," *Journal of transportation engineering*, vol. 127, pp. 159-166, 2001.
[85] J. Winkler, L. Duenas-Osorio, R. Stein, and D. Subramanian, "Performance assessment of topologically diverse power systems subjected to hurricane events," *Reliability Engineering & System Safety*, vol. 95, pp. 323-336, 2010.
[86] Taleb, "The Black Swan: The impact of the highly improbable," ed: New York Random House, 2007.
[87] "Leaks, damaged cable cause of 4-hour delay on Circle Line " *The Strait Times*, vol. 29 September 2011.
[88] L. Ignatius, "Singapore's MRT Breakdown Chaos Leaves Thousands Stranded," *The Strait Times*, December 16, 2011.
[89] "SMRT Network Map. ," *Available at: <http://www.lta.gov.sg>*.
[90] "Singapore MRT Map. ," *Available at: <http://www.exploresg.com/mrt/pedia>*.
[91] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Error and attack tolerance of complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 340, pp. 388-394, 2004.
[92] S. Wang, "Cascading Model of Infrastructure Networks based on Complex Network," *Journal of Networks*, vol. 8, pp. 1448-1454, 2013.
[93] D. A. Niemeier, "Accessibility: an evaluation using consumer welfare," *Transportation*, vol. 24, pp. 377-396, 1997.
[94] M. A. Taylor, "Remoteness and accessibility in the vulnerability analysis of regional road networks," *Transportation research part A: policy and practice*, vol. 46, pp. 761-771, 2012.
[95] M. Ouyang, L. Zhao, L. Hong, and Z. Pan, "Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability," *Reliability Engineering & System Safety*, vol. 123, pp. 38-46, 2014.
[96] E. Jahanpour and X. Chen, "Analysis of complex network performance and heuristic node removal strategies," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, pp. 3458-3468, 2013.
[97] U. Wilensky, "NetLogo: Center for connected learning and computer-based modeling," *Northwestern University*, 1999.
[98] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025-1028, 2010.
[99] J. H. Holland, "Genetic algorithms," *Scientific american*, vol. 267, pp. 66-72, 1992.

[100] K. Deb, "An introduction to genetic algorithms," in *Sadhana (Academy Proceedings in Engineering Sciences)*, 1999, pp. 293-315.
[101] A. Konak, D. W. Coit, and A. E. Smith, "Multi-objective optimization using genetic algorithms: A tutorial," *Reliability Engineering & System Safety*, vol. 91, pp. 992-1007, 2006.
[102] Y. Nojima, K. Narukawa, S. Kaige, and H. Ishibuchi, "Effects of removing overlapping solutions on the performance of the NSGA-II algorithm," in *Evolutionary Multi-Criterion Optimization*, 2005, pp. 341-354.
[103] C. Y. Lam, J. Lin, M. S. Sim, and K. Tai, "Identifying vulnerabilities in critical infrastructures by network analysis," *International journal of critical infrastructures*, vol. 9, pp. 190-210, 2013.
[104] R. Tarjan, "Depth-first search and linear graph algorithms," *SIAM journal on computing*, vol. 1, pp. 146-160, 1972.

APPENDIX A

Terms used in network theory

A graph or network is a mathematical structure consisting of a set of vertices or nodes and a set of edges or links connecting the nodes. It is usually denoted by $G(V, E)$ where V is the set of nodes and E is the set of links.

Node:-A node is a terminal point or an intersection point of a network. It is the abstraction of a location such as a city, a router in a data network, a bus stop, a transit terminal, a petrol pump station, etc. The node set of a network G is usually denoted by $V(G)$ or simply V and the number of nodes in a network is represented by n.

***Link*:-**A link is a connection between two nodes. A link is the abstraction of a transport mechanism supporting movements between nodes and it usually represents roads, communication channels, pipes, etc. The link set of G is usually denoted by $E(G)$. The total number of links in a network is usually denoted by m. A link is directed if connects an ordered pair of nodes and a directed link can be represented graphically as an arrow drawn between the end nodes. A link is considered undirected if it disregards any sense of direction and treats both end nodes interchangeably.

Directed and Undirected Networks:-A directed network is the one whose links are directed and an undirected network is the one in which the links are not directed.

Degree:-The degree of a node in an undirected network is the total number of its links. For a directed network there are two types of degrees: in-degree and out-degree. The in-degree of a node is the number of its incoming links and out-degree of a node is the number of its outgoing links.

Path:-A sequence of links that are traveled in the same direction. For a path to exist between two nodes, it must be possible to travel an uninterrupted sequence of links.

Length of a link or path:-It can denote physical distance, the amount of traffic, the capacity or any attribute of a link.

Subnetwork: **-** A subnetwork of a network G is a network whose node set is a subset of that of the entire node set of network G. The subnetwork of a network G is denoted by g.

Connected Network:- A network is connected if a path exists from any node to any other node in the network.

Circuit:- If the path is a simple path, with no repeated nodes or links other than the starting and ending nodes, it is called a circuit.

Cycle:-It can be a closed walk or a simple cycle. If the path is a simple path, with no repeated nodes or links other than the starting and ending nodes, it is called a circuit or simple cycle. If repeated nodes are allowed, the path is called a closed walk.

Tree:- A connected network without a cycle is a tree. If a link is removed from such a network, it ceases to be connected. If a new link is added between any two nodes of a tree, a circuit is created.

Spanning tree:-A spanning tree of a network *G* is a tree composed of all the nodes and some (or perhaps all) of the links of *G*.

Order:-The order of a network is the number of its nodes. Order of a component is the number of nodes in that component.

Loop:-A loop is a link whose endpoints are the same nodes.

Complete networks:-A complete network is the one in which every node is connected to every other node in the network.

Cut vertex:-A cut vertex is a vertex whose removal disconnects the network.

***Component*:-** A component of a network is defined as a subnetwork in which a path exists from every node to every other node(i.e., they are mutually reachable).

Giant Component:-It is the largest component in a network.

APPENDIX B

NODE	PRIMARY LINKS	SECOND-ARY LINKS	BUFFER-ING TIME	RECOVERY TIME	PROBA-BILITY OF FAILURE
1	9, 39	0	9	9	0.500
2	0	0	0	10	0.490
3	20, 21, 25, 27, 33, 43	0	20	0	0.350
4	0	0	0	0	0.480
5	14	0	3	0	0.500
6	0	0	0	7	0.460
7	0	0	0	8	0.450
8	0	0	0	12	0.440
9	23, 29, 38, 42	0	2	2	0.260
10	43	0	0	0	0.390
11	0	0	0	9	0.380
12	0	0	0	5	0.500
13	0	0	0	0	0.360
14	5, 32	0	3	3	0.200
15	8, 17, 37	0	8	0	0.360
16	20, 37	9, 27	0	3	0.320
17	0	0	0	4	0.310
18	16, 42	0	6	16	0.300
19	24, 27, 43	0	0	0	0.290
20	41	6	4	14	0.280
21	4, 13	0	0	0	0.270
22	9	0	9	0	0.260
23	0	0	0	0	0.250
24	0	0	0	2	0.240
25	43	0	4	0	0.230
26	0	28	0	0	0.220

27	2, 6, 10, 25	0	6	7	0.320
28	7, 11, 15, 30, 31, 37, 39, 42	9, 27	7	5	0.100
29	0	0	0	0	0.200
30	0	0	2	0	0.190
31	32, 33	0	0	5	0.410
32	30, 40	0	2	0	0.170
33	0	0	0	12	0.160
34	14	0	0	0	0.150
35	34	0	3	3	0.300
36	14	0	0	7	0.130
37	12	0	12	2	0.350
38	0	6	0	0	0.110
39	10, 30, 40	0	10	0	0.100
40	0	0	0	9	0.090
41	22, 36	28	0	10	0.080
42	0	0	0	0	0.070
43	0	0	8	0	0.500