Critical node identification for accessing network vulnerability: a necessary consideration

Critical Node Identification for Accessing Network Vulnerability, A Necessary Consideration

By
Waqar Asif
120050615

Supervisors
Dr. Muttukrishnan Rajarajan
Dr. Marios Lestas
Dr. Hassaan Khaliq Qureshi
Dr. Veselin Rakocevic

A THESIS SUBMITTED TO THE SCHOOL OF ENGINEERING AND MATHEMATICAL SCIENCES, CITY UNIVERSITY, LONDON IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

(Sept 2016)

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text. This dissertation contains fewer than 65,000 words including bibliography, footnotes, tables and equations and has fewer than 150 figures.

Waqar Asif

Acknowledgement

First And foremost, I am immensely thankful to Almighty Allah for letting me pursue and fulfil my dreams. Nothing could have been possible without His blessings.

I would like to thank my parents for their support throughout my educational career, specially during my Ph.D years, where their unending financial and moral support has helped me in completing this work. I would also like to thank my sisters, my elder brother and my fiance for always being their for me at all times. I wish to express my gratitude to my academic advisors: Dr. Muttukrishnan Rajarajan, Dr. Marios Lestas, Dr. Hassaan Khaliq Qureshi and Dr. Veselin Rakocevic for guiding me throughout this work. I specially want to thank Dr. Marios Lestas for being more of a friend than a supervisor to me and guiding me through in every possible matter in life and for making my stay in Cyprus one of the best moments. I must acknowledge Dr. Arshad Ali and Dr. Christos Themistos for their sincere efforts and for selecting me as an exchange student for Cyprus. Here I would also like to thank everyone from the coordinating team of Erasmus Mundas Strong Ties who sponsored my stay in Cyprus and helped me groom both as a person and as a researcher.

List of Abbreviations

CBDI . . . . . Combined Banzhaf & Diversity Index

WSN . . . . . Wireless Sensor Network

CDS . . . . . Connected Dominating Set

APL . . . . . Average Path Length

VRAM . . . . Variable Rate Adaptive Modulation

NAW . . . . . Neighbour Avoiding Walk

HILPR . . . . Hybrid Interactive Linear Programming Rounding

QAM . . . . . Quadrature Amplitude Modulation

BFS . . . . . . Breath First Search

SNR . . . . . Signal to Noise Ratio

BER . . . . . Bit Error Rate

RF . . . . . . Radio Frequency

WFB . . . . . Wireless Flow Betweenness

CSMA/CA . Carrier Sense Multiple Access with Collision Avoidance

NS3 . . . . . . Network Simulator 3

OLSR . . . . Optimized Link State Routing

Cont . . . . . Controllability of complex networks

NUM . . . . . Network Utility Maximization

LHS . . . . . Left Hand Side

RHS . . . . . Right Hand Side

SSD . . . . . . Sum Squared Difference

NSSD . . . . Normalized Sum Squared Difference

SPNC . . . . Spectral Partitioning for Node Criticality

Abstract

Timely identification of critical nodes is crucial for assessing network vulnerability and survivability. This thesis presents two new approaches for the identification of critical nodes in a network with the first being an intuition based approach and the second being build on a mathematical framework. The first approach which is referred to as the Combined Banzhaf & Diversity Index (CBDI) uses a newly devised diversity metric, that uses the variability of a node's attributes relative to its neighbours and the Banzhaf power index which characterizes the degree of participation of a node in forming the shortest path route. The Banzhaf power index is inspired from the theory of voting games in game theory whereas, the diversity index is inspired from the analysis and understanding of the influence of the average path length of a network on its performance. This thesis also presents a new approach for evaluating this average path length metric of a network with reduced computational complexity and proposes a new mechanism for reducing the average path length of a network for relatively larger network structures. The proposed average path length reduction mechanism is tested for a wireless sensor network and the results compared for multiple existing approaches. It has been observed using simulations that, the proposed average path

length reduction mechanism outperforms existing approaches by reducing the average path length to a greater extent and with a simpler hardware requirement.

The second approach proposed in this thesis for the identification of critical nodes is build on a mathematical framework and it is based on suboptimal solutions of two optimization problems, namely the algebraic connectivity minimization problem and a min-max network utility problem. The former attempts to address the topological aspect of node criticality whereas, the latter attempts to address its connection-oriented nature. The suboptimal solution of the algebraic connectivity minimization problem is obtained through spectral partitioning considerations. This approach leads to a distributed solution which is computationally less expensive than other approaches that exist in the literature and is near optimal, in the sense that it is shown through simulations to approximate a lower bound which is obtained analytically. Despite the generality of the proposed approaches, this thesis evaluates their performance on a wireless ad hoc network and demonstrates through extensive simulations that the proposed solutions are able to choose more critical nodes relative to other approaches, as it is observed that when these nodes are removed they lead to the highest degradation in network performance in terms of the achieved network throughput, the average network delay, the average network jitter and the number of dropped packets.

Publications

The following seven publications are part of this thesis:

0.1 Conference Publications:

1. Waqar Asif, Hassaan Khaliq Qureshi, Muttukrishnan Rajarajan, "Variable Rate Adaptive Modulation (VRAM) for introducing Small-World model into WSNs," in 47th Annual Conference on Information Sciences and Systems (CISS), 2013, pp,1-6.

2. Waqar Asif, Hassaan Khaliq, Muttukrishnan Rajarajan, Marios Lestas, "CBDI: Combined Banzhaf & diversity index for finding critical nodes," Global Communications Conference (GLOBECOM), 2014 IEEE, Austin, TX, 2014, pp. 758-763.

3. Waqar Asif, Marios Lestas, Hassaan Khaliq, Muttukrishnan Rajarajan, "Spectral partitioning for node criticality," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 877-882.

0.2 Journal Publications:

1. Mahzeb Fiaz, Roomana Yousaf, Maryam Hanif, Waqar Asif, Hassaan Khaliq Qureshi, Muttukrishnan Rajarajan, "Adding the Reliability on Tree Based Topology Construction Algorithms for Wireless Sensor Networks". Wireless Personal Communication, January 2014, Volume 74, Issue 2, pp 989-1004.

2. Waqar Asif, Hassaan Khaliq Qureshi, Adnan Iqbal, Muttukrishnan Rajarajan, "On the Complexity of Average Path Length for Biological Networks and Patterns", International Journal of Biomathematics 7.04 (2014): 1450038.

3. Waqar Asif, Hassaan Khaliq, Muttukrishnan Rajarajan, Marios Lestas, "Combined Banzhaf & Diversity Index (CBDI) for critical node detection." Journal of Network and Computer Applications 64 (2016): 76-88.

4. Waqar Asif, Marios Lestas, Hassaan Khaliq, Muttukrishnan Rajarajan, "Optimization Based Spectral Partitioning for Node Criticality Assessment", submitted at Journal of Network and Computer Applications.

Table of Contents

List of Figures

Chapter 1

Introduction

The importance of Graph theory was first recognized by Euler in 1736. He used it to identify a suitable path with which a single person could pass through seven bridges in the city of Königsberg exactly once and return to the starting point [31]. Euler not only proved that such a path does exist, but also gave a general solution that could be applied to any arbitrarily arranged landmass and bridge structure. He also identified that the physical distance and the geographical locations of the bridges were not important for identifying the correct solution and what matters is the geometric position of the bridges.

A graph is a mathematical representation of a network which comprises of interconnected components known as nodes with the links between these nodes known as edges. A graph can be represented in a number of different ways: an undirected graph depicts no directional information to the connections whereas, a directed graph denotes the direction of flow of information through the links. Moreover, in binary graphs, the presence of an edge is denoted by a one and the absence of an edge is denoted by a zero, whereas, in a weighted graph the interconnection strength is quantified as weights of the links. Furthermore, the density of connections can range from fully connected graphs which are also referred to as completely connected graphs to very sparse graphs.

A graph can easily depict an abstraction of the reality and this is why graph theory methods have been widely used for understanding a wide range of systems. In a graph theoretic representation, network components are represented in terms of nodes and edges that connect these nodes. In a transport geography most network have an obvious spatial foundation, namely the road and rail networks, which tend to be defined more by their links than by their nodes. This is not necessarily the case for all transportation networks. For instance, maritime and air networks tend to be more defined by their nodes than by their links since links are often not clearly defined. A telecommunication system can also be represented as a network, while its spatial expression can have limited importance and would actually be difficult to represent. Mobile telephone networks or the internet, possibly the most complex graphs to be considered, are relevant cases of networks having a structure that can be difficult to symbolize. However, cellular phones and antennas can be represented as nodes while the links could be individual phone calls. Servers, the core of the internet, can also be represented as nodes within a graph while the physical infrastructure between them, namely fiber optic cables, can act as links. Consequently, all transport/communication networks can be represented by graph theory in one way or the other.

Every graph differs from the other based on the attributes of its individual nodes and edges, where attributes of a node comprise of the nodes location and the attributes of an edge incorporating its length and capacity. These individual components of a network influence their individuality upon the other thus enabling researchers to analyse carefully the characteristics of a network by only monitoring one set of components, either nodes or edges. The interconnectivity of these individual components defines the structure of a network and in the past a lot of research has been done in identifying prominent/vital network structures [21][27][91]. In a multihop Wireless Sensor Network (WSN), nodes are connected using various edges, each having a smaller length, compared to a conventional WSN, for the reduction in transmission energy consumption for the network. Nodes in a network are evaluated based on both their geographical location and the combined influence of all the edges that are connected to that node. The geographical location of a node helps approximate the traffic flow rate through nodes as it is established that a nodes close to the center of the network will experience a higher traffic flow compared to nodes close to the end of a network. The later, on the other hand has its own importance, such as, a node with a higher number of edges is neighbours to a larger number of nodes in the network and therefore, it is critical for ensuring connectivity of the network. More elaboration of this phenomenon is explained later in this thesis.

The combined affect of both the aforementioned attributes defines the importance of a nodes in a network. Due to these attributes, there are a few nodes in a network which when removed result in disconnecting a chunk of the network and thus affect the performance of a network. These nodes are referred to as the articulation points.

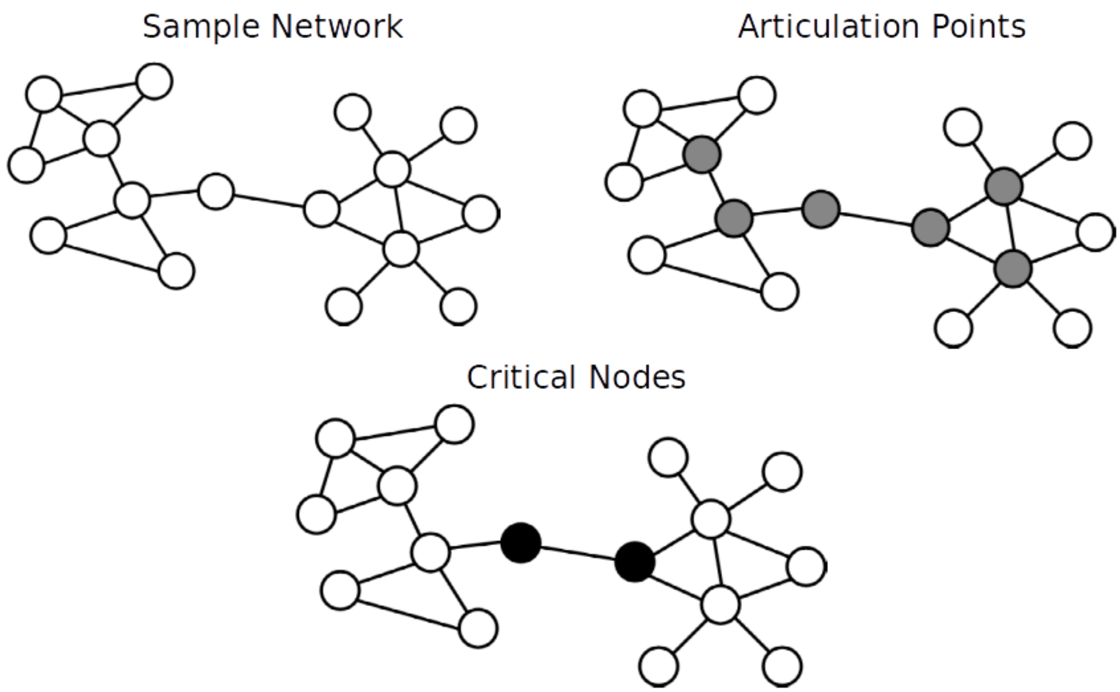


Figure 1.1: Difference in articulation points and critical node.

In the sample network of Fig 1.1, we represent the articulation points in grey color. It is clear from the figure that, removal of these articulation points will render the network disconnected, where we use the term disconnected for a network in which every node is not accessible by every other node in the network. A few of these articulation points have shown to report a higher reduction in the performance of the network and these points which are coloured in black are referred to as the critical nodes of a network.

The identification of these critical nodes is vital for assessing the vulnerability of a network and this is the main motivation behind this thesis. The next section explains in detail the motivation.

1.1 Motivation

Evaluation of node criticality is significant in various complex networks. A few nodes in the network which are referred to as the critical nodes have been shown in literature to have a higher impact on the performance of a network [4][11][52]. This initiates the need for timely identification of these critical nodes for the purpose of timely rectifications and avoidance of any unexpected/unwanted network performance changes.

The importance of critical node identification was reignited when a Georgian woman in march 2011 disconnected 90% of Armenia from the access to the internet by accidentally sabotaging an optical fiber that was passing by her house [11]. She was scavenging for copper to sell as scrap when she came across this cable. Coincidently she had cut the only fiber cable that was connecting 3.2million Armenian people, thus depriving them from the access to the internet for continuous 5 hours. This highlighted the fact that despite the looks of the internet as depicted in Fig 1.2 the removal of a single critical node can have a high affect on the performance of the network.

The influence of critical nodes is not only limited to the internet, but it is also reflected in other fields such as a Peer to Peer Gnutella Network which reported a major network fragmentation after a removal of 4% of the most critical nodes of a network [52] and the North American power grid network which reported a 60% loss of network connectivity upon the removal of only 4% of the nodes in the network [4].

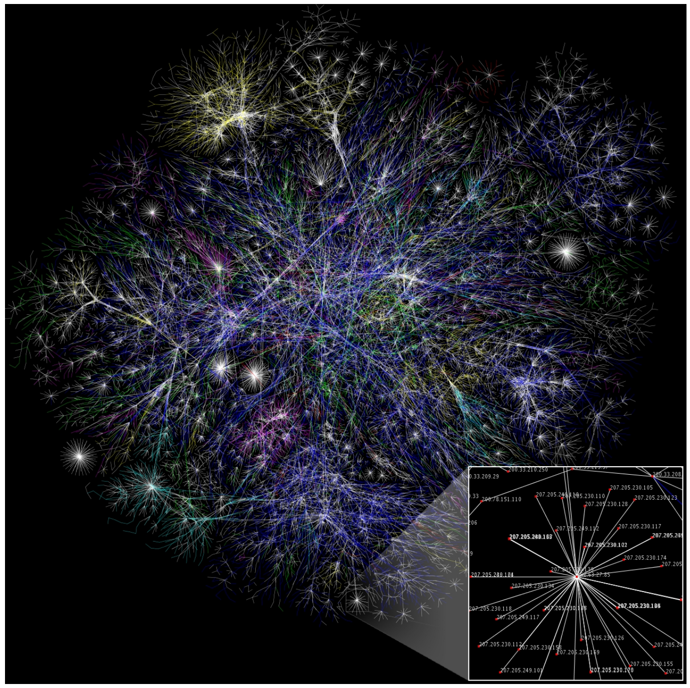


Figure 1.2: Partial map of the Internet based on the date found on January 15, 2005 [72].

Similarly, in transportation networks [66], the need to identify critical node has increased with the ever increasing population which provokes the need for having a better and reliable network. These transportation networks, are prone both to the predictable human intervention and the unpredictable natural disasters such as hurricanes, floods and earthquakes. The more predictable human interventions can cause network blockages due to two broadly defined reason, either a regular network edge between two critical points is observing blockage due to limited link capacity or the transportation network observes occasional network blockages near a couple of famous touristic spots (critical nodes) in the network. In the former scenario, an efficient critical node detection algorithm will help in identifying such a critical link and thus to avoid the blockage, an alternate re-route can be designed that avoids the identified link. In the later scenario, the need of an extra special edge across all the critical nodes of the network can be avoided by efficiently re-routing traffic through edges that are not commonly used by various critical nodes of the network, thus avoiding network blockage. On the other hand, despite the unpredictable nature of the natural disasters, proactive measures can help in improving the pace of the rescue and recovery processes [23]. The proactive identification of critical nodes such as schools and hospitals can aid the rescuers to act quickly by using shortest and the most affective paths and similarly for the reconstruction of an area that has been hit by a natural disaster such as a hurricane, the identification of critical nodes will aid the authorities in deciding as to which roads should be built first.

Likewise, in Telecommunication networks [7], the need to identify these critical nodes has never been more important then now. These days, with the introduction of smart phone for the purpose of increasing connectivity between people and for making life easier, we have also increased the risk of sabotaging our privacy by creating nodes (such as cellphones and tablets) that have all our vital information. A single bug that reaches our smart device can extract vital information such as our credit card details, our home address, can have access to our email and the list goes on. These viruses/bugs travel through our telecommunication network and thus to prevent the spread of such bugs, it is essential to timely identify the critical nodes and suppress their communication and thus avoid spreading these viruses and also maintain normal functionality for the rest of the customers [51]. Similarly, in biological networks [15], the detection of critical nodes can aid in neutralizing potentially harmful organisms such as bacteria and viruses. The interaction of protein with other proteins in a network can be represented in terms of graph theory and it is generally referred to as the protein-protein interaction network. These structures provide vital information for understanding biological structures and thus are widely used for designing drugs [29]. In particular, drugs are designed to affect the minimum cardinality set of proteins (the critical node set of a graph) whose removal will destroy the primal interaction and thus help neutralize the potentially harmful organism. The next section, explains in detail the problem statement of this thesis.

1.2 Problem Definition

Wireless Sensor Networks (WSN)s generally comprise of a large number of intelligent low cost and power constrained devices. These devices relay data between intermediate neighbouring nodes for ensuring data delivery at the destination node. Among these networks, the energy cost of communication is one of the major factors influencing the network energy depletion rate [3]. This rate is directly proportional to the number of intermediate nodes that are participating in relaying the transmitted data, thus in order to reduce the energy depletion rate of the network, reduction in participation of the intermediate nodes is required which should not affect the fault tolerance and reliability mechanism of the WSN. To address this power constraint problem various approaches exist in literature which are broadly referred to as the Connected Dominating Set (CDS) based schemes [108][104][103][73][75][76][74]. The idea behind these schemes is to identify a minimum set of nodes which when connected to each other form the backbone for the complete network. Despite the fact that this is known to be a well suited technique for reducing the energy depletion rate of a network, this also increases the number of articulation points in a network, thus initiating the need for timely identification of critical nodes. As highlighted earlier, the identification of critical nodes is essential for accessing network vulnerability and for this various aforementioned approaches exist in literature.

Some of the existing algorithms are based on intuition, whereas others are based on mathematical abstractions of networks of arbitrary topology and are thus characterized by properties which can be verified analytically prior to implementation. Most of these approaches either identify critical nodes based on the affect of a node on the traffic flow pattern of the network or they use the topological structure of the network to identify these critical nodes. To the best of our knowledge, no such algorithm exists in literature that identifies critical nodes based on both the topological structure and the traffic flow pattern of the network. To address this problem, this thesis proposes two metrics, the first is based on intuition and it uses a newly defined node diversity metric which incorporates the weighted node degree and the variation in link length capability of a node to address the topological properties of a network. The weighted node degree metric is a slight variant of the well know degree centrality metric [35], the major difference lies in the evaluation of the degree of a node based on the number of new nodes that are introduced by a particular node if it is accessible in the network. The variation in link length metric originates from [10] which evaluates the affect of Average Path Length (APL) of a network. The variation in link length metric evaluates the diversity of a network by using the difference in path length that a node is maintaining, the intuition behind this approach is that a node that connects multiple nodes at varying distances is highly likely acting as a bridge node among various nodes in the network thus, it is probable that by removing that node the network will report a higher degradation in performance. The traffic flow pattern on the other side is incorporated in this critical node evaluation metric with the use of the Banzhaf power index, it is a slight variant of the well known betweenness centrality metric [35] and was previously used for weighted voting games.

The second metric is based on pure mathematical abstraction where we formulate the critical node identification problem in the form of an optimization problem where the objective is to identify a node that when removed has the highest impact on both, the algebraic connectivity of the network and the maximum traffic flow of the complete network. Here, the first part of the optimization problem deals with the topological properties of the network and the second part deals with the traffic flow of the network, thus addressing both sides of the problem. More detail on both these metrics are explained in Chapter 5 and 6 respectively.

1.3 Research Objectives

The objective of this research is to develop a new model that can correctly identify critical nodes in a network. The identified node, upon its removal, should:

- Increase the average path length of the network, thus increasing the time taken for nodes to communicate with each other.

- Reduce the Algebraic connectivity of the network, which means that the network is loosely connected and the removal of a few nodes will result in network partitioning. These few nodes that are holding the network together are the ones that will create bottleneck for the complete network.

- Increase network congestion and probability of collision thus reducing the network throughput and increasing per packet delay of the network.

Furthermore, the objectives include:

- The design of a distributed algorithm that can correctly identify the most critical node of a network without the need of a centralized monitoring body. This will aid in implementing this algorithm in complex networks such as, Wireless Sensor Network (WSN), Road networks, Communication networks and various other large sized complex network for the assessment of network vulnerability.

- The distributed critical node identification algorithm should be computationally less complex, thus increasing the possibility of its implementation in computationally complex networks.

1.4 Research Method

In order to identify the most critical node in a network, it is essential to identify the right metric that can comprehend the cumulative influence of most of the individual attributes of a node in a network. This thesis uses the node attributes in a network to evaluate various metrics. This selection is based on the consideration that the edge attributes are reflected in the node attributes of the nodes that are connected through that edge. A well known metric that reflects the node attributes of a network is known as the Average Path Length metric. The Average Path Length metric reflects the average time it takes a message to move from one node to any other node in the network. This thesis first emphasises on the existing approaches for estimating the Average Path Length of a network as it is known to be one of the major influencing factor for node criticality and then proposes a new approach that reduces the time complexity of calculating the Average Path Length (APL) of complex networks.

Later, this thesis highlights the affects of changing the Average Path Length of a network and propose a new methodology for its reduction. The new methodology uses a Variable Rate Adaptive Modulation (VRAM) scheme on top of a Neighbour Avoiding Walk (NAW) mechanism for reducing the Average Path Length using the same transmission power. This helps in building an intuition based metric for the identification of critical nodes in a network. The intuition based critical node identification metric is referred to as the Combined Banzhaf & Diversity Index (CBDI). The Diversity index in CBDI originates from the Neighbour avoiding walk mechanism discussed in the APL reduction mechanism and the Banzhaf Power index in CBDI is a variant of the well known betweenness centrality metric. The CBDI mechanism is tested using simulations and it has shown to perform well in identifying critical nodes in a network.

The intuition based CBDI metric lacks in providing mathematical ground about the way that it works and for this a new critical node identification metric is proposed that is the resultant of the suboptimal solutions of two optimization problems. The critical node identification metric originating from these suboptimal solutions is tested through simulations and analysis. These suboptimal solutions have shown to perform well in identifying the most critical node in the network and they are used to formulate a critical node identification algorithm which is also among the contributions of this thesis.

1.5 Contribution

In this thesis, a new mathematical model is presented that evaluates the Average Path Length of a tree structured network. This is an advancement upon the existing approaches that require tedious computation of all the possible paths in a network for the approximation of the average path length of a network. This contribution is also accompanied by a new approach for the reduction of the average path length of a network which can be used in various network scenarios for the introduction of small world network phenomenon into comparatively large networks.

The contribution of this thesis also incorporates the introduction of a network distributed critical node identification metric which is the outcome of the suboptimal solutions of two well known optimization problems. This thesis also presents a mathematical formulation that identifies the algebraic connectivity of the resultant network after critical nodes are removed from the network. Along with this, a deviation of the degree centrality metric is also proposed which is referred to as the weighted degree centrality metric and is shown through analysis and simulation that it is a better metric than the conventionally used degree centrality metric.

1.6 Thesis Structure

Chapter 1: Introduction This chapter provides information on the context of the research in hand along with the focus of the research work. It also highlights the aims and objectives of the research work.

Chapter 2: Related Work This chapter explains in detail the existing work that relates to the work in this thesis and highlights the deficiencies of the existing work that had initiated the need for this work.

Chapter 3: Average Path Length Calculation For Complex Tree Structures This chapter describes the conventional approaches used for calculating the APL of a complex topology and then proposes a simpler approach, that reduces the computational complexity of calculating the APL of a complex structure.

Chapter 4: Average Path Length and Network Performance This chapter highlights the affects of changing the APL of a network and in it we propose a new mechanism for reducing the APL.

Chapter 5: Intuition Based Critical Node Identification Approach This chapter elaborates on the importance of critical node detection and propose a new intuition based metric for identifying the most critical node in the network.

Chapter 6: Optimization Based Spectral Partitioning for Node Criticality Assessment This chapter discusses the use of optimization theory for the identification of critical nodes in a network and with the aid of this theory we propose a new algorithm that can identify critical nodes in any arbitrary network.

Chapter 7: Conclusion and Future Work This chapter concludes this thesis and presents the future direction of work of this domain.

Chapter 2

Related Work

2.1 Introduction

A number of approaches have been proposed in literature for the identification of these critical nodes in a network. These approaches can be broadly categorized into two categories namely the connection based approach and the topology based approach, where the former uses the information flow pattern of the network to identify the most critical node and the later uses the topological structure of the network to identify the most critical node in the network.

2.2 Connection based schemes

The connection based approaches identify the criticality of a node based on the information flow pattern of a network. The information flow pattern in a network highlights the data flow rate through each individual node and also enables in identifying the node that can be the cause of a potential bottleneck in the network. Both of these parameters play a key role in identifying node criticality and a number of approaches exist in literature that use the information flow pattern of a network to identify the criticality of a node. This section highlights a few well known approaches that are later referred to as the connection based approaches in this thesis.

2.2.1 Average Path Length metric

The average path length metric is among the very widely used metrics and it is also referred to as the characteristic path length metric of a network [45]. This metric uses the sum of the shortest path of every node to every other node in the network for the identification of the most critical node in the network. In a graph $G = (V, E)$, where V is the set of vertices and E is the set of edges, the characteristic path length is defined by:

$$l \equiv d(v, w) \equiv \frac{1}{N(N-1)} \sum_{v \in V} \sum_{w \neq v \in V} d(v, w) \tag{2.1}$$

where, $d(v, w)$ is the geodesic distance between v and w with $v, w \in V$, i.e., the cumulative distance of all the edges that lie in the shortest path between the two nodes and the factor $1/N(N-1)$ is the one over the total number of pairs of vertices. In such a network, a larger value of l represents a relatively larger time for the message to be disseminated inside a network whereas, a smaller value of l denotes a tightly bonded network where nodes are placed close to each other. The average path length metric identifies such a node as the most critical node which has the highest influence on the average path length of the complete network. It is easily relateable that the node with the shortest path length to every other node in the network, will have the highest influence on average path length of the network where, the average is computed using eq 2.1.

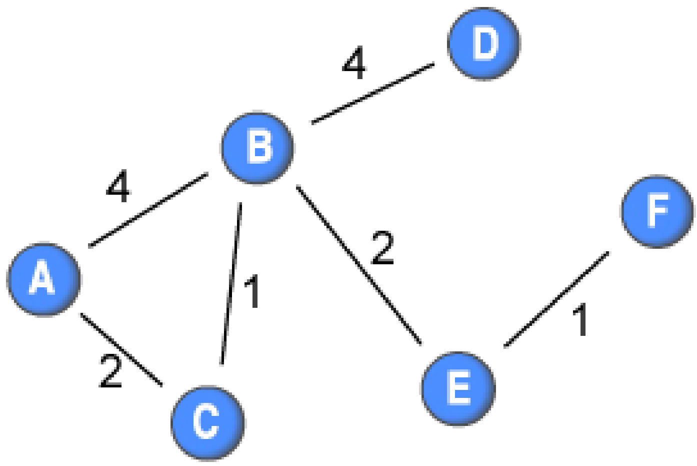


Figure 2.1: Weighted sample network for accessing shortest path length metric.

The sample network in Fig 2.1 shows an undirected weighted network of six nodes where, the weights represent the length of an edge. The shortest path length metric calculates the distance of every node to every other node in the network and then the node that has the shortest path length among the whole network is referred to as the most critical node in the network. The shortest path lengths for the sample network are shown in the symmetric matrix of table 2.1.

It is clear from the table that node B has a shortest distance of 14 units from all the nodes in the network, thus it is assumed to be in the center of the network and the most accessible node in the network. Removing such a node will thus increase the average path length of the network and this makes it the most critical node in

Table 2.1: Path length matrix for Fig 2.1

	A	B	C	D	E	F
A	-	4	2	7	5	6
B	4	-	1	4	2	3
C	2	1	-	5	3	4
D	7	4	5	-	6	7
E	5	2	3	6	-	1
F	6	3	4	7	1	-

the network according to this average path length metric.

2.2.2 Closeness Centrality metric

Another well known approach that has been in consideration for a long time is the closeness centrality metric [35]. This metric identifies the criticality of a node by analysing the total distance of one node with all the nodes in the network and thus a node that has the lowest total distance and therefore is closer to all the nodes in the network is thus considered as critical in the network. The phenomenon behind the use of this metric is that a node closer to all the other nodes in the network will eventually have the highest network traffic flow through it, as it can reach maximum nodes in the network with the shortest distance. In order to calculate the closeness centrality of a node, researchers use the reciprocal of the total distance from a particular node to all other nodes in a network [12]:

$$CC(v) = \frac{1}{\sum_{u \in V} d(v, u)} \tag{2.2}$$

Unlike the average shortest path metric which is defined as the average distance of the whole network, the closeness centrality metric is a node specific metric, it identifies how close each individual node is to the rest of the network nodes. Fig 2.2 shows a sample network of 34 nodes where the criticality of the node is represented with both color and size of the node. A bright red node with the biggest size is considered as the most critical node in the network. As expected from the definition of the closeness centrality metric, the nodes close to the center of the network have a higher closeness centrality among all the nodes in the network.

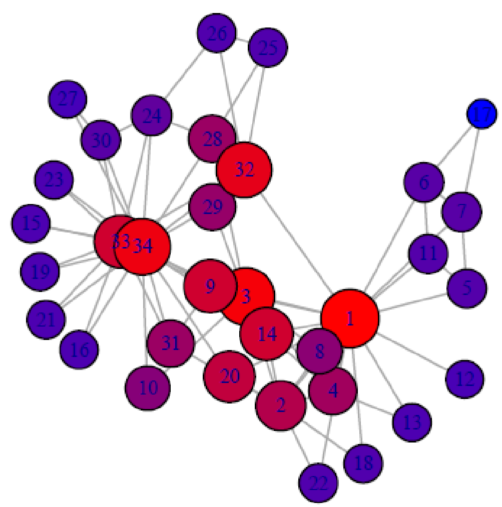


Figure 2.2: Sample network representing nodes with the highest closeness centrality [1].

2.2.3 Betweenness Centrality metric

The betweenness centrality metric was originally proposed by Freeman in his seminal paper [34] and since then it has been used by various researchers for identifying critical nodes in a network [4][12][68]. This is also a shortest path enumeration based metric and it identifies the most critical node based on the number of shortest paths that a node participates in, a node that participates in the highest number of shortest paths will have the highest influence on the performance of the network upon its removal and thus it is considered as the most critical node in the network. Let $\delta_{uv}(x)$ denote the fraction of shortest paths between node u and v that pass through node x, then [12]:

$$\delta_{uv}(x) = \frac{\sigma_{uv}(x)}{\sigma_{uv}} \tag{2.3}$$

The betweenness centrality of a vertex x is then defined as [12]:

$$BC(x) = \sum_{u \neq v \neq t \in V} \delta_{uv}(x) \tag{2.4}$$

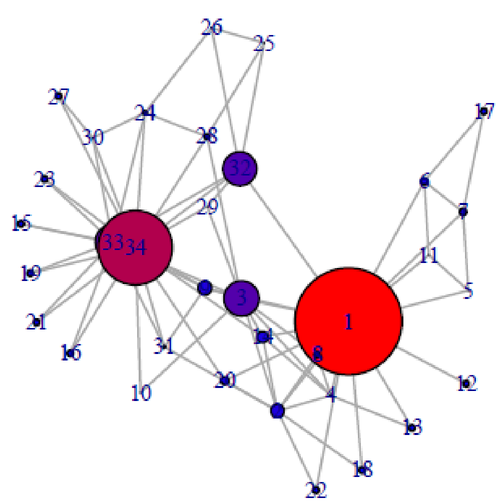


Figure 2.3: Sample network representing nodes with the highest betweenness centrality [1].

The betweenness centrality of a node measures the control of a node on the overall communication in a network, and it is therefore used to identify critical nodes in a network. A higher centrality index indicates that a node lies on a large number of shortest path routes and thus by its removal the network will face a greater decrease in the average network traffic flow rate. Fig 2.3 shows in red the nodes that participate in maximum shortest path routes in a network of 34 nodes. The size of the node reflects its importance in the network and therefore the node with the largest size and the brightest red color is referred to as the most critical node in the network based on the betweenness centrality metric.

2.2.4 Ego centrality metric

A slight variant of the betweenness centrality is the ego centrality metric [19][36]. The ego centrality metric was designed for a special class of graphs that are known as the centred graphs [36], these graphs are in a star structure and thus restrict nodes from either having a direct link with the neighbour or a path of 2 hops between any two nodes in the network. The ego centrality metric takes benefit of this graph structure and determines the criticality of a node based on the number of times a node participates in forming this two hop path between any two nodes. This definition is in line with the previously defined betweenness centrality metric but the major difference lies in the network structure type. As the ego centrality metric was mainly defined for the star network, thus the maximum length between two nodes of a graph cannot exceed two hop counts [36].

2.2.5 Network traffic flow metric

Nasiruzzaman et al. [67] on the other hand believe that it is not necessary that all real life networks use the shortest path routes to relay traffic/messages. Instead they propose a new metric which is build on the phenomenon that the traffic flow pattern is a better estimation metric for the evaluation of critical nodes in a network. Therefore, their proposed approach considers a node to be critical if it observes a higher traffic flow through it. Let F_a be the net maximum power flowing through node a in the network with source node $s \in S$ and load node $l \in L$. Then F_a is defined as:

$$F_a = \sum_{s \in S} \sum_{l \in L} F_a^{sl} \tag{2.5}$$

where $s \neq l \neq a$. Also let, F_n be the net maximum power flowing through the network with the source node $s \in S$ and load node $l \in L$, which is defined as:

$$F_n = \sum_{s \in S} \sum_{l \in L} F_n^{sl} \tag{2.6}$$

The ratio of these two powers could be used to measure the importance of a node and this ratio is called the flow betweenness. This flow betweenness is defined as:

$$C_B(a) = \frac{F_a}{F_n} \tag{2.7}$$

With this approach, a node that has a relatively higher flow betweenness in the network is then considered as the most critical node in the network.

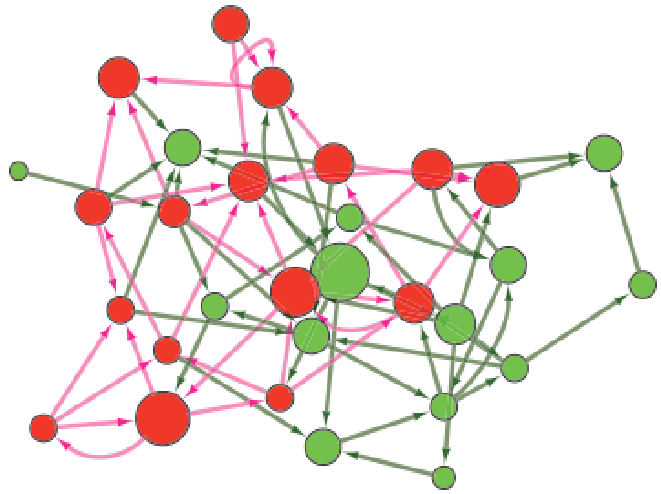


Figure 2.4: Sample network representing nodes with the rank of each node in the network [59].

2.2.6 The Rank matrix

Another approach that exists in literature is the rank matrix approach [59][55]. This matrix uses the traffic that passes through a node to form a $N \times N$ matrix to evaluate the most critical nodes in the network. Unlike previous approaches, this metric identifies a set of critical nodes whereas, the previously stated approaches can identify a single most critical node in the network. In this approach, the minimum number of nodes that report a full rank of $N \times N$ matrix of the network are reported as the most critical nodes. Here the $N \times N$ matrix represents the traffic on the link between nodes in the network. Fig 2.4 represents a network with multiple nodes where, the size of a node represents the degree whereas, the color represents the criticality. Nodes in red are the ones that have the highest influence on the rank of the network. As per the rank matrix, the node that has the highest degree and has the most influence on the rank of the matrix is considered as the most critical node in the network, this means that the larger red nodes are the most critical nodes in the network.

2.3 Topology based schemes

The topology of a network refers to the arrangement of nodes and their interconnection through edges. These topology based schemes have always been of keen interest to researchers when it comes to network where there is no relative traffic flow such as, social networks. To tackle this phenomenon of network structure and to understand node criticality based on this structure, various approaches have been proposed in the literature. This subsection highlights a few of these approaches that are highly relevant to the work presented.

2.3.1 Degree Centrality metric

Among all the topology based approaches, the most widely used approach is the degree centrality metric [12][35]. The degree centrality metric as obvious form the name, uses the degree of a node to identify the most critical node of a network. The node that reports the highest node degree is thus referred to as the most critical node of the network. The key idea here is that, a node with a higher node degree is neighbours to more nodes in the network and thus by removing that particular node a higher number of non-neighbouring nodes will loose connection with each other. Fig 5.3 shows a graph of 34 nodes with the size and color of a node representing the criticality of a node in a network based on the degree centrality metric. It is evident from the definition of the degree centrality metric that the most critical node will lie in the center of the network and that is also depicted in Fig 5.3.

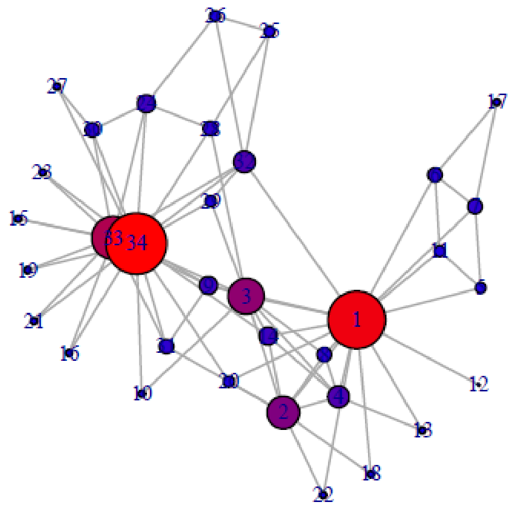


Figure 2.5: Sample network representing nodes with the degree of each node in the network [59].

2.3.2 Bonachich metric

Bonachich et al. in [16] improvised on the degree centrality by proposing a new power measure and then connecting it with a modified degree centrality measure to obtain a better centrality metric. Bonachich metric is build on the phenomenon that, the neighbours of a node play a vital role in determining its importance in a network. A node whose neighbours are connected to less neighbours makes the particular node more powerful as it is likely that the node under consideration is the reason that its neighbours are connected to multiple nodes in the network. Therefore, a node whose neighbours are less connected makes that node more powerful as, by its removal the neighbouring nodes will lose connectivity. On the other hand, if you are connected to more neighbouring nodes then this makes you more central and less powerful thus, the identification of node criticality requires a trade off between node power and centrality. Fig 2.6 shows a network of 34 nodes with the colors and size of the nodes representing the criticality of a node. It is worth mentioning that the modifications that Bonachich et al. proposed has identified a different node as compared to the one that was pointed out by the degree centrality metric.

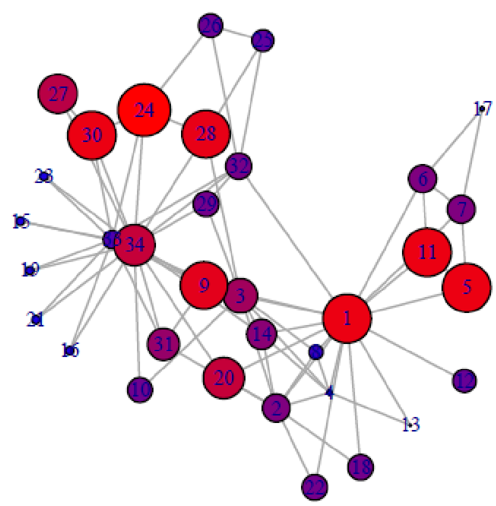


Figure 2.6: Sample network representing nodes with the highest bonachich centrality [1].

2.3.3 Eigenvector Centrality metric

Another approach that exists in literature is the eigenvector centrality [17][107]. Eigenvector centrality is a measure of the influence of a node in a network. It assigns relative scores to all the nodes in a network based on the concept that connections to high scoring nodes contributes more to the score of a node when compared to equal connections of low scoring nodes. For a given graph $G = (V, E)$ the adjacency matrix

$A = (a_{v,t})$ will have $a_{v,t} = 1$ if node v is linked to node t and zero otherwise. The centrality score of node v is defined as:

$$x_v = \frac{1}{\lambda} \sum_{t \in M(v)} x_t \tag{2.8}$$

where $M(v)$ is a set of the neighbours of v and λ is a constant. With a small rearrangement this can be rewritten in a vector notation as the eigenvector equation:

$$Ax = \lambda x \tag{2.9}$$

In general, there will be many different eigenvalues λ for which an eigenvector solution exists but considering the additional requirement of all positive eigenvectors only the highest eigenvalue reports the desired result.

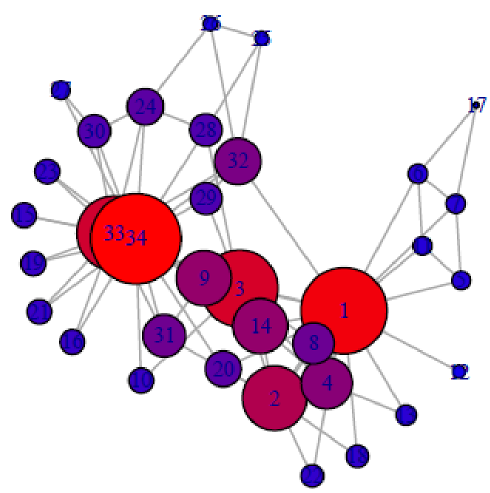


Figure 2.7: Sample network representing nodes with the highest eigencentrality. [1].

Fig 2.7 reflects the most critical node in the network with aid of size and color. the brightest red coloured node with the biggest size is represented as the most critical node in the network.

2.3.4 The HILPR metric

In the Hybrid Interactive Linear Programming Rounding (HILPR) algorithm [82] Yilin et al. propose a different approach of defining node criticality based on the pairwise connectivity of the resultant network after the node removal. They emphasise that the node pair whose removal leads to the most balanced disconnected components and ensures the non-existence of giant components will result in the highest degradation in the performance of the network and thus should be ranked as the most critical node of the network. A similar approach is followed in the GREEDY Critical Node Detection Problem approach (GREEDY-CNDP) [92] and the $\beta - disruptor$ approach [28], both of which propose an efficient algorithm to minimize pairwise connectivity upon removal of k nodes from the network. Another approach that exists in literature is the the algebraic connectivity metric [32][58][57], which is also the focus of this work and is explained in detail in later chapters. The phenomenon here is that the algebraic connectivity is known to be a well defined connectivity metric for a network, therefore to identify a critical node, it is vital to identify the node that reports the highest reduction in the algebraic connectivity of the network. The node that reports the highest reduction in the algebraic connectivity of the network will thus be identified as the most critical node of the network.

Chapter 3

Average Path Length Calculation For Complex Tree Structures

WSNs generally comprise of a large number of intelligent low cost and power constrained devices. These devices relay data between intermediate neighbouring nodes for ensuring the delivery of data at the destination node. Among these networks, the energy cost of communication is one of the major factors influencing the network energy depletion rate [3]. This rate is directly proportional to the number of intermediate nodes that are participating in relaying the transmitted data, thus in order to reduce the energy depletion rate of the network, reduction in participation of the intermediate nodes is required which should not affect the fault tolerance and reliability mechanism of the WNSs. One such known strategy is of forming a Connected Dominating Set (CDS) based Topology Control (TC) scheme.

TC consists of two components: *topology construction* mechanism, which finds a set of backbone nodes to work on behalf of rest of the nodes while maintaining network connectivity and coverage, and *topology maintenance* mechanism, which changes the role of backbone nodes for uniform distribution of resources. Both these mechanisms work in an iterative manner until the network is depleted, thus together they increase the network life time when compared to a continuously running WSN without TC mechanism [111]. In CDS based TC schemes, only the backbone nodes are responsible for relaying messages over the network. The non-backbone nodes can thus turn off their transceiver and hence save energy. The backbone or a CDS size is a critical parameter, since it has been manipulated in many different ways. It has been seen that most researchers reduce the size of backbone, which they argue provides better reliability as the hop count gets reduced among backbone nodes. On the other hand, the reduction in the size of the backbone causes only few nodes to work on behalf of rest of the nodes thus forcing them to deplete their energy more quickly and hence reducing the network lifetime. Various approaches exist in literature that address the problem of reducing the energy depletion rate of a network. In [5],[94] distributed algorithms for constructing CDSs in unit disk graphs (UDGs) were first proposed. These algorithms consist of two phases to form a CDS. First they form a spanning tree and use it to find maximal independent sets (MIS), in which all nodes are coloured black. In second phase, some new blue coloured nodes are added to connect the black nodes to form a CDS. Likewise Zeng Yuanyuan et al. in [108] proposed Energy Efficient CDS (EECDS) algorithm which follows a two phase TC scheme in order to form a CDS based coordinated reconstruction mechanism to prolong network lifetime and balance energy consumption. Similarly Jie Wu et al. in [104] proposed a two phase TC scheme that uses marking and pruning rules for exchanging neighbours list among a set of nodes. In CDS Rule K [104] a node remains marked as long as there is at least a pair of unconnected nodes in its neighbours; it is unmarked when it finds that all its neighbours are covered with high priority. All the above studies focus on increasing the network lifetime by forming a reduced topology but, they do not analyse the impact of a reduced topology on network reliability.

Network reliability is assured by Lanny Sitanayah et al. in [84] by adding extra relay nodes in a *single tiered* network. In a *single tiered* network all nodes forward packets directly to each other instead of relaying it through the backbone node. Similarly Han et al. in [43] provide reliability in full fault tolerant and partial fault tolerant environment for heterogeneous wireless sensor networks. They ensure reliability by adding extra relay nodes with an assumption that, relay nodes use the same transmission radii while sensor nodes have different transmission radii. Both these algorithms inherently add overhead by adding extra relay nodes in a network. This results in extra node energy and reduces network lifetime. Hence, an algorithm was required that, while keeping in consideration the energy constraint, ensures reliability for the complete network among every set of backbone nodes.

This thesis limits the participation of these nodes in a network, by defining Poly3 which is a further refinement of an earlier work proposed by H.K.Qureshi et al. in [75]. Poly3 reduces the energy depletion rate and simultaneously adds reliability on the tree based topology construction algorithms for WSNs by forming cliques of size

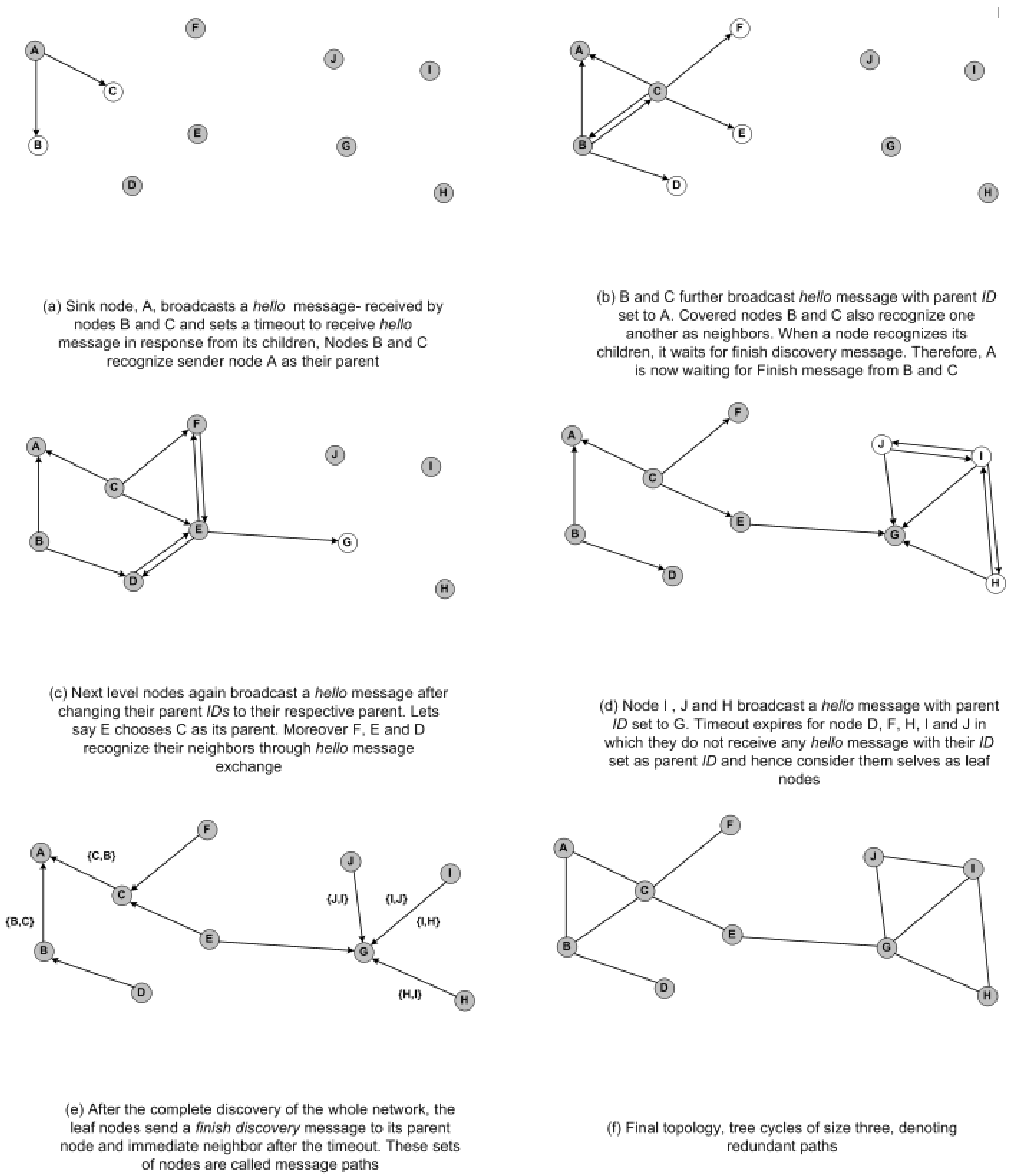


Figure 3.1: The Poly3 Algorithm.

three – a tunable parameter – which is maintained throughout the network.

3.1 The Poly3 algorithm

The Poly3 algorithm provides a solution to the network wide reliability problem in mission critical WSNs. Poly3 assumes no prior information about the position or orientation of the nodes, so the geometrical view of the topology is not visible to the nodes. The subsequent subsection explains in detail the topology construction phase of Poly3.

3.1.1 Topology Construction

Topology construction phase in Poly3 is subdivided in to three phases. In the first phase, a backbone based on CDS formulation is created. In the second phase, nodes send their neighbors list to the sink node, which they maintain during the first phase. In the last phase, which is a tunable phase, cliques of size three are retained. It is worth noting that during this phase few nodes also become active – if there are any – during the retention of the three clique set. The topology construction phase of Poly3 is similar to Poly [75] except for the last step in which instead of a single polygon, multiple cliques of size three are retained.

The backbone construction phase in Poly3 is started by a randomly selected initiator node. The selection is dependent on the criteria that the node with the largest ID persists in case more nodes initiate the construction process. To start the process, the initiator node broadcasts Hello message in its communication area. The Hello message lists the parent ID of sending node. For sink node it is empty since the sink node is assumed to be parent of all nodes.

For the elaboration of the algorithm, we take a sample network shown in Fig 3.1. It is supposed that node A in Fig 3.1 initiates the backbone construction process by broadcasting the Hello message. It also sets a time out period for receiving the replies from any of its children. The broadcasted Hello message is received by node B and node C, which lie in the communication range of node A. After the reception of node A, both node B and node C rebroadcast the same message while only changing their parent ID, which is now set to node A. The messages by node B and node C are also received by node A which helps identifying node A that it has been chosen as a parent node. Once this process is completed, nodes B and C are considered as covered and thus causing node A to become active. Node A now waits for finish discovery message from its children. At this stage, for the sake of clarity, we assume that contention mechanism is available in case if messages by different nodes are received at the same instance of time. On the other hand, when uncovered nodes receive the message, they set the sender as their parent and repeat the same process. It is also worth noting that the reception of Hello message starts the process of maintaining a neighbors list until the whole network is covered.

These nodes now rebroadcast the Hello message with A as their parent node and set their own timers for receiving responses from their children nodes. This re-broadcasted Hello message is also received by parent node A, which in turn identifies sender as its children nodes. Once identified these nodes are considered as covered, the parent node switches to an active state and starts waiting for finish discovery message from its children. When an uncovered node receives Hello message it sets the sender as its neighbor. In this way, the CDS creation nodes find their neighbors and the process is repeated until the whole network is covered.

As shown in Fig 3.1, the message sent by node B and node C is received by their neighbors, which repeats the same process until Hello message arrives at leaf nodes i.e. nodes H, I and J. These nodes also repeat the same process but the expiry of the time out allows them to send a Finish Discovery message back to their respective parent nodes. In Finish Discovery message, nodes send the list of their neighbors to the parent node, thus starting the second phase of the algorithm. The parent node receiving the Finish Discovery message repeats the same process in the backward direction until the message is received at the sink node, which is the parent of all nodes. In this way, the Finish Discovery message converges towards the sink node.

After the reception of the finish discovery message at the sink node, the third phase of the algorithm starts. In this phase, the sink node compares the message paths visible from the neighbors list for the construction of clique set of size three for reducing the message complexity. The comparison is based on the fact that the nodes common between message paths lead towards a clique of size three i.e. message path G, I and J and message path G, J and I have two nodes in common. In addition, both paths comprise of the same parent node and therefore allowing forming a clique of size three. Once the clique set is chosen, the sink node creates the final topology by broadcasting the Create Topology message. Paths which have nodes C and B in common and both the paths are initiating from node A hence they form a polygon of size three as shown in Fig 3.1. As mentioned earlier, that the reliability is a tunable parameter, therefore for the sake of this purpose we created a bound on the third phase of the algorithm. During this phase, if desired, one can set the number of three cliques that are required in the final topology. By doing this, the complexity gets increased but at the sake of required level of reliability and energy efficiency which is now dependent on the number of active clique set which contains the list of nodes that are part of the polygons.

When a node receives create topology message from sink node it checks if its name is in the list of active nodes, if it is in the list, it sets its state to active. At the end of this process, each node is in either active or sleep mode. The set of active nodes act as a communication backbone for the network. To better understand the benefit of this approach, the next section explains in detail the parameters that influence the reliability of a network.

3.2 Network Reliability

Network Reliability has been defined in two ways namely packet delivery reliability and link redundancy. The former is dependent on path length among active set of nodes and the second is dependent on number of extra links used throughout the network. This section explains in details different notations associated with the metrics and also presents a comparison of Poly3 on both set of performance metrics.

- Packet Forwarding Probability: Packet forwarding probability (P_f) is defined as, the probability that a packet will be successfully delivered to the next hop in the path length between the source and the destination node. The packet forwarding probability is the product between the probability of not having a collision at the MAC layer P_c and the probability that a packet is not lost due to channel errors (P_e), and is given by:

$$P_f = P_c P_e \tag{3.1}$$

- Average Path Length: Average path length is defined as the mean of the shortest path lengths between all pair of vertices and it represents how quick information transfer can be done in a network. It is given by:

$$l = \frac{1}{n(n-1)}[\sum_{i,j} d(v_i, v_j,)] \tag{3.2}$$

Here n represents the number of nodes/vertices in a network and d is the distance between nodes i and j for all pair of active nodes in the network.

3.2.1 Packet Delivery Reliability

Most of the tree based solutions ensure that every pair of nodes is connected to each other through at most one path. Hence, a packet sent from node A to node D can have only one path in order to reach the destination. As a result, the tree based algorithms are not viable since the network is prone to failure and can be decomposed into two or more disjoint components. On the other hand, reducing the path length with varying

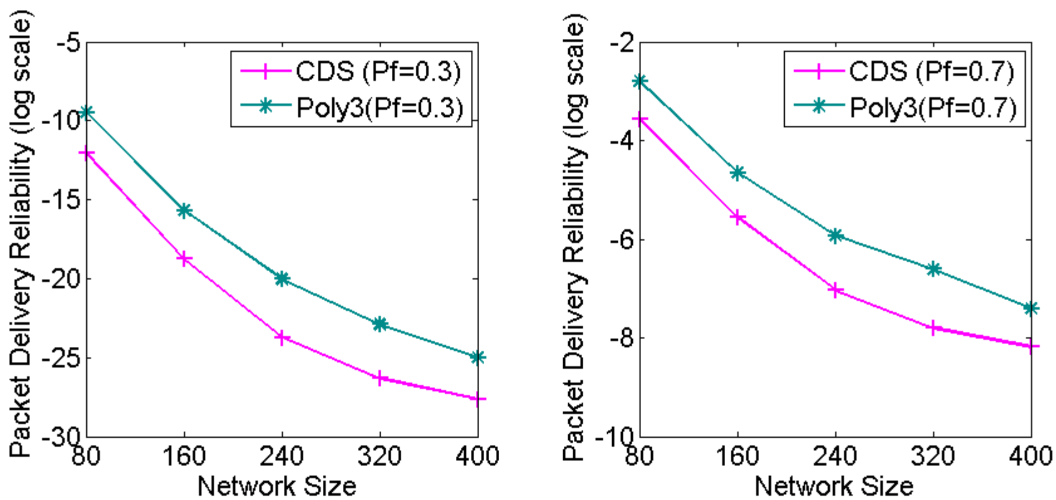


Figure 3.2: Packet Delivery Reliability for $P_f = 0.3$ and $P_f = 0.7$.

node density among set of backbone nodes provides a solution to increase the packet delivery reliability. Therefore, the packet delivery reliability is given by:

$$R(P_f, l) = P_f^l \tag{3.3}$$

The possibility that the packet will be received by the destination node is dependent on the path length among set of backbone nodes, since they are responsible for relaying information towards the sink node. In order to address the Packet Delivery reliability, Poly3 forms a clique set of size three which provides polygenic redundancy while also helping reducing the path length among set of nodes in the network. It is due to the reason that high degree backbone nodes get connected with other bunch of nodes, thus reducing the overall path length.

Fig 3.2 shows the Packet Delivery Reliability of Poly3 and Tree based CDS algorithms. In order to see the impact of increasing path length, the results are computed by varying the node density up to 400 nodes. In addition, different WSN applications can have different packet forwarding probability due to the vagaries of communication, therefore, the results are computed for $P_f = 0.3$ and $P_f = 0.7$. Results were computed under the Network Analyzer tool available as a plugin in Cytoscape [85]. It is evident that increase in node density increase the path length, however, Poly3 provides better Packet delivery reliability due to the fact that backbone nodes are connected in the form of many cliques set.

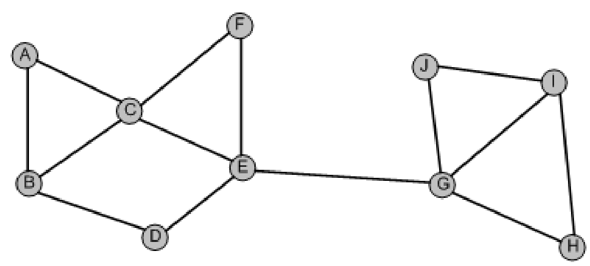


Figure 3.3: A sample network.

3.2.2 Link Success Reliability

The redundancy in graph theory is defined as the expected number of spanning tree that are functional [24]. Due to this reason, removal of a single edge in a spanning tree leads to a graph of many disjoint components. Therefore, all individual edges play a key role for the successful delivery of data. The tree based algorithms based on CDS forms a backbone, which is also a tree, therefore, the lack of non-identical spanning tree under dynamically changing conditions exposes the algorithms for mission critical applications. On the other hand, failure of a link triggers the topology maintenance algorithm again and again and hence putting constraint on energy stringent WSN devices. It is therefore very important that the topology is constructed in a robust way, which to certain extent also helps in achieving energy efficiency under topology maintenance.

Reliability, which is associated with redundancy, is defined as the probability that there is at least a functional spanning tree or a connected network under random link failures. Therefore, the more the redundancy in the network, the more is the reliability in the network. However, for WSNs, the level of redundancy is dependent on the energy efficiency that is required in most of the application scenarios. To demonstrate the performance of Poly3, consider a sample network shown in Fig 3.3 for which the reliability is computed using the Linear Algebra package available in Maple [2].

Let $B = (b_{i.j})_{n.n}$ be the adjacency matrix of the graph G, then

$$b_{i.j} = \begin{cases} 1 & \text{if vertices } v_i \text{ and } v_j \text{ are adjacent,} \\ 0 & \text{otherwise.} \end{cases}$$

The degrees of the vertices are represented by a diagonal matrix. If $D = (d_{i.j})_{n.n}$ denote the diagonal matrix of graph G, then

$$d_{i.j} = \begin{cases} deg(v_i), & \text{for } i = j, \\ 0 & i \neq j. \end{cases}$$

The matrix tree theorem [2] when used identifies that the spanning trees of a graph G is the value of the cofactor of a matrix, i.e. $T = D - A$. Therefore, the matrix T for the assumed network equals

$$T = \begin{bmatrix} 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 \\ -1 & 0 & 3 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 4 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 3 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & -1 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & 4 \end{bmatrix}$$

The cofactor of a matrix T equals 24, which means that there are 24 possible combinations of spanning trees. These combinations represent the total redundancy in the network. However, to demonstrate the reliability, the interest lies in measuring the probability that network remains connected under random link failure. To compute this, all the spanning trees are represented as a disjoint product which is given below:

$$P(t_1 \vee t_2 \vee t_3 \vee ...... \vee t_{24}) = P(t_1) + P(t_2\overline{t_1}) + P(t_3\overline{t_2 t_1}) + \\ \ldots + P(t_{24}\overline{t_{23} t_{22}}....\overline{t_1}),$$

where t is a spanning tree in the network.

If all the edges have the same reliability $P_1 = P_2 = ... = P_n = P$, then, the reliability of the network shown in Fig 3.3 is given by: $24p^9 - 49p^{10} + 34p^{11} - 8p^{12}$. The adjacency matrix for all tree based CDS algorithms remain the same as all these algorithms maintain a single spanning tree.

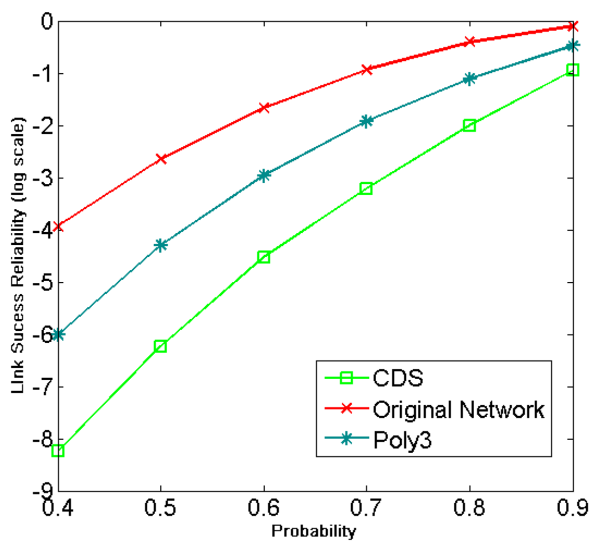


Figure 3.4: Link Success Reliability.

Fig 3.4 compares Poly3 algorithm with CDS tree based algorithm. It also draws the link success reliability of the original sample network shown in Fig 3.4. The results were computed by varying the probability up to 0.9 and by inserting them in the equation computed previously. The results show that Original Network provides better link success reliability because all the links are functional. However, taking up this sort of a network further would impact on the energy. On the other hand, Poly3 provides better reliability when compared with CDS algorithms. It is due to the fact that few redundant links are maintained, which allows having a more reliable network. Therefore, it is evident that Poly3 can work better for mission critical WSN applications when compared with tree based algorithms [104]. The performance of CDS based schemes increases with the increase in probability but is lesser than that provided by Poly3 because CDS based algorithms have all the nodes connected through a single path only.

The proposed Poly3 approach performs well in improving network reliability but it still does not address the problem of reducing the influence of critical nodes on the performance of a network. To address this issue, this chapter further elaborates on the factors that affect the packet delivery reliability of a network namely the average path length metric and based on this in later chapters, this thesis identifies the most critical nodes in the network, which if by passed using backup paths would result in reduced network vulnerability and increased network lifetime.

3.3 APL of a network

Average Path Length (APL) is defined as the mean of the shortest path lengths between all pair of vertices and it represents the closeness and consequently, how quickly information transfer takes place in a network [110]. Most real world networks unexpectedly have short average path lengths, as popularized by six degree of freedom play. This property is known as the Small-World property and is studied in detail in [90]. Most real networks are differentiated in being small world or ultra-small world network due to the behaviour of their APL as logarithmic or double logarithmic scaling with network size n nodes [109].

Since APL is an important metric, several formulas have been proposed for its estimation. The most commonly used method is to traverse a complete graph and then average out all the path lengths to calculate its APL. It is denoted as:

$$l = \frac{1}{n(n-1)}[\sum_{i,j} d(v_i, v_j)], \tag{3.4}$$

Where n, is the number of nodes in the network and d is the distance between nodes i and j for all pair of nodes in the network. For large sized networks this is quite non-trivial, hence, for simplicity Fronczak et al. in [37] used the hidden variable network model generalized in [79] to derive a formula for the average distance between each pair of nodes which was characterized by the given values of hidden variables h_i and h_j. They attained a good agreement but only for dense networks. Likewise Zhongzhi et al. in [109] have derived a formula for APL characterization for the Apollonian network. Their analytical method is based on a recursive construction and a similar structure of Apollonian network. They have provided rigorous results showing that APL grows logarithmically with the number of nodes. This result is in contradiction with Jose et al. who state in [6] that Apollonian networks scale sub-logarithmically with the network size.

Similarly, various other models have been proposed for networks with small average distance [78] [39] such as the static Watts-Strogatz model, in which a small percentage of edges are changed in a low dimensional lattice [98] or dynamic models, in which distance between nodes becomes smaller as more nodes are added to the network. Philippe et al. in [40] provide a closed form formula for an upper bound on APL for a recently proposed recursively growing network in [110].

All these proposed formulations focus on determining APL for recursively growing networks and are incapable of identifying the APL of a network at a particular instance whereas, this chapter presents a new method to calculate APL for graphs that does not require traversing the complete graph and is computationally less expensive. In the next section, a mathematical model for calculating the APL is presented.

3.4 Path length calculation

Average Path Length (APL) of a graph l is defined as the average number of edges along the shortest path for all possible pairs of network nodes and is represented using eq 3.4. For any general graph, calculating l requires traversing a complete graph several times. However, if the graph is a regular one then simpler and less time consuming methods can be found.

The hierarchical structure of a WSN depicts the form of a tree [106] hence, the proposed approach uses the basic tree structure graphs and follow a divide and conquer approach by first modeling individual sub-parts of the tree network and then joining them together to get a unified formula.

APL is defined as the mean of the shortest path lengths of all the nodes in a graph and is denoted using eq 3.4. The averaging factor $1/n(n-1)$ remains same for all set of graphs, hence, the focus is on calculating path lengths for different graphs. If we have a line graph with n nodes, than for non-edge nodes we have paths in two directions the upper side of graph and the lower side of graph. If we move from top to bottom or vice versa than we have:

$$l = \frac{1}{n(n-1)}(\sum_{i=1}^{n-1} d(i+0) + \sum_{i=1}^{n-2} d(i+1) + \sum_{i=1}^{n-3} d(i+2) \tag{3.5}$$
$$.... + \sum_{i=1}^{n-1} d(i) + \sum_{i=1}^{n-n} d(i)),$$

While traversing the complete graph the average distance of a node replicates itself after crossing the center of the line graph resulting in:

$$l = \frac{1}{n(n-1)}2(\sum_{i=1}^{n-1} i + \sum_{i=1}^{n-2} i + \sum_{i=1}^{n-3} i \tag{3.6}$$
$$.... + \sum_{i=1}^{2} i + \sum_{i=1}^{1} i),$$

The summation function ($\sum_{i=1}^{n-1} i$) is an arithmetic series and can be simplified as $\frac{n(n+1)}{2}$, hence

$$l = \frac{1}{n(n-1)}2(\frac{(n-1)(n-1+1)}{2} + \frac{(n-2)(n-2+1)}{2} \tag{3.7}$$
$$.... + \frac{2(2+1)}{2} + \frac{2(1+1)}{2}),$$

Eq 3.7 when simplified, results into:

$$l = \frac{1}{n(n-1)}(n(n-1) + (n-1)(n-2) + ... + 6 + 2), \tag{3.8}$$

Eq 3.8 can further be simplified to:

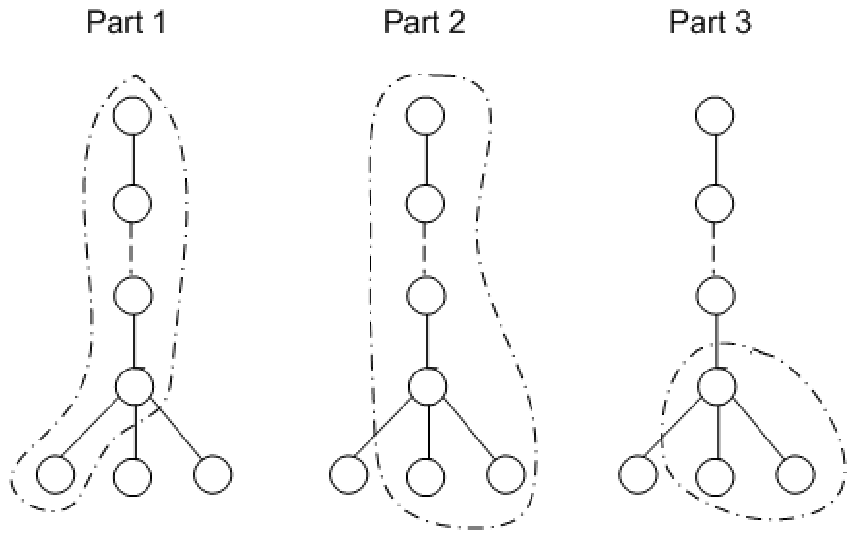


Figure 3.5: Tree graph further divided into three parts.

$$l = \frac{1}{n(n-1)} \sum_{i=1}^{n-1} (i)(i+1), \tag{3.9}$$

By expanding this the final form for the APL of a line graph becomes:

$$l = \frac{1}{n(n-1)} (\frac{n(n-1)(2n-1)}{6} + \frac{n(n-1)}{2}), \tag{3.10}$$

Similarly for finding the APL for a tree graph, one can divide a tree into three parts: a line graph that starts from the top of the tree to the lowest end of a tree, the second part calculates the distance of all the leaf nodes connected to the highest degree node and the third part calculates the distance of all the nodes connected to the highest degree node with each other.

3.4.1 Part I: APL of a line structure

The path length of the line graph can be calculated using eq 3.9, but this requires the elimination of all leaf nodes except one and this can be represented as:

$$l = \frac{1}{n(n-1)}(\sum_{i=1}^{n-(d-1)} i + \sum_{i=1}^{n-(d-1)} i^2), \tag{3.11}$$

Eq 3.11 when expanded results as:

$$l = \frac{1}{n(n-1)}\frac{(n-d+1)(n-d+2)}{2}(1 + \frac{2n-2d+3}{3}), \tag{3.12}$$

3.4.2 Part II: APL for leaf nodes

This part calculates the path length of all the leaf nodes of the tree to all the non-leaf nodes in a graph. This is achieved by summing up the path length of all the leaf nodes except those that are covered in *Part I*. This part varies from the first part in a way that in *Part I*, we also include the distance between all the nodes in the line whereas *Part II* calculates the path length of any single node (that is part of the line graph) to all the leaf nodes except the one considered in *Part I*. Starting from the farthest node in the line graph and moving towards the lower part (leaf nodes), we sum up the path lengths of all the non-leaf nodes with only the leaf nodes. The path length between all the non-leaf nodes is calculated in *Part I*, hence, *Part II* does not take them into consideration. The path length for this part can be represented by:

$$l = \frac{1}{n(n-1)}[2(d-1)\sum_{i=1}^{n-(d-2)} i], \tag{3.13}$$

3.4.3 Part III: APL for the inter-leaf nodes

This part calculates the inter leaf nodes path length. The distance between any two leaf nodes is two units and the total number of such combinations can be represented by:

$$l = \frac{1}{n(n-1)}(2(d-1)(d-2)), \tag{3.14}$$

3.4.4 APL for a tree graph

Now the APL of a tree structure is the sum of eq 3.12, 3.13 and 3.14. Which leads to:

$$l = \frac{1}{n(n-1)}\frac{(n-d+2)(n-d+1)}{2}[\frac{2n-2d+3}{3}+1]+ \tag{3.15}$$

$$2(d-1)\sum_{i=1}^{n-(d-2)} i + 2[(d-1)(d-2)],$$

Eq 3.15 can be generalized for calculating the path length of any given graph:

$$l = \frac{1}{n(n-1)}(n-d+1)(n-d+2)+ \tag{3.16}$$

$$[\frac{1}{2}(\frac{(2n-2d+3)}{3}+1)+(d-2)]+2[(d-1)(d-2)],$$

By simply inserting the values of the highest degree and the total number of nodes, one can find the APL for any arbitrary graph at any instance.

3.5 Summary

In this chapter, a new approach for determining the APL of a complex tree structure is proposed which uses the value of the highest degree and the total number of nodes of a network as an input. It computes the APL of any complex tree structure and unlike the previously proposed algorithms, the complexity of the proposed algorithm does not increase with the increase in number of nodes in the network. This insight about calculating the APL of a complex tree structure is utilized in the next chapter for reducing the APL of WSN, for the implementation of the Small-World phenomenon.

Chapter 4

Average Path Length and Network Performance

4.1 Introduction

According to the Small-World phenomenon, the average separation between a source and a destination node in a social network lies between five and six [64]. As WSNs are scalable up to a size of thousand nodes, hence such an immense reduction in the number of intermediate nodes would lead to great improvement in increasing network life time and reducing the rate of depletion of node energy. In social networks, connections between nodes are not constrained by the distance between them whereas, a connection between two nodes in a WSN only exists if those nodes exist in the transmission range of each other. This transmission range limitation bounds us from using the Small-World phenomenon in its original form. Small-World phenomenon uses a random rewiring mechanism in which a few edges are randomly rewired between nodes to reduce the APL between nodes. This chapter explains in detail the mechanism adopted for introducing the Small-World phenomenon into the WSN.

As WSNs are spatial graphs, it is possible to reduce the APL between nodes by simply adding shortcut paths. These paths can only benefit the network if deployed after properly considering the topological characteristics of the network. Since, in WSNs a connection between two nodes exists if they both are in the transmission range of each other, hence, in order to reduce the APL between distant nodes, one needs to increase the transmission range of a node. The transmission radius of a node is dependent upon the nodes transmit signal energy [81]. This leads to the requirement of an efficient mechanism that increases the transmission radius while considering the dependence on the energy consumption. The next section explains in detail the existing work in this domain and also highlight the need for a better solution. Section 4.3 presents the proposed protocol and explains in detail how it overcomes the deficiencies of the existing approaches.

4.2 Related Work

In this section, some techniques are presented, which introduce the Small-World property into WSN's.

In [97], Watt and Strogatz proposed a model to construct a Small-World network out of a regular graph whose topology is of a low density regular lattice. A regular graph is rewired using the probability p, an edge is reconnected to a randomly chosen vertex, while avoiding duplicate edge formation. In the next phase, considering the probability p, the process is repeated for the edges that connect the vertex to the second nearest neighbour. This process continues circulating around the ring, unless each edge of the original lattice is considered once. Watt and Strogatz conclude that by using this model and rewiring only 1% of the edges, an APL reduction of 80% can be achieved. Despite having such an advantage, this model is in-appropriate for use in WSNs. Implementing such a model would result in selecting random nodes in the network to become neighbours, forcing the nodes to extend their transmission radius over the complete network.

Considering the transmission radius limitation and spatial dependence of WSNs, Sharma and Mazumdar [80] used wired links to create shortcut paths in WSNs. These wired links have wireless transceivers attached at both ends to make it replenish their energy, as there is no energy constraint at the wire links. They show that by adding few wired-links in a WSN, hop count for multi-path routing can be reduced, resulting in reduced energy dissipation. A node intending to relay data to a far-away node shall forward it to the wired-link, which shall transfer it to the other end, and by using wireless transceivers at both ends, forward data to its desired destination node. However, in many application scenarios like, node movement tracking, such a mechanism would not be able to facilitate because these wired-links once deployed will not be able to move along the movement of the wireless devices.

To solve this issue, Chetan Kumar et al. in [93] equip gateway nodes with two radios, a short range and a long range. The long range radio is dedicatedly used for establishing a link between distant nodes. Addition of such links improves network performance by 25% and reduces the APL up to 43%, but it is not feasible for mission critical sensor network applications where increasing the network lifetime is one of the prime focus. Use of extra hardware will deplete the node energy at a higher rate resulting in reduced network lifetime.

On the other hand, Eleni et al. in [89] have proposed a topology control based approach, intended to aid multi-hop communication in an intelligent and effective manner. They use directional antennas between nodes having the highest degree. A node having higher degree is more likely to be handling heavy traffic and is hence equipped with a shortcut link to reduce multi-hops for messages intended for distant nodes.

Likewise Abhik Banerjee et al. in [13] have reduced APL with the use of directional antennas along with a distributed self-organizing framework, which figures out highly connected nodes without using node's traffic flow. They believe that nodes having higher traffic flow are better candidates to be connected for path reduction. Traffic flow in WSNs is bursty in nature [95] hence; the value of this parameter will change in a random order, resulting as a constant change in nodes selected to use directional antennas. Directional antennas have a limitation of reducing the covered angle for the increase in covered distance, hence if a node intends to cover a longer distance; it will have to direct its energy into a narrower beam-width at the cost of losing connections with its neighbours. To overcome this deficiency a new scheme is proposed in this chapter.

The proposed technique eliminates the deficiency faced in using directional antennas of reducing transmission angle for the increase of transmission distance. It uses neighbour avoiding walk mechanism for calculating betweenness centrality and selects a group of nodes that uses variable modulation technique for data transfer. Variable modulation scheme is employed to guarantee signal interpretation quality while adding to form long distance relay path without the use of any additional infrastructure.

4.3 Variable Rate Adaptive Modulation (VRAM)

This section discusses how shortcut paths can be added into the network, while using the available resources and maintaining the topological characteristics of the network. Here, the overall aim is to reduce the mean path length between two randomly selected nodes, while simultaneously maintaining the energy consumption of nodes, with the use of variable modulation. Variable modulation scheme enables nodes to cover a greater distance by just reducing the modulation scheme to a lower index, from $64QAM$ to $16QAM$. A higher order modulation scheme has a higher path loss exponent, increasing the bit error rate with increase in distance, hence by using a lower order modulation scheme ($16QAM$) for a limited number of nodes, the overall data rate is not effected [86]. The selection procedure is explained in the next subsection.

4.3.1 Centrality Indices Based On Neighbour Avoiding Walk

Wireless Sensor Networks are conveniently described as graphs $G = (V, E)$, where E represents the set of edges and V represents the set of vertices. If there exists a path from $a \in V$ to $b \in V$, beginning from a and ending at b then the minimum distance between node a and b can be denoted as $G_d(a, b)$. By definition $G_d(a, a) = 0$ for every set of $a \in V$ and $G_d(a, b) = G_d(b, a)$ for any $a, b \in V$. Let $\sigma_{a,b}$ denote the number of shortest paths from $a \in V$ and $b \in V$, where by convention $\sigma_{a,a} = 1$ for every set of $a \in V$. If $\sigma_{a,b}(z)$ denotes shortest path from a to b which passes through a node $z \in V$ than the betweenness centrality will be:

$$B_C(z) = \sum_{(a,b,z)\in V} \frac{\sigma_{ab}(z)}{\sigma_{ab}}. \tag{4.1}$$

A high centrality score shows that a vertex can reach others on a relatively short path. For ease in understanding and to control the size of the network, the value of betweenness centrality is kept between zero and one. The size of a WSN makes the evaluation of betweenness centrality computationally expensive. Hence, for simplicity the computation of the betweenness centrality is based on the Bellman criterion, according to which a vertex $z \in V$ lies on the shortest path between vertex $a, b \in V$, if and only if $G_d(a, b) = G_d(a, z) + G_d(z, b)$.

Given the shortest path and the pairwise distances, the pair dependency $\delta_{ab}(z) = \sigma_{ab}(z)/\sigma_{ab}$ of a pair $a, b \in V$ is on an intermediate vertex $z \in V$ [18]. Therefore, the ratio of the shortest path between a and b that z lies on is given by:

$$\sigma_{ab}(z) = \begin{cases} 0 & if\ G_d(a,b) < G_d(a,z) + G_d(z,b) \\ \sigma_{az} \cdot \sigma_{zb} & \text{otherwise} \end{cases}$$

From this the betweenness centrality of a vertex v is simply the sum of the pair-dependencies of all pairs of vertices, hence:

$$B_C(z) = \sum_{(a,b,z \in V)} \delta_{ab}(z). \tag{4.2}$$

This shows that betweenness centrality can be determined in two steps:

1. Compute length of the shortest paths between all pair of vertex
2. Sum all pair dependencies

The complexity of determining the betweenness centrality is dominated by the second step, since $O(n^2)$ pair dependencies need to be summed for each vertex and the running time of the implementation is dominated by the time spent on matrix multiplication. It is clear that algebraic path counting computes more information than needed; hence traversal algorithms are used to exploit the scarcity of typical instances. Brandes et al. in [18] used both breath-first search (BFS) for un-weighted and Dijkstra's algorithm for weighted graphs. Considering the amount of nodes to be traversed for path counting, this thesis emphasises on using the Neighbour Avoiding Walks (NAW) to reduce this overhead.

In NAW, the walker starting from the sink node, does not visit any node previously visited up to a certain depth n nor does it visit the neighbour of a previously visited

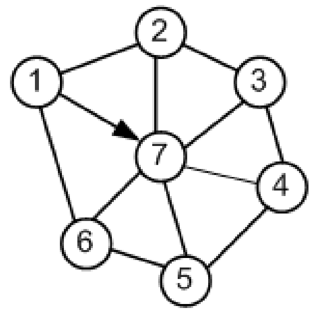


Figure 4.1: Long Leg Capability.

vertex up to a distance m. For simplicity, consider the depth $n = 1$ and distance $m = 1$ then the neighbours not being covered by this rule will receive messages according to a random policy which is normally uniform.

This policy of using NAW with $n = 1$ and $m = 1$ has two advantages: a long leg capability and an enhanced bridge crossing. Fig 4.1 highlights the first advantage: Suppose that a message that was located at vertex 1 at a previous time step and has now moved to vertex 7. In case of a memory less system, where a node can visit any randomly selected node, it can be routed to all the neighbours of vertex 7. Whereas, according to NAW it can be routed to all the neighbours of vertex 7, except vertex 1 and neighbours of vertex 1.

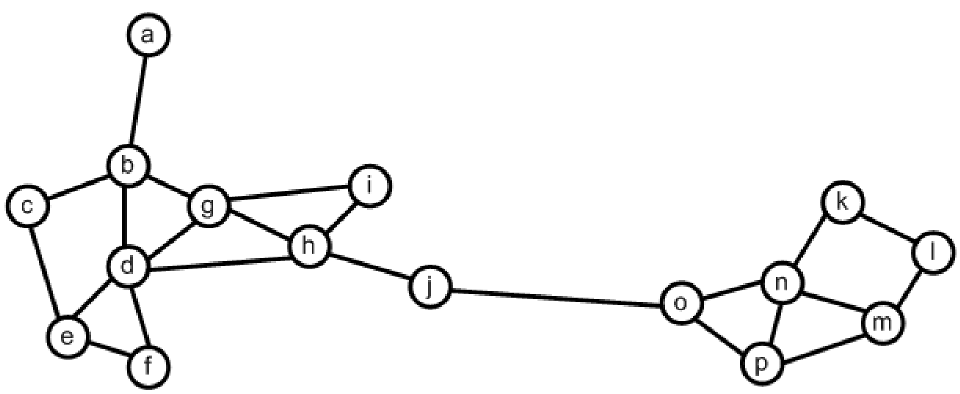


Figure 4.2: Enhanced Bridge Crossing.

The second advantage of this mechanism is that, in a network shown in Fig 4.2, where the walk reaches from a well-connected area to a node which represents the end of a bridge, then the favourite path of that walk is through the bridge, because by definition the node at the opposite end cannot be neighbour of the previous node.

The extra stiffness is added in NAW by not visiting neighbours of the previously visited vertex results in an increased path walked by the walker due to the square root law of diffusion [46]. Once each node has been visited and betweenness centrality is calculated by all nodes in the network, then nodes having the highest betweenness centrality value form long distance links by using VRAM.

4.3.2 Variable Rate Adaptive Modulation (VRAM)

Mobile radio channels are prone to burst errors due to deep fades, even when the channel Signal to Noise Ratio (SNR) is kept high. This can be reduced by the use of variable transmission power or by varying the constellation size. In the former, with the increase in transmission power, the co-channel interference also increases [101]. This leads to the notion of varying the constellation size under uniform transmission power, so that when a longer distance is to be covered, a lower order constellation is used and for a shorter distance a higher order constellation is used. This change in constellation size provides us with variable data rates, while maintaining a constant bit error rate (BER) [101]. Such an approach also helps avoid bit errors occurring in bursts, hence if we maintain a constant BER, and only change the modulation scheme than we can cover a longer transmission distance. This chapter proposes the use of

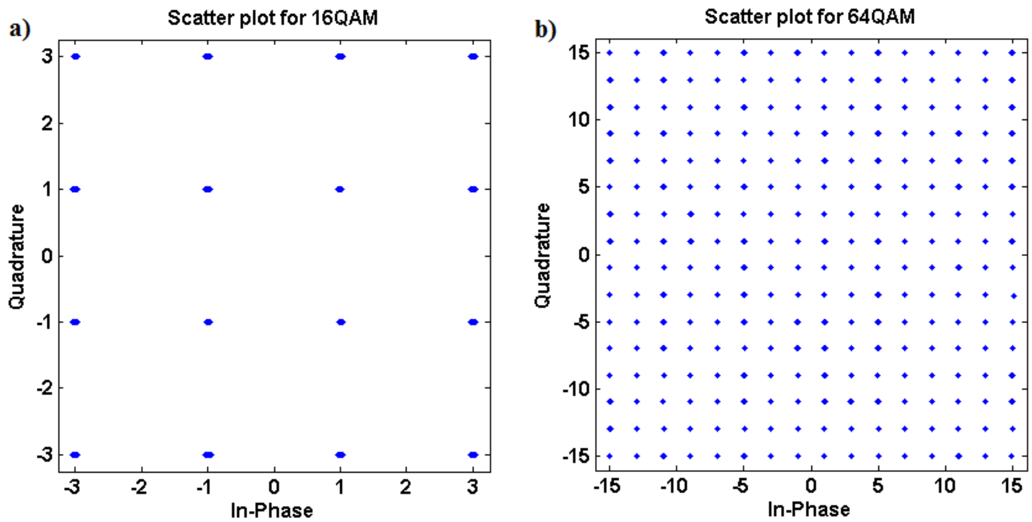


Figure 4.3: a) Constellation diagram for 16QAM, b) Constellation diagram for 64QAM.

conventional $16QAM$ and $64QAM$ modulation scheme with square constellation as shown in Fig 4.3 for covering a longer distance.

The basic assumption here is that, the interference from other nodes can be modelled as Gaussian noise and the effect of this interference can be incorporated into thermal noise power $N_o/2$. The target BER P_b of a QAM signal can be related to the number of symbols in the modulation constellation M according to [25] as.

$$P_b = \frac{4}{b}(1 - \frac{1}{\sqrt{M}})Q(\sqrt{\frac{3}{M-1}\gamma_b}). \tag{4.3}$$

Here, BER is calculated over Rayleigh fading channel, and γ_b is the average SNR per bit defined as $\gamma_b = E_s/N_o$. E_s is the required energy per symbol at the receiver for a given BER requirement and b is the constellation size. Using the Chernoff bound eq 4.3 can be reduced to:

$$P_b \leq \frac{4}{b}(1 - \frac{1}{\sqrt{M}})(\frac{1.5E_s}{N_o(M-1)})^{-1}. \tag{4.4}$$

Here $M = 2^b$ and the symbol energy can be replaced by $(E_b b)$, where E_b is the required energy per bit required at the receiver. Hence, eq 4.4 an be used to obtain the average transmission energy per bit as follows:

$$\frac{P_b}{4}(\frac{1}{1-\frac{1}{2^{\frac{b}{2}}}}) \leq (\frac{1.5E_b b}{N_o(2^b-1)})^{-1},$$

When further simplified, it reduces to:

$$E_b \leq \frac{3}{2}(\frac{P_b}{4})^{-1}(\frac{\sqrt{2^b}-1}{\sqrt{2^b}})(\frac{N_o(2^b-1)}{b^2}),$$

Finally:

$$E_b \leq (1+\alpha)\frac{3}{2}(\frac{P_b}{4})^{-1}(\frac{(2^{\frac{b}{2}}-1)(2^b-1)}{2^{\frac{b}{2}}})\frac{N_o}{b^2}Gd^2. \tag{4.5}$$

Where α is the drain efficiency of the RF power amplifier and d is the distance between the transmitter and the receiver G is the antenna gain at both the transmitter and the receiver. Here, it is assumed that path loss obeys the square root law. Now for the same transmitters, using same transmission energy but different modulation schemes ($16QAM$ and $64QAM$) eq 4.5 can be reduced to:

$$\frac{(\sqrt{2^{16}}-1)(2^{16}-1)(d_{16})^2}{\sqrt{(2^{16})}16^2} = \frac{(\sqrt{2^{64}}-1)(2^{64}-1)(d_{64})^2}{\sqrt{(2^{64})}64^2},$$

Here, d_{16} represents the distance covered by a QAM signal working on a constellation size of 16 and likewise d_{64} represents the distance coverage of a signal transmitted using a QAM signal with a constellation size of 64. Now the above expression is simplified to obtain a relation between the distance covered by a $16QAM$ signal and a $64QAM$ signal using similar transmitters and under similar environmental conditions, it results in:

$$d_{16} = \frac{2\sqrt{105}}{15} d_{64}. \tag{4.6}$$

Eq(4.6) denotes that by using the same amount of transmission energy and under the same BER requirements, a $16QAM$ signal travels $\frac{2\sqrt{105}}{15}$ more distance when compared to $64QAM$. The main reason for covering a longer distance is the Euclidean distance between the constellation points of a $16QAM$ signal when compared to $64QAM$ as shown in Fig 4.3. A signal that has a greater distance in its constellation points is less prone to error. A noise signal has to have greater amplitude, in order to mix one constellation point into another at the receiver, for detection. Hence, a $16QAM$ signal can travel a longer distance.

Using this concept,the proposed approach equips nodes having a higher betweenness centrality, a lower order modulation scheme, to cover longer distances. Fig 4.4 shows the change in network topology after use of VRAM for an area of $1000 \times 1000m^2$. Fig 4.4a, shows the initial network setup where random links are formed between nodes, Fig 4.4b and Fig 4.4c show the area covered by nodes when 3% and 10% of nodes using VRAM where nodes form links with every neighbouring node inside a

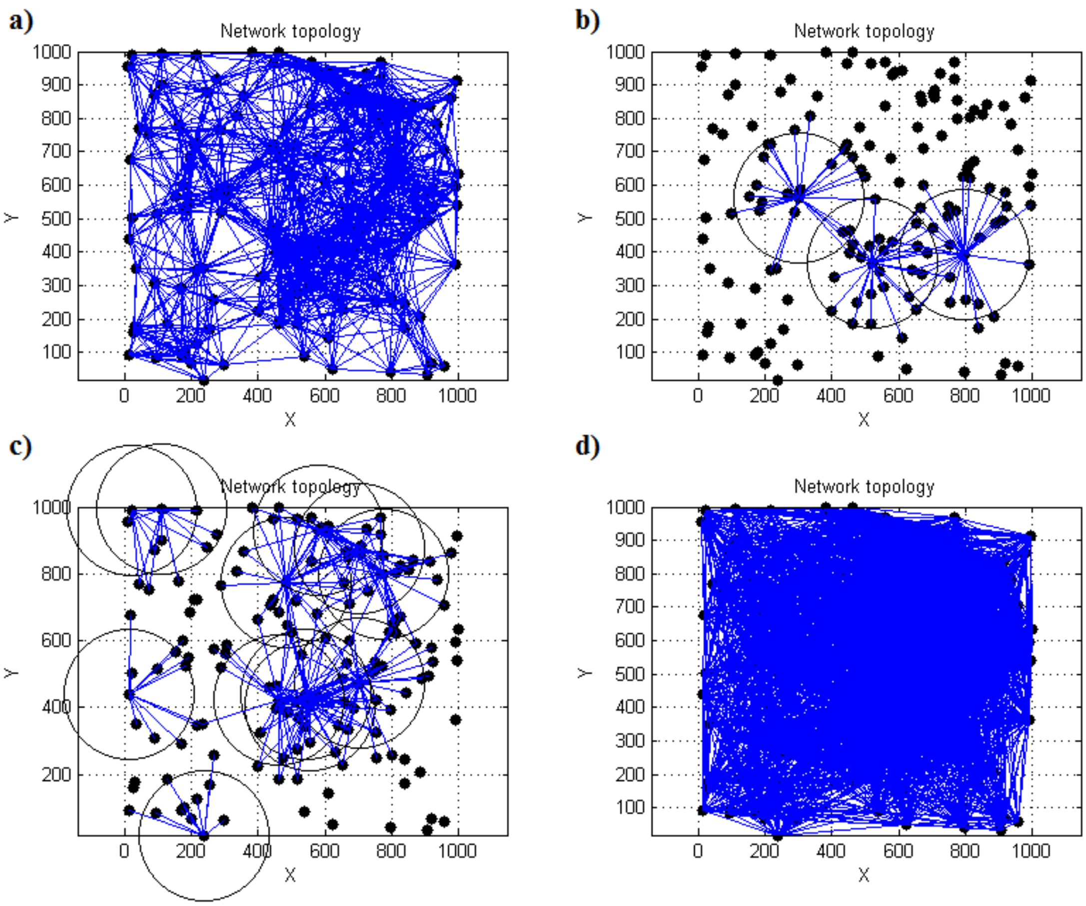


Figure 4.4: Demonstration of topology modification mechanism. (a) Initial network with random link formation between nodes. (b) 3% nodes form long distance links using VRAM. (c) 10% nodes form long distance links using VRAM. (d) Network with 10% nodes forming links using VRAM and 90% nodes using random link formation.

specific region resulting in increased node degree. The final network formation is shown in Fig 4.4d where only 10% of nodes use VRAM for long range links and 90% nodes have random links of the initial setup.

4.4 Simulation Results

The proposed model is evaluated for a network consisting of omni-directional antennas, distributed randomly over a rectangular region. It accesses the impact of using VRAM for forming long distance relay paths. The simulations were run in Matlab and the proposed model was compared with methods proposed by [13] and [89] namely *Directional-WFB* and *Socially Inspired* respectively. The proposed model is also compared with a random network, where all the edges are randomly connected to analyze the change in node degree and it is referred as *Omni-directional*. The results shown were averaged for all node pairs and 50 different topologies. The simulation setup was based on a realistic assumption that, the network can be disconnected due to limitation in transmission range and any node that cannot be accessed has a path length of infinity (in these experiments 100000 is our infinity for better realization of APL).

The first set of simulations, vary the number of nodes in the network for a fixed network area of $1000 \times 1000m^2$. The percentage of nodes forming long distance relay paths is 10% for optimum performance [13][89]. Nodes are equipped with homogeneous amount of energy and use CSMA/CA for packet collision avoidance. It is assumed that the transmission radius of an omni-directional antenna is $250m$. The distance covered by directional antennas is obtained from [13], stated as:

$$r(\Theta) = r\sqrt{\frac{2\pi}{\Theta}}. \tag{4.7}$$

Where $r(\Theta)$ is the beam-length for a beam-width Θ and r is the omni-directional transmission distance.

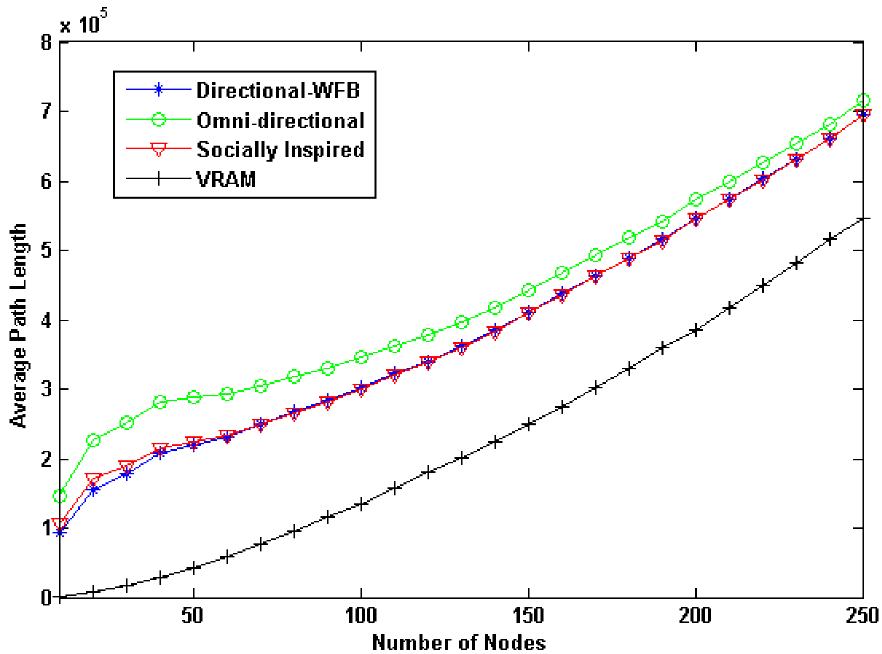


Figure 4.5: Average path length with varying number of nodes.

Fig 4.5 denotes the variation in APL with change in the amount of nodes present in the network, under fixed network area. By varying the number of nodes in the range $[10 - 250]$ it is observed that, *Directional-WFB* and *Socially Inspired* have a similar pattern, this shows that the distributed selection mechanism of node with highest degree has similar performance to the scheme provided by *Socially Inspired*, where a node is selected using an iterative mechanism for long distance relay path formation. *VRAM* outperforms the rest due to its covered angle, the use of a lower order modulation scheme along with an omni-directional antenna allows the node to have long distance communication covering 2π radians. The use of directional antennas, as in *Directional-WFB* and *Socially Inspired* limit the node to communicate in a particular direction only.

As APL is the average distance of a particular node to all the nodes present in the network, so in case of a directional antenna, a node present in the exact opposite direction of the directional antenna's face will have a longer path length and a packet has to be relayed through neighbouring nodes, this results in an increased path length. The major improvement in APL is due to the consideration of enhanced bridge crossing as shown in Fig 4.2. APL is measured in units of 10^5 due to the consideration of random networks, where networks can be disconnected, resulting in high APL as nodes in a network can be in-accessible due to transmission range limitation. *VRAM* is the only technique that caters for Enhanced Bridge Crossing, resulting in major improvement in APL. With a lower number of nodes, APL for *Directional-WFB*, *Socially Inspired* and *Omni-directional* increases due to widely spread nodes, forming network chunks. With the increase in number of nodes, these network chunks spread over and form a single network resulting in a smooth increase in APL.

Fig 4.6 represents the variation in Average Node Degree with the change in number of nodes for the same network area. *Directional-WFB* and *Socially Inspired* have a lower average node degree as they use directional antennas. Directional antennas form long distance relay path by breaking their current links and concentrating all

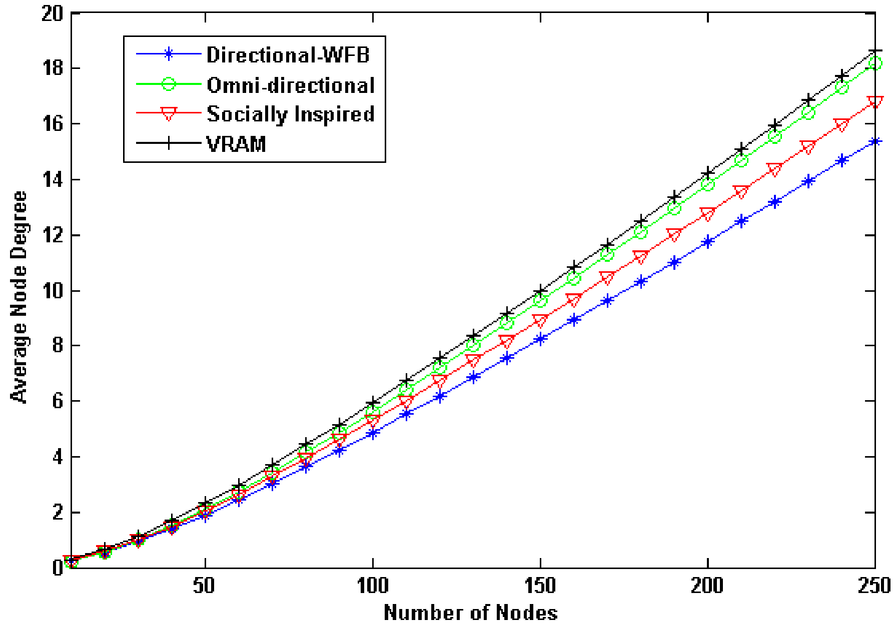


Figure 4.6: Average node degree with varying number of nodes.

the antenna power into one particular direction, this is executed at the loss of current links formed in all 2π radians. On the other hand, *VRAM* forms long distance omni-directional links. It makes new long distance relay path, while maintaining its current communication paths, resulting in a higher average node degree.

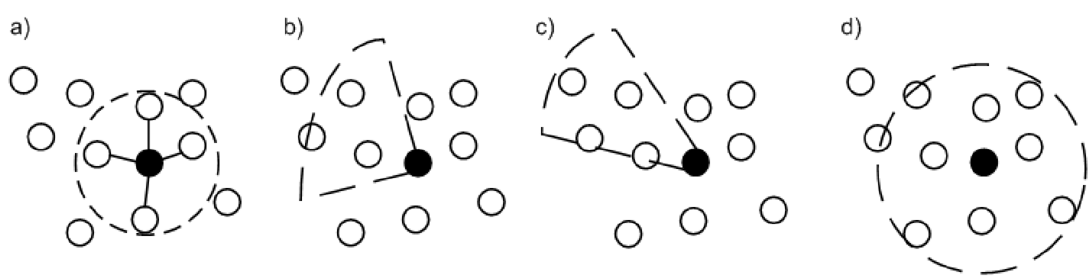


Figure 4.7: Effect of changing beam width on beam angle and comparison node degree of VRAM.

Fig 4.7a shows the node degree of a node having links while using an omni-directional antenna, as the beam-angle of a directional antenna is reduced the beam-length increases, decreasing the covered area and hence reducing the node degree as shown in Fig 4.7b and Fig 4.7c. This trend results in reduced node degree of *Directional-WFB* and *Socially Inspired*. A relatively high node degree value represents that only 10% of nodes are equipped with directional antennas whereas, the rest of the nodes have omni directional antennas and they form links such as shown in Fig 4.7a. *VRAM* follows a trend shown in Fig 4.7d, due to which 10% of nodes have higher node degree, resulting in an overall higher node degree. This enables nodes to relay data in any direction, reducing the overall cost of relaying messages.

The second set of simulation analyses the network performance for varying initial radius values in the range $[100m, 500m]$. Number of nodes used is kept constant at 100 nodes. The effect of varying the initial transmission radius on the APL and node degree is monitored.

Fig 4.8 shows that as the initial radius of a node is increased APL tends to decrease for *Directional-WFB* and *Socially Inspired*, as they can relay messages to a greater distance with increase in initial radius. APL for *Omni-directional* decreases as more nodes are directly connected to a single node due to extended transmission radius. *Directional-WFB*, *Socially Inspired* and *Omni-directional* do not cater for the enhanced bridge crossing problem and hence have cases when the network is partitioned. As the value of the initial transmission radius increases, these inaccessible nodes become reachable and hence the APL decreases. The proposed mechanism of choosing the node with the highest betweenness centrality considers such nodes and hence the APL is always lower. The increase in APL is due to the increase in value of

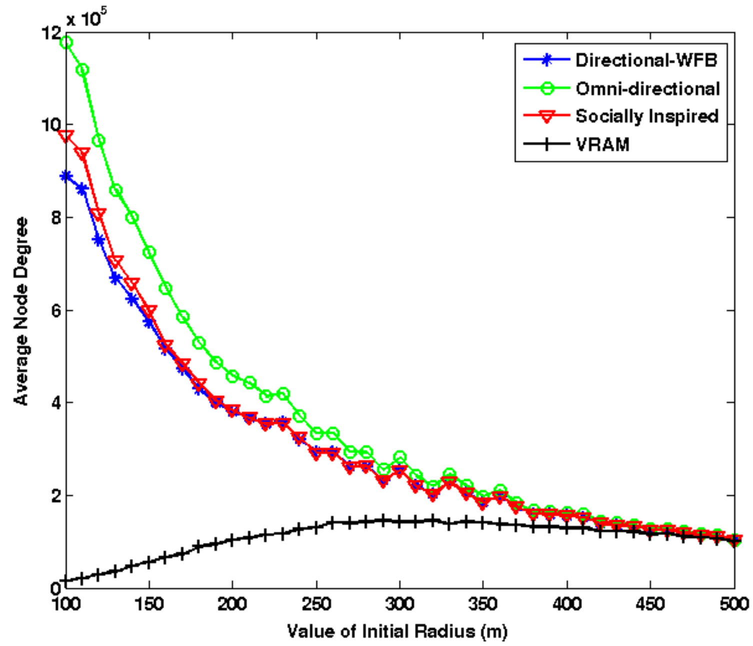


Figure 4.8: Average path length with increasing initial radius.

initial radius, more nodes come in direct contact, reducing number of hops and hence slightly increasing the APL. As the value of initial radius increases, the transmission radius of a node increases and more and more nodes can be accessed directly, reducing the APL at very high values of initial radius.

Fig 4.9 represents the variation in Average Node degree with varying the value of the initial radius. Similar to results shown in Fig 4.6, average node degree of *VRAM* is higher than that of simple *Omni-directional* antennas because in this mechanism, a node maintains its entire current links while building new long distance communication links.

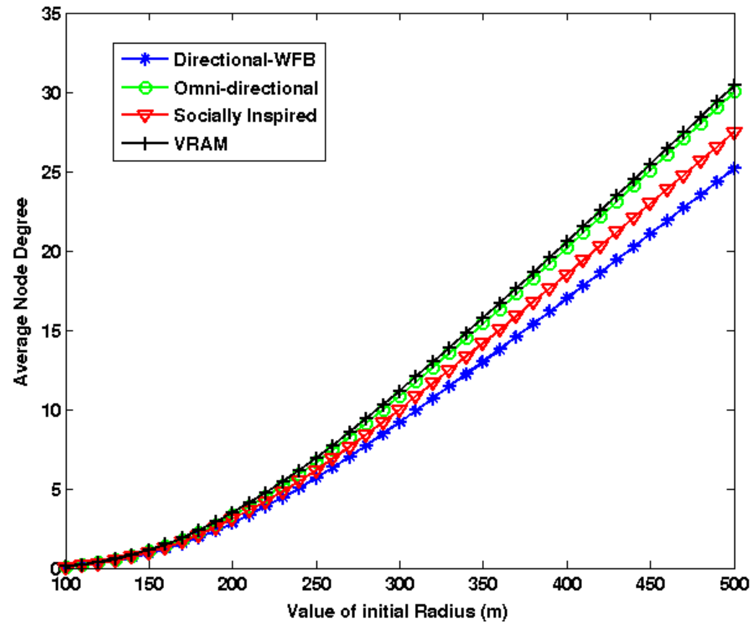


Figure 4.9: Average node degree with varying initial radius value.

4.5 Summary

This chapter introduced the use of VRAM for formation of long distance communication links to reduce the APL of a WSN. The proposed method overcomes the deficiencies faced by traditionally used directional antennas of limiting the beam-width to increase the beam-length. This chapter proposes a mechanism that enables nodes to calculate the betweenness centrality measure by walking through a lower number of nodes, using neighbour avoiding walk and it is shown using simulations that significant performance is achieved by using variable modulation technique, over use of directional antennas for the formation of long distance relay paths.

The introduction of these long distance communication links reduces the APL of the network but, it also increases the privacy risk in a network. The nodes forming these long length links act as a bridge between distant nodes, ensuring communication between multiple neighbouring nodes. This capability increases the participation of these nodes in relaying data between distant nodes and hence, this increases the criticality of these nodes. A malicious node can eavesdrop and overhear maximum information, or it can broadcast itself as having the shortest path to maximum nodes in the network and then alter the incoming messages. An attack by a malicious node on to a critical node will have a greater impact on the network performance when compared to an attack on a regular node in the network. The next chapter formally defines node criticality and then analyses the affect on the criticality of a node due to the formation of long length links.

Chapter 5

Intuition Based Critical Node Identification Approach

5.1 Introduction

Critical node discovery is an important process for understanding network vulnerability. A node is deemed as critical, if it plays a vital role in maintaining network performance and by removing that node, the overall performance deteriorates and in some cases leads to network partitioning [83] which is highly undesirable. Evaluating the criticality of nodes is significant in various complex networks. In Wireless Sensor Networks (WSNs) employing geographical routing, for example, malicious attack or malfunction of a few beacon nodes leads to fallacious node discovery for the remaining nodes in the network, thus jeopardizing the stable operation of the routing protocol [56]. Moreover, in [52] it was observed that removal of 4% of the nodes in a Peer to

Peer Gnutella Network resulted in major fragmentation of the whole network. The node criticality problem in Peer to Peer and overlay networks was also addressed in [44]. Finally, in [7] it was shown that in a telecommunication network, the penetration of a virus can be prevented by removing a few critical nodes. The node criticality problem is significant in network paradigms beyond computer networks. In road networks, for example, intersections which can be considered as nodes in a graph theoretic framework, might experience heavy traffic loads when in proximity to a major landmark. Identifying such critical nodes is significant when investigating possible extensions of the existing infrastructure [66]. Likewise, in a social network of terrorist activists, the removal of a few critical nodes can paralyse the communication in the network, making the network ineffective [53].

Several studies have addressed the node criticality problem and various metrics have been proposed to characterize the criticality of nodes in a network. In this chapter, based on the preliminary results in [9], a new criticality metric is proposed which is shown to be more successful in identifying nodes, the removal of which, significantly affects network operation. The metric encompasses three main node attributes: the weighted node degree, the variation in link length of the node from its neighbours and its contribution in forming shortest paths. Unlike previous proposals which take into account the absolute node degree, this proposal considers the node degree weighted by the average common neighbours of the node with all its neighbours. The presence of common neighbours is an indication of the presence of path alternatives which undermine the criticality of a node. In addition, in order to account for long range links which cause nodes to act as relay nodes thus accommodating heavy traffic and becoming critical for the whole network operation, this chapter introduces the notion of variation in link length between neighbouring nodes. The diversity in the number of neighbours and the diversity in link lengths thus contribute to the criticality of a node and are used to form the diversity index. This then account for the contribution of each node in forming the routing paths by employing a new technique which is inspired by voting games in game theory. The metric emanating from this technique is known as the Banzhaf Power index. The combination of the latter with the diversity index yields the proposed criticality metric which is referred to as the *Combined Banzhaf & Diversity Index (CBDI)*.

Performance of the proposed metric is evaluated using analysis and simulations. The evaluation is based on the degradation in performance reported when nodes selected using the criticality metric under consideration are removed from the network. The proposed metric is compared against other metrics that have been proposed in the literature, namely the *Hybrid Interactive Linear Programming Rounding (HILPR)* proposed in [83], the *Controllability of complex networks (Cont)* in [59] and the *degree centrality*, *betweenness centrality*, *closeness centrality* used in [34]. The Random Network Topology, the WaxMan Network Topology and the Small World Network Topology were considered in the simulation experiments and network performance was evaluated using a number of performance metrics which include the average node degree, the average path length, the number of isolated nodes, the network throughput, the average per packet delay, the average per packet jitter, the number of dropped packets and the algebraic connectivity. The latter, defined as the second smallest eigenvalue of the Laplacian of a network, serves as connectivity robustness metric. It provides an analytical perspective as to why the proposed metric and its key features work effectively. Extensive simulations indicate that the proposed criticality metric in the considered scenarios is able to achieve a more severe degradation in network performance compared to other approaches, indicating that it is superior in characterizing the criticality of the network nodes.

5.2 Proposed Criticality Metric

As mentioned in the introduction, this chapter proposes a new criticality metric which is the combination of the Banzhaf power index and the diversity index. This section explains the reasoning behind such a design choice and formally defines the diversity index and the Banzhaf power index. It then shows the two are combined to form the proposed criticality metric.

5.2.1 Diversity index

Diversity index is a measure of the variation of node properties between neighbouring nodes. This thesis considers variation of two attributes of neighbouring nodes which are logically related to their criticality: the variability in link lengths and the variability in their list of neighbours. Increasing both the variability of link lengths and the variability in the list of neighbours implies greater node criticality. The proceeding subsection gives a detailed description of the two and explain how they are combined to form the diversity index.

Variation in link length

This attribute measures the variation in the length of the links between neighbouring nodes. A greater variation in link length certifies the existence of both long distance and short distance links. A node with the aforementioned property is capable of acting as a relay node between the nodes in proximity and the distant ones. This will aid neighbouring nodes in getting their data relayed to distant nodes and vice versa at a reduced network energy and time cost [110]. Since a node with a higher variation in link length has a higher probability of acting as a relay node hence, it is deemed as critical for information dissemination.

Variation of link length is defined as the average difference between the transmission radii of neighbouring nodes. Assume a graph $G = (V, E)$, where V represents the set of Nodes and E represents the set of Edges. Each node x in V is characterized by its transmission radius T_x. For each node x, the set of nodes which lie within the transmission range of x is the set of its neighbours and is denoted by $N(x)$. The variation in link length of x is denoted by $D_d(x)$ and is given by:

$$D_d(x) = \frac{1}{|N(x)|} \sum_{u \in N(x)} (T_x - T_u) \tag{5.1}$$

In order to demonstrate the way that the variation in link length characterizes the criticality of node, consider the example network of Fig 5.1. The links between nodes are drawn to scale so that longer link lengths on the diagram, indicate longer

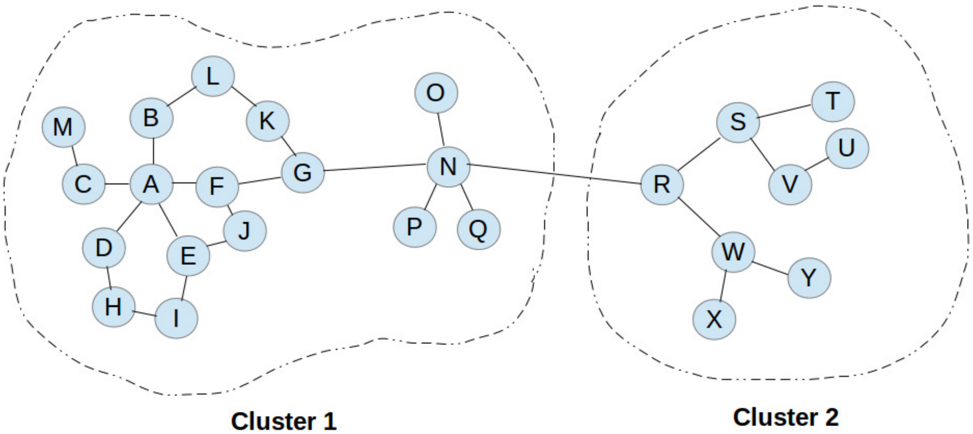


Figure 5.1: Node N acts as a relay node between the two network partitions and thus has a higher variation in link length value compared to node A.

link lengths in the actual network. Nodes A and N in the considered network share the same node degree. However, node N reports a larger value of the variation in link length metric, as it has both short and long length links. Node A on the other hand, only has short length links resulting in a low variation in link length value. The removal of node A partitions the network, however, it only isolates nodes C and M. The removal of node N, on the other hand, partitions clusters 1 and 2 thus resulting in isolation of a far larger number of nodes. This demonstrates the higher criticality of node N which is reflected in a higher value of variation in link length.

Weighted Node Degree

Node degree was used by Freeman in [34] for determining the criticality of a node. Despite the simplicity of the method it fails to take into consideration self loops and one hop reachability of neighbouring nodes which leads to overestimates of node criticality. Therefore, this thesis avoids the consideration of these redundant paths by elaborating on the variability of the list of neighbours of neighbouring nodes, leading to the notion of weighted node degree. The weighted node degree takes values between 0 and 1, and increases as the number of common neighbour decreases. A greater number of common neighbours implies more one hop paths between neighbouring nodes which undermines the criticality of a node. The weighted node degree of x is represented by $D_n(x)$ and is given by:

$$D_n(x) = \sum_{u \in N(x)} \frac{|N(u) \backslash N(x)|}{|N(u)|} \tag{5.2}$$

where $\backslash$ denotes the set difference and $|.|$ denotes the cardinality of the set. So, the weighted node degree of a node x is calculated by summing the dissimilarity ratios of all of its neighbours. The dissimilarity ratio for a particular neighbour u is the ratio of number of neighbours of u which are not neighbours of x over the set of all neighbours of u.

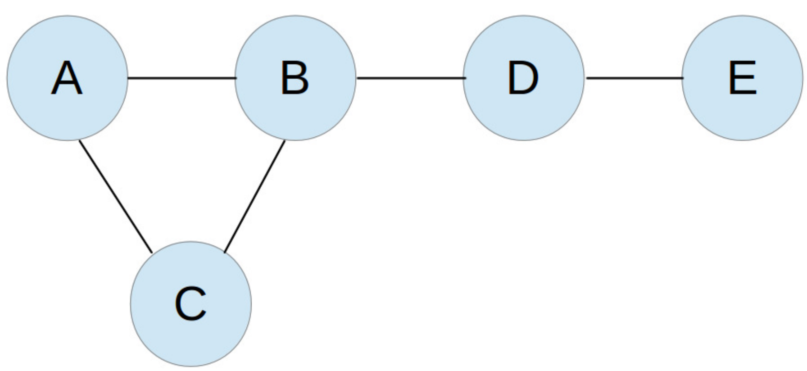


Figure 5.2: Example network to highlight the rationale behind the consideration of the weighted node degree.

In order to highlight the methodology with which the weighted node degree determines the criticality of a node consider the example network of Fig 5.2. In this network, nodes A and D share the same node degree but a different weighted node degree. The weighted node degree of node A is lower than that of node D due to the link between nodes B and C which causes the neighbours of A to have one common link. This extra link adds to the redundancy of connections of node A and thus when node A is removed from the network, the resultant network is still connected through the link between nodes B and C. On the other hand, the removal of node D completely isolates node E and hence partitions the network in two segments. This demonstrates that a node with a higher weighted node degree has a higher influence on the network upon its removal and is thus a more critical node.

Both the variation in link length and the weighted node degree of a node described above are used to calculate the diversity index of that node. The diversity index $H(x)$ is defined as the product of the two metrics such that:

$$H(x) = D_d(x)D_n(x) \tag{5.3}$$

It follows from the discussion above that the greater the diversity index, the more critical a node is. The criticality of a node is further refined by weighing its participation in path formation.

5.2.2 Banzhaf power index

In game theory, different assumptions have led to different definitions for determining the importance of an agent in a game. One of the most prominent among these is the Banzhaf power index [30]. This index has been widely used primarily for the purpose of weighted voting games. In a voting game, each voter is assigned a weight and the coalition of these voters determines the outcome of the game. A game is considered as a winning game, if the sum of all the weights of the nodes in a coalition is greater than or equal to a predefined threshold weight. A node has a pivotal role if its removal transforms a winning game into a loosing game. Nodes with the aforementioned property are called swing nodes. A node that acts as a swing node in maximum coalitions is the most critical node and is assigned the highest Banzhaf power index.

This aforementioned idea is adopted in a communication network setting in order to characterize the criticality of nodes participating in the network. In the same way that weights are being used to select coalitions in a voting game setting, the proposed approach uses the link bandwidths in a communication network setting to select the nodes participating in shortest path formation. A coalition of nodes is considered as a winning coalition, if the path they form satisfies the bandwidth requirements of a particular source destination pair. Therefore, such links that cannot support these bandwidth requirements are discarded. Once a shortest path has been established, a node is called a swing node if it participates in the shortest path. The removal of a node that participates in maximum shortest path routes, will have a higher impact on network performance and is thus considered a critical node in the network. So, in analogy to the voting games setting, a node which acts as a swing node in maximum coalitions is the most critical node and is assigned the highest Banzhaf power index formally defined below.

In the graph $G = (V, E)$, I denotes the set of all source destination pairs $w = (i, j)$, $i, j \in V$. For each $w \in I$, $L(w)$ contains the set of nodes which constitute the shortest path route that fulfils the bandwidth requirements. A node k that belongs in $L(w)$ acts as a swing node for the source destination pair w. The Banzhaf power index for a node is the ratio between, the number of times a node acts as a swing node, over the total number of times all the nodes in V act as swing nodes. The Banzhaf power index is denoted by C_k and is given by:

$$C_k = \frac{\sum_{w \in I}(|L(w)| - |L(w) \backslash k|)}{\sum_{p \in V} \sum_{w \in I}(|L(w)| - |L(w) \backslash p|)} \tag{5.4}$$

5.2.3 Combined Banzhaf & Diversity Index *(CBDI)*

The proposed criticality metric is obtained by multiplying the diversity index and the Banzhaf Power Index as shown below:

$$CBDI(x) = C_x H(x) \tag{5.5}$$

The combination method used is a design parameter and this section is supported using simulations in section 5.4. The metric is referred to as Combined Banzhaf & Diversity Index (*CBDI*) and refines the mechanism of critical node detection. According to this index, a node is critical not only if it participates in maximum shortest path routes but if it is also prominent among its neighbours due to a higher variation in node attributes. The index, unlike previous approaches, is able to refine nodes which participate in the same number of shortest paths by differentiating between nodes which relay information from multiple inputs to multiple outputs and nodes which relay information from a single input to a single output. Further, it can identify nodes which can relay data to distant nodes thus having a high probability of experiencing heavy traffic. Finally, it is able to refine the information obtained by the node degree by excluding neighbouring nodes whose participation in path formation is not critical.

5.3 Algebraic Connectivity of a Network

Algebraic connectivity, also referred to as the Fiedler value, is a spectral metric defined as the second smallest eigenvalue of the Laplacian matrix of a network. Its significance stems from a theorem by Fiedler [32] which states that a network is disconnected, if and only if, the algebraic connectivity attains a value of zero. It has thus been conjectured that the algebraic connectivity can be used as a connectivity or robustness measure of the network in the sense, that the higher its value is, the more difficult it is to partition the network. Such a conjecture is supported by a number of theorems which offer insights towards this direction. The algebraic connectivity is related to the criticality of a node as it provides an analytical metric with which one can assess the degradation in network connectivity when the node is removed. This section reviews key definitions and theorems pertinent to the algebraic connectivity concept and also provides an insight on the key features of the proposed criticality metric.

Let $G = \{V, E\}$ be a graph of $|V| = n$ nodes and $|E| = m$ edges. If G is undirected then, $A(G) = (a_{ij})$ is the adjacency matrix of G with $a_{ij} = 1$ if nodes i and j share an edge $z \in E$ and $a_{ij} = 0$ otherwise, for $i, j \in V$. The diagonal degree matrix $\delta(G) = diag(deg_i, deg_{i+1}, ...deg_n)$ is an $n \times n$ matrix with the diagonal entry deg_i representing the degree of the node $i \in V$ and all non-diagonal entries equal to zero. The Laplacian matrix for such an undirected graph G is an $n \times n$ matrix, $L(G) = \delta(G) - A(G)$. In case of a directed graph, the Laplacian matrix is represented by $L(G) = N(G)N(G)^t$ where, $N(G)$ denotes the incidence matrix [65]. The incidence matrix $N(G)$ is an $n \times n$ matrix with $n_{ij} = 1$ if an edge is directed from node i to j, $n_{ij} = -1$ if the edge is directed from node j to i and $n_{ij} = 0$ otherwise. The laplacian matrix $L(G)$ of a graph is real, symmetric and non-negative semi-definite with all its eigenvalues being real and non-negative [48]. These eigenvalues are highly correlated with the connectivity of a graph and this relation is further elaborated in the following lemma [71].

Lemma 1: If $0 = \lambda_0(G) \leq \lambda_1(G) \leq ... \leq \lambda_{n-1}(G)$ are the eigenvalues of the Laplacian matrix L in an ascending order, then $\lambda_1(G) > 0$ if G is connected. Additionally, if $\lambda_i(G) = 0$ and $\lambda_{i+1}(G) \neq 0$, then G has exactly $i+1$ disjoint connected components.

The zero row and column sum of the Laplacian matrix generates an eigenvalue of zero which is considered as the smallest eigenvalue λ_0 of the matrix. The aforementioned lemma indicates that if a graph is connected then the eigenvalue of zero will have a multiplicity of one whereas, if the eigenvalue of zero has a multiplicity of j then there are j disconnected components of the graph. Similar to the smallest eigenvalue, the largest eigenvalue $\lambda_{n-1}(G)$ also has a multiplicity of 1 if the graph is connected [60]. The largest eigenvalue is upper bounded by the maximum degree D_{max} and lower bounded by $max\ (\bar{D}(G), \sqrt{D_{max}(G)})$ [60].

Apart from the smallest and the largest eigenvalues, the second smallest eigenvalue λ_1, which is also referred to as the Fiedler value, is of vital importance for determining the connectivity of a graph [32]. A higher order Fiedler value, which is strictly larger than zero, shows a connected graph whereas, a smaller value shows a weakly connected graph. It is lower bounded by the smallest eigenvalue of zero and upper bounded by the minimal nodal degree of the network. The minimal nodal degree defines the minimum number of links that if broken could possibly result in another disconnected component and hence, the bounds on the Fiedler value can be expressed as [48]:

$$0 \leq \lambda_1(G) \leq \frac{n}{n-1} D_{min}(G) \tag{5.6}$$

Here, D_{min} is the minimal nodal degree of an incomplete graph. The above inequality indicates that the algebraic connectivity can be used as a connectivity robustness measure. The smaller the D_{min} value, the easier it is for the network to become disconnected as fewer node removals are required to lead to network partitioning. As D_{min} decreases, so does the upper bound on the algebraic connectivity and one may thus conjecture that the easier it is for the network to become disconnected the more likely it is for the algebraic connectivity to attain a small value. Reversing the argument, one may conjecture that the smaller the algebraic connectivity value, the easier it is for the network to become disconnected. The use of the algebraic connectivity as a connectivity robustness measure can be further supported by the following lemma [48][32]:

Lemma 2: If there are two edge disjoint graphs with the same number of nodes G_a and G_b, then $\lambda_1(G_a) + \lambda_1(G_b) \leq \lambda_1(G_a \cup G_b)$.

Corollary 1: Likewise, if there are two graphs with the same number of nodes but different set of edges, such that $G_a(V, E_a)$ and $G_b(V, E_b)$ for $E_a \subseteq E_b$ then the Fiedler value is non-decreasing and can be represented as, $\lambda_1(G_a) \leq \lambda_1(G_b)$.

Corollary 1 suggests that the removal of edges from a network, which makes it easier for the network to become disconnected, leads to a decrease in the algebraic connectivity. Again reversing the argument one can conjecture that the smaller the algebraic connectivity value is, the easier it is for the network to become disconnected. The effect of removing edges from the network on the algebraic connectivity is captured by Corollary 1. Removal of nodes is also of primal importance as the criticality of a node is assessed by its impact on the network performance when it is removed. The following Lemma describes how the algebraic connectivity is affected by node removal.

Lemma 3: If G_1 is the resultant graph after removal of k vertices along with all the adjacent edges, then:

$$\lambda_1(G_1) \geq \lambda_1(G) - k$$

The Lemma suggests that the removal of nodes decreases the lower bound on the algebraic connectivity. This means that by appropriate choice of the nodes, one can decrease the algebraic connectivity thus making it easier for the network to become disconnected. The above properties of the algebraic connectivity are now used to explain how a key feature of the proposed criticality metric, namely the weighted node degree, identifies more critical nodes than if the normal degree was used.

Assume an arbitrary network G_1 and an arbitrary node within the network u_1. The weighted degree of any node becomes higher when the number of common neighbours with all its neighbours becomes smaller. The number of common neighbours can be reduced by removing particular edges of the network. Edges are chosen which do not affect the degree of node u_1 and are removed to yield network G_2. G_1 and G_2 have the same number of nodes. Node u_1 maintains its degree in G_1 and G_2, however, its weighted node degree in G_2 is higher. Since u_1 has the same node degree in G_1 and G_2, its removal will result in G_2 having less edges than G_1 by construction. From Lemma 3 one can thus conclude that:

$$\lambda(G_2) \leq \lambda(G_1) \tag{5.7}$$

The above indicates that when nodes with the same node degree but higher weighted node degree are removed then the algebraic connectivity of the network decreases. The weighted node degree can thus be used to refine the node degree concept and identify more critical nodes.

5.4 Performance Evaluation

This section discusses the performance evaluation of the proposed criticality index using simulations conducted on Matlab [61] and the Network Simulator (NS-3) [69]. A comparative study was conducted, the objective of which was to investigate the performance of the proposed index against other approaches that have appeared in the literature: the Hybrid Interactive Linear Programming Rounding (HILPR) algorithm proposed in [83], the algorithm in [59] (Cont) which attempts to reduce the rank of the routing matrix and the node centrality metrics such as the betweenness centrality, closeness centrality and degree centrality metrics that are used in [35]. Among all criticality indices proposed in literature the aforementioned indices were chosen as they contain some of the features included in the proposed approach, namely the diversity, the node degree and the participation in shortest paths. In addition, they have been shown to outperform the other proposals in a number of scenarios. In each conducted simulation experiment, nodes participating in the network are assigned a criticality measure based on the criticality index under consideration. A fixed percentage of the most critical nodes were removed and the degradation in network performance was evaluated. The most effective criticality index is the one that leads to a greater degradation in performance.

In the first set of simulation experiments conducted on Matlab network performance was evaluated in terms of topological performance metrics, in the second set of simulation experiments network performance was evaluated in terms of the algebraic connectivity of the network and in the third set of simulation experiments conducted on the NS-3 simulator, network performance was evaluated in terms of the network centric performance metrics.

5.4.1 Topology Based Evaluation

The first set of simulation experiment conducted on Matlab evaluates the ability of the proposed metric to choose critical nodes in terms of topology based performance metrics such as the Average Node Degree, the Average Path Length and the Number of Isolated Nodes. The *Average Node Degree* is the average number of neighbours of all nodes participating in the network. Small average node degree values imply smaller connectivity and so the smaller the average node degree, the greater is the degradation in network performance. The *Average Path length* is obtained by calculating the average of all path lengths over all source destination paths in the network. High average path length in a network implies lack of critical nodes which can participate in shortest path routes. So, the higher the average path length, the greater is the degradation in network performance. Finally, the *Number of Isolated Nodes* are the nodes that have no connections with any other node in the network. High number of isolated nodes is undesirable as it implies greater network partitioning.

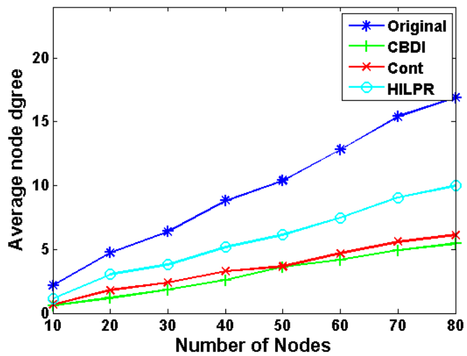
The evaluation was conducted using three different network topologies in an area of $1000 \times 1000m^2$.The *Random Network Topology* assumes x and y coordinates of the nodes which are uniformly distributed in the area under consideration. The number of nodes were chosen in the range of $10 - 80$ and among them 90% of the nodes were assumed to have a constant transmission range equal to $300m$ whereas, some randomly selected 10% of nodes were assigned a transmission range of $450m$ in order to enable long distance links [10]. In the *WaxMan Network Model* [100], the probability that a connection is established between any two randomly distributed nodes u, v in the network $P(u, v)$ depends on the distance d between the nodes as shown below:

$$P(u, v) = \alpha e^{-d/bL} \tag{5.8}$$

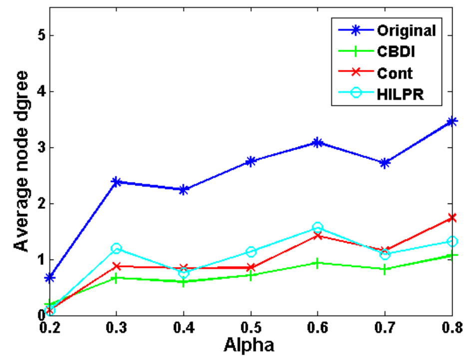
where $0 < \alpha < 1$ and $b <= 1$ are constants and L is the maximum distance between any two nodes. As α increases, the probability of having edges between two nodes increases, whereas, with the increase in b, the ratio of long distance to short distance edges increases. The simulation experiments presented later in this section consider a fixed number of nodes of 80 and considers a constant value of $b = 0.5$. In order to analyse the effect of node density on the performance of the network, the value of α is varied from $20 - 80\%$. Finally, in the *Small World Network Model* [99], N nodes form a one-dimensional lattice with each node placed uniformly on the boundary of a circle. Each node in the network forms a direct connection with its k^{th} nearest neighbours, where k is a constant and it represents the edge connectivity of the network. In this network topology, a network size varying from $20 - 80$ was considered, with a fixed edge connectivity of $k = 2$. In addition, 10% of the edges were randomly re-wired to introduce the long range links in the network. These long range links reduce the average path length between the nodes.

In each of these topologies, the criticality metric was evaluated by removing the selected critical nodes from the network and then measuring the network performance. In order to reduce the variance of the obtained results, each simulation experiment was repeated 50 times and the values presented, are averages over all obtained outputs. All the simulation in this section assume a fluid flow model of the network and the bandwidth of each node is randomly selected according to a uniform distribution with a maximum value of 2Gbits/sec. Information sources are assumed to be non-responsive and their data rate is chosen from a uniform distribution in the range 0-2Gbits/sec. In each experiment, the performance of the reference network (referred to it as the original network) was evaluated and then compared with the performance of the network when 20% of the total nodes were removed. The nodes which were removed are the ones which had been assigned the highest criticality value according to the criticality index under investigation.

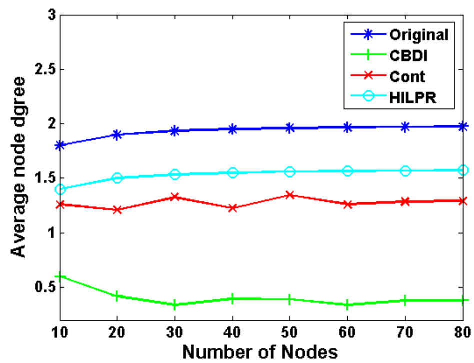
Fig 5.3 for each network topology shows the average node degree values obtained in the original network and compares it with the values obtained when the most critical nodes were removed using the three criticality metrics under investigation. For the Random Network Topology, and the Small World Topology, the average node degree is plotted against the number of nodes within the network. In the WaxMan Topology, the average node degree is plotted against the parameter α of the model which is a measure of the edge density within the network. The greater the value of α, the greater is the edge density and thus the number of edges. It is noticeable that in all cases, the proposed CBDI criticality metric achieves a larger reduction in the average node degree, a strong indication of a greater degradation in network performance. This



(a) Random Network Topology



(b) WaxMan Network Topology

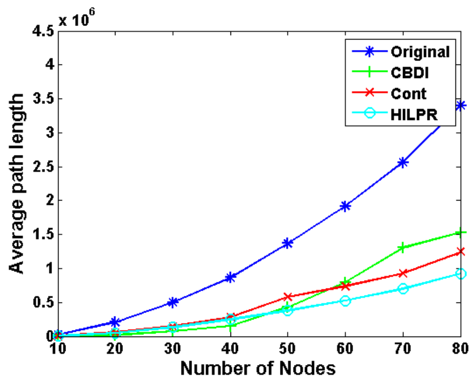


(c) Small World Network Topology

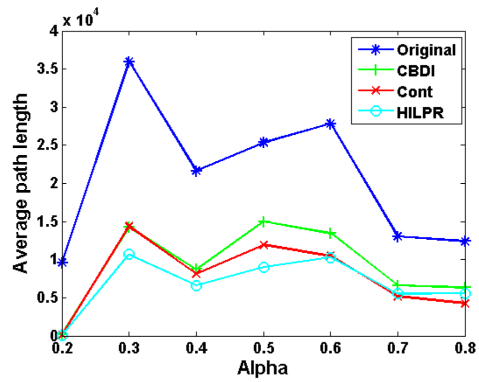
Figure 5.3: Average Node Degree versus the number of nodes and α for the *Original* network and when nodes are removed using the *CBDI*, *Cont* and *HILPR* algorithms, in three different network topologies.

implies that the nodes removed using the proposed CBDI metric are more critical. The highest impact of the proposed approach compared to the others is observed in the Small World Topology whereas, the smallest impact is reported in the Random Network Topology. It is worth noting that in the Random Network Topology as the number of nodes increases, so does the average node degree. This is expected due to the increase in node density. A similar pattern is observed in the WaxMan Network

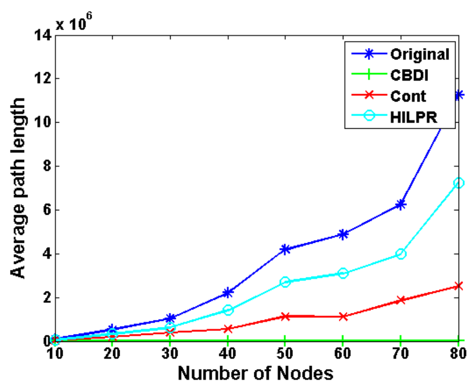
Topology, however, the increase rate is smaller. For the Small World topology, the average node degree is fairly constant with increasing number of nodes due to the nature of the model which assumes a constant value for the average node degree equal to 2.



(a) Random Network Topology



(b) WaxMan Network Topology

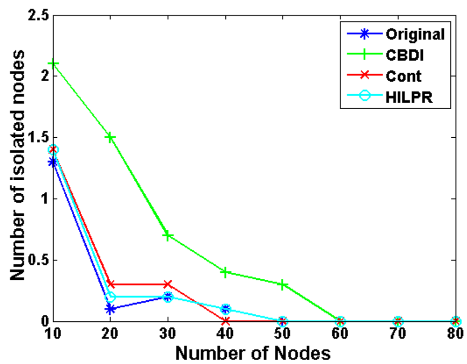


(c) Small World Network Topology

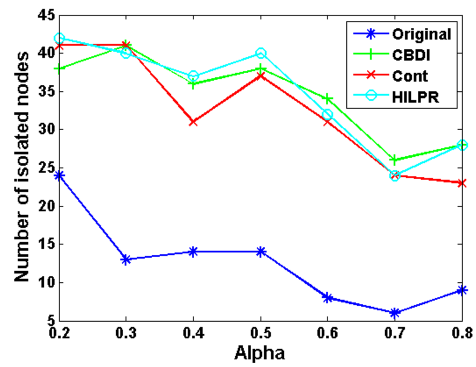
Figure 5.4: Average Path Length versus the number of nodes and α, for the *Original* network and when nodes are removed using the *CBDI*, *Cont* and *HILPR* algorithms, in three different network topologies.

Fig 5.4, for each considered network topology, we show the Average Path Length reported in the original network and the network resulting from the removal of the critical nodes. The critical nodes were chosen using the proposed criticality metric and the other two metrics under consideration. Higher Average Path Length values are desirable, when removing critical nodes, as they imply the removal of nodes which participate in shortest paths. It is observable that, the proposed metric, is able to slightly increase the average path length in the WaxMan and Random Network Topologies, at high α and number of node values respectively. This is expected due to a higher variability in node attributes when increasing the node density. In the Small World Network almost zero path length values are reported by the CBDI metric due to the large number of isolated nodes that it creates.

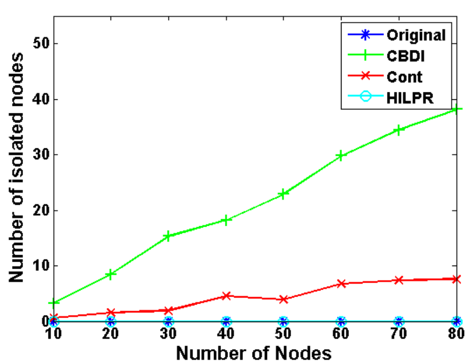
Finally, Fig 5.5 shows the number of isolated nodes reported in each of the network topologies under consideration. The number of isolated nodes is shown for increasing values of the number of nodes and α in the original network and when the critical nodes have been removed using the considered criticality metrics. The results demonstrate the superiority of the proposed metric, especially in the case of the Random Network Topology and the Small World topology. In all three topologies, the removal of critical nodes using the proposed CBDI criticality metric yields a larger number of isolated nodes implying a severe degradation in network performance. Increasing number of isolated nodes suggests that the network becomes increasingly intermittent in nature. It is worth noting that, in the Random Network Topology and the WaxMan Network Topology, as the number of nodes and α increase, the isolated nodes decrease. This is expected due to the fact that an increase in the node or edge density makes isolation of nodes more improbable. On the other hand, in the case of the Small World Topology as the number of nodes increases, so does the number of isolated nodes. This is due to the fact that in this topology the average node degree is fixed, which means that as the number of nodes increases, the number of nodes removed also increases which renders more nodes to become isolated. The fact that the node degree is originally fixed yields zero isolated nodes in the original network, as shown in Fig 5.5.



(a) Random Network Topology



(b) WaxMan Network Topology



(c) Small World Network Topology

Figure 5.5: Number of Isolated nodes versus the number of nodes and α, for the *Original* network and when nodes are removed using the *CBDI*, *Cont* and *HILPR* algorithms, in three different network topologies.

5.4.2 Algebraic Connectivity Evaluation

This section builds on the argument presented in section 5.3 about the use of algebraic connectivity as a robustness metric for the connectivity of a network and it is used here to show that the proposed criticality metric and key constituents such as the weighted node degree and the variation in link length outperform other proposals which have been proposed in literature. The evaluation has been simulative with the experiments conducted on Matlab. The Random Network Topology was considered. The number of nodes in the considered area were chosen in the range $20-80$, and the 10% most critical nodes were removed each time.

The first experiment compares the proposed weighted node degree against the node degree metric. The weighted node degree aims at refining the criticality assessment of the normal degree metric by taking into account one hop paths which are identified by the existence of common neighbours. The reported algebraic connectivity values for various number of nodes are shown in Fig 5.6 for the original network, for the network when 10% of the most critical nodes are removed according to the weighted node degree metric and when they are removed according to the degree centrality metric. It is observed that weighted node degree achieves the most significant reduction in the algebraic connectivity value. Since the algebraic connectivity is a connectivity robustness metric it follows that the weighted node degree renders the network more susceptible to network partitioning indicating that it is more successful in identifying the most critical nodes.

The next experiment uses the algebraic connectivity to compare the variation

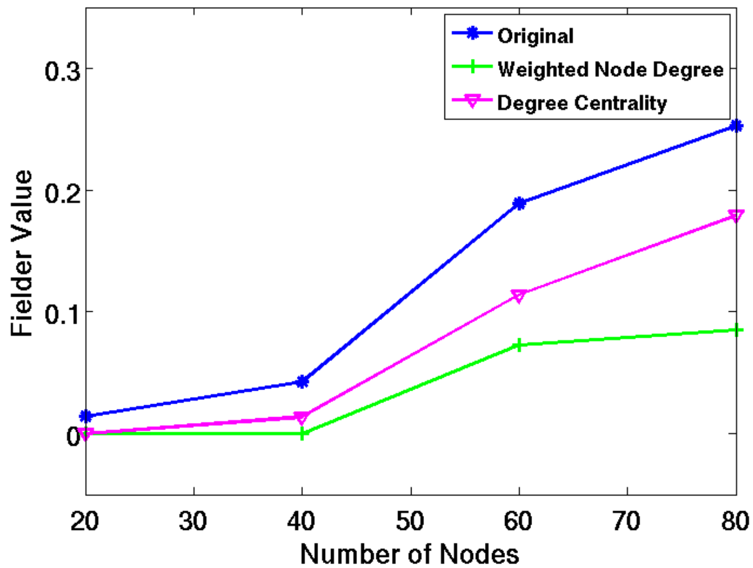


Figure 5.6: Comparison of the weighted node degree and the degree centrality metrics in terms of the algebraic connectivity for different number of nodes in a Random Network Topology.

in link length against the closeness centrality metric and the betweenness centrality metric. The variation in link length uses local information (neighbouring link length information) to identify nodes which are likely to act as relay nodes thus accommodating a large number of active connections. The number of active connections at a node is also considered by the betweenness centrality metric which, however, requires full network information in order to calculate all shortest paths in the network. Fig 5.7 shows the reduction in the algebraic connectivity achieved by the closeness centrality, the betweenness centrality and the proposed variation in link length. It is noticeable that, the betweenness centrality and the variation in link length achieve the most severe reduction in the algebraic connectivity indicating that they are able to best assess the criticality of the nodes. In addition, it is clear from the figure that despite the fact that the variation in link length requires only local information its performance is comparable to that of betweenness centrality.

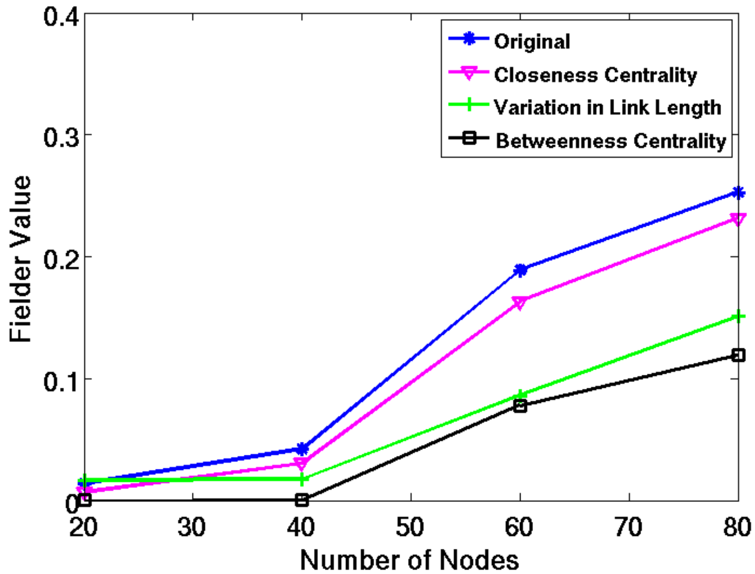


Figure 5.7: Comparison of the Variation in Link Length, closeness centrality and and betweenness centrality metric in terms of the algebraic connectivity for different number of nodes in a Random Network Topology.

Finally, the algebraic connectivity is used to compare the performance of the proposed CBDI metric against the performance of the HILPR scheme and the Cont Scheme. The results are shown in Fig 5.8. We observed that the CBDI scheme removes nodes which reduce the algebraic connectivity to the greatest extent, indicating that the connectivity of the network is mostly affected. The Cont scheme achieves a smaller reduction, while the HILPR scheme leads to a slight increase in the algebraic connectivity despite the node removal.

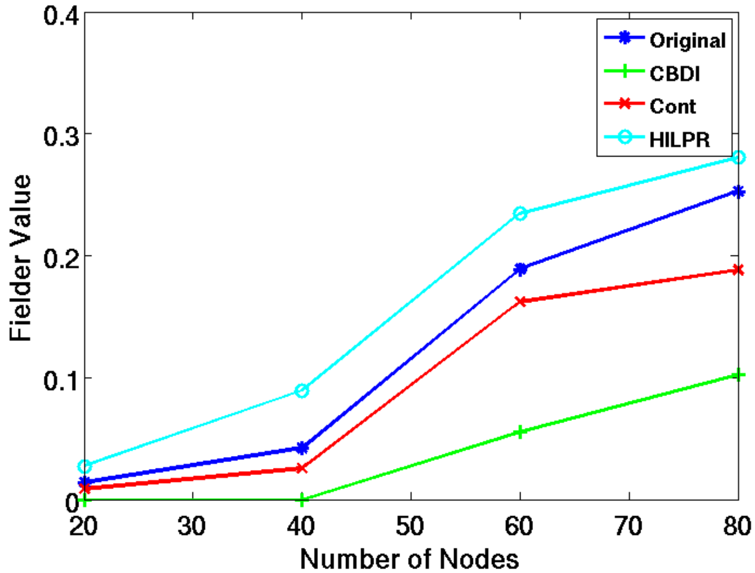


Figure 5.8: Comparison of the proposed CBDI metirc with the existing HILPR and Cont metrics in terms of the algebraic connectivity for different number of nodes in a Random Network Topology.

5.4.3 Network Centric Evaluation

The final set of experiments aim at evaluating the performance of the proposed criticality metric in more realistic network scenarios. Simulation experiments were conducted on NS-3 Simulator (NS-3) [69] for the evaluation of network performance using network centric performance criteria such as the total throughput, the average per packet delay, the average per packet jitter and the number of packet drops. In all the simulations the Random Network Topology was used to evaluate the performance of the proposed criticality metric against metrics such as: Cont [59], HILPR [83], Degree centrality, closeness centrality and betweenness centrality [34].

The evaluation was conducted on a wireless adhoc network of 100 nodes which were uniformly distributed in an area of $1500 \times 1500m^2$ thus forming a Random Network

Topology. Each node was equipped with a 802.11b transceiver with a transmit power of $7.5dbm$. Out of all the nodes in the network, 15% had the option of transmitting at a power of $1.5 \times 7.5dbm$ [10] thus forming long range communication links. The degradation in signal strength as a function of the distance covered was represented by the Friss loss propagation model. A randomly selected set of 20 source/sink pairs initiate the communication in the network by transmitting packets at a rate of $2.048Kb/s$ each. Packet based transmission was assumed with the packet size set to $64byte$ packets. Routing paths within the network were formed using the OLSR routing protocol [62]. All measurements were obtained in the interval $100-300$ seconds after the start of the simulation. This provides sufficient time for the OLSR algorithm to converge to its equilibrium state. The degradation in network performance was evaluated after 10% of the most critical nodes are removed from the network. This process was repeated 10 times with the results averaged to decrease the stochastic uncertainty of the obtained results.

To begin with, the performance of the proposed criticality metric was evaluated against the HILPR and Cont Algorithms in terms of the throughput achieved. The throughput is defined as the total number of packets delivered to their destinations within the network per unit time. Fig 5.9 shows that the achieved throughput is a function of time when 10% of the nodes are removed using the three metrics under consideration. It is observed that, the CBDI algorithm reports the largest decrease in the achieved throughput relative to the original network before node removal. This demonstrates that the proposed algorithm is successful in choosing more critical

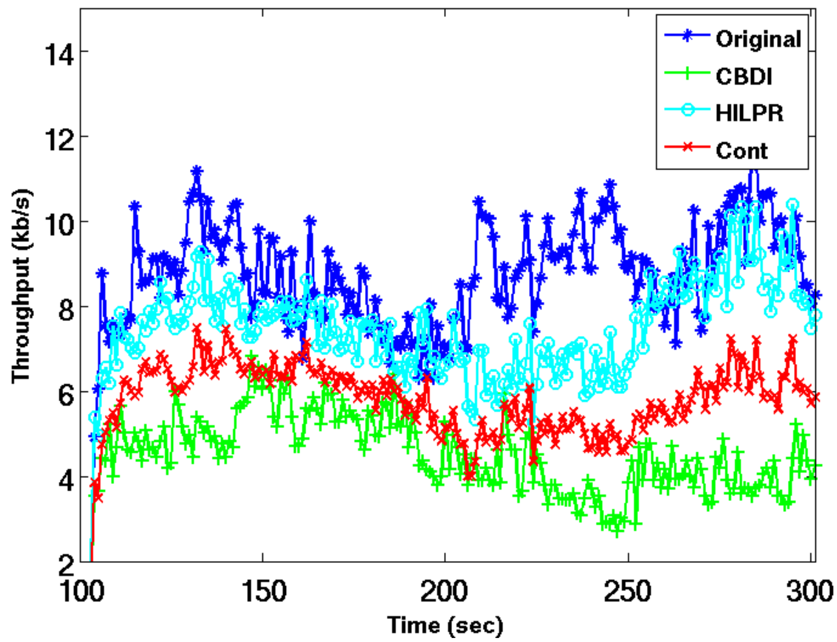


Figure 5.9: Time evolution of the network throughput for the original network and when nodes are removed according to the *CBDI*, *HILPR* and *Cont* metrics.

nodes. The decrease in average throughput observed at certain periods of time is due to long range link enabled nodes attempting to transmit at that time. Since their transmission power is higher, they attempt to reserve a larger portion of the common communication medium, thus increasing the probability of collisions and leading to throughput degradation.

Next, the achieved throughput was used as the performance metric in order to compare key components of the proposed CBDI metric against similar approaches which exist in the literature. The first comparison evaluates the weighted node degree metric against the degree centrality metric. The proposed weighted node degree refines the degree centrality metric by considering as more critical, nodes which have small number of common neighbours with their neighbours. Smaller number of com-

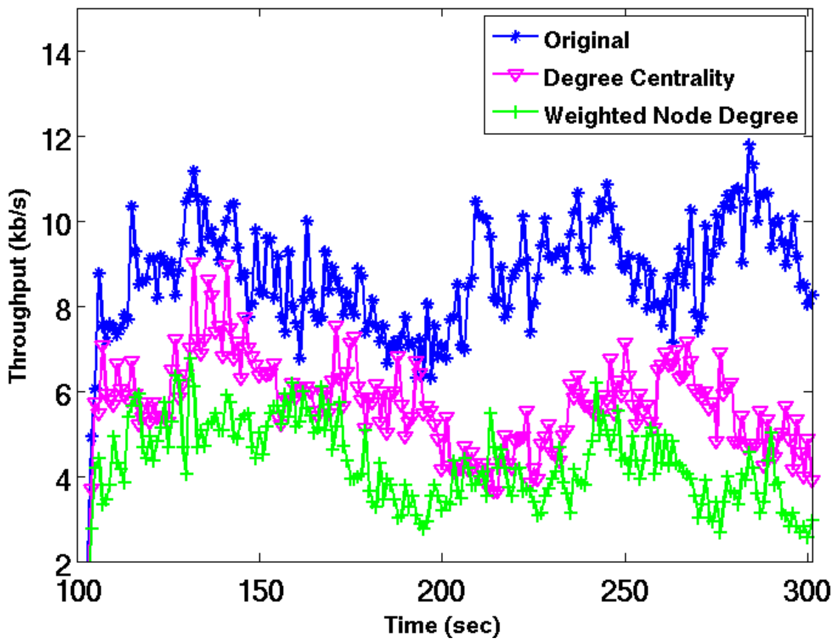


Figure 5.10: Time evolution of the network throughput for the original network and when nodes are removed according to the *Degree Centrality* and *Weighted Node Degree* metrics.

mon neighbours indicates smaller number of one hop path alternatives when the node is removed. So, upon removal of a node with high criticality, it is easier for the network to become disconnected thus increasing the probability of reporting a smaller throughput. This is in fact what is reported by the simulation results presented in Fig 5.10. When removing nodes identified as critical using the weighted node degree, a larger degradation in throughput is achieved compared to node removal using the degree centrality metric. This demonstrates the superiority of the weighted node degree metric.

The next comparison evaluates the proposed variation in link length metric against the betweenness centrality and the closeness centrality metrics. All three approaches

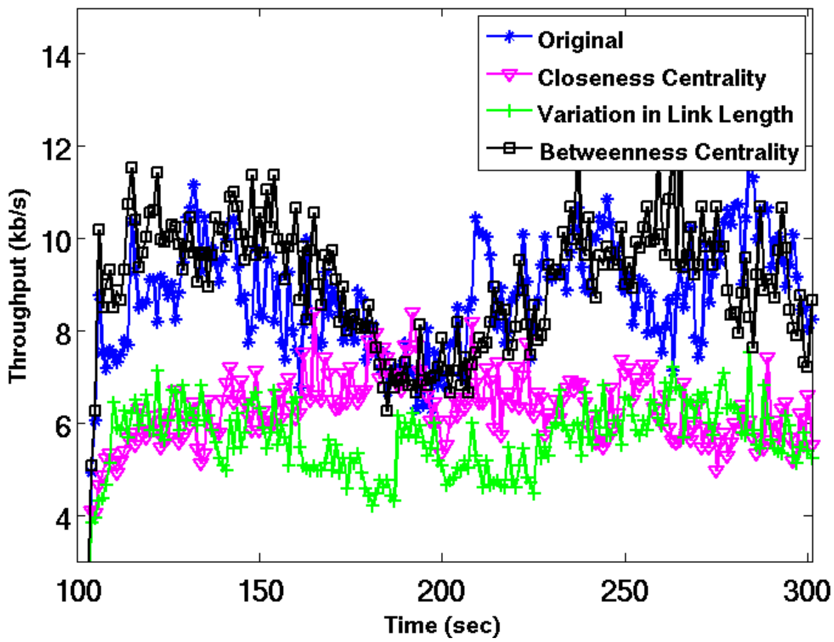
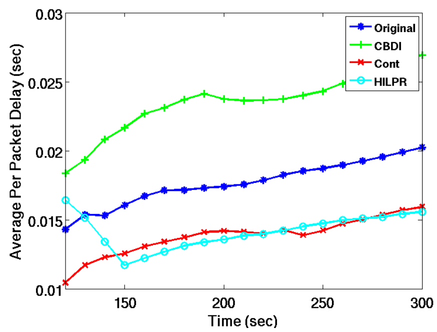
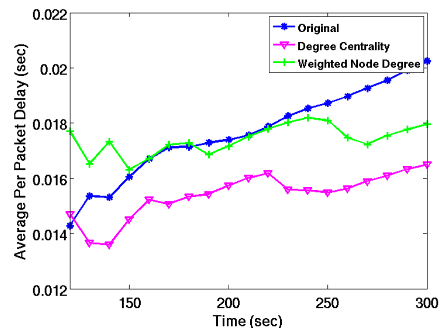


Figure 5.11: Time evolution of the network throughput for the original network and when nodes are removed according to the *closeness centrality*, *betweenness centrality* and *Variation in Link Length* metrics.

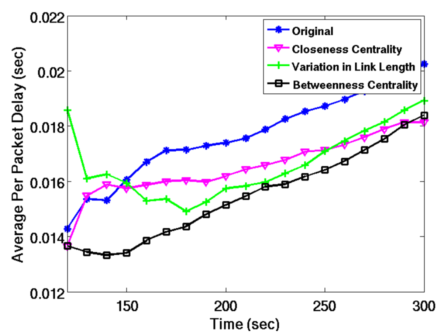
aim at identifying nodes which accommodate the largest number of active connections. However, the closeness centrality and the betweenness centrality metrics use global network information whereas, the variation in link length utilizes local information only to achieve the same thing. The throughput achieved for the original network and when nodes are removed according to the various metrics are shown in Fig 5.11. The closeness centrality and the variation in link length achieve significant reduction in the throughput achieved. It is really striking to note that the betweenness centrality metric reports similar throughput to the original network prior to node removal. A possible explanation is the existence of alternative paths which upon node removal continue to render the network, ensuring high network throughput.



(a)



(b)



(c)

Figure 5.12: Time evolution of the average per packet delay when nodes are removed based on a) *CBDI*, *Cont* and *HILPR*, b) *degree centrality*, *Weighted Node Degree*, c) *closeness centrality*, *betweenness centrality*, *Variation in Link Length*.

Based on the above stated results, further experiments were conducted, aiming at comparing the proposed criticality metric and its key constituents against other approaches, using other performance metrics. The delay experienced by packets in transit is an important network attribute which describes its performance. Low delays are preferable. In wireless ad hoc networks, such as the one considered in this section, delays are due to a number of reasons: network congestion resulting in queuing delays, poor channel behaviour, resulting in re-transmissions and contention resulting in large vacant medium delay times due to the CSMA/CA mechanism. The first performance evaluation metric that is considered in this section is the average per packet delay. This is calculated by dividing the total number of delays observed with the number of delays transmitted throughout the simulation time. Fig 6.7 shows the time evolution of the average per packet delay reported in the original network and when nodes are removed according to a number of proposed criticality metrics including the proposed criticality metric and its key constituents. It is observed that, the proposed CBDI metric is able to bring a major degradation in performance as the average per packet delay increases significantly when nodes are removed. In addition, the weighted node degree does not on average increase the per packet delays however, it does manage to outperform the degree centrality metric which reports smaller per packet delay values. When the variation in link length is now compared to the closeness centrality and the betweenness centrality metrics, it is observed that, they eventually exhibit similar behaviour by decreasing the per packet delays compared with the original network. However, what is important is that despite individual constituent elements not always

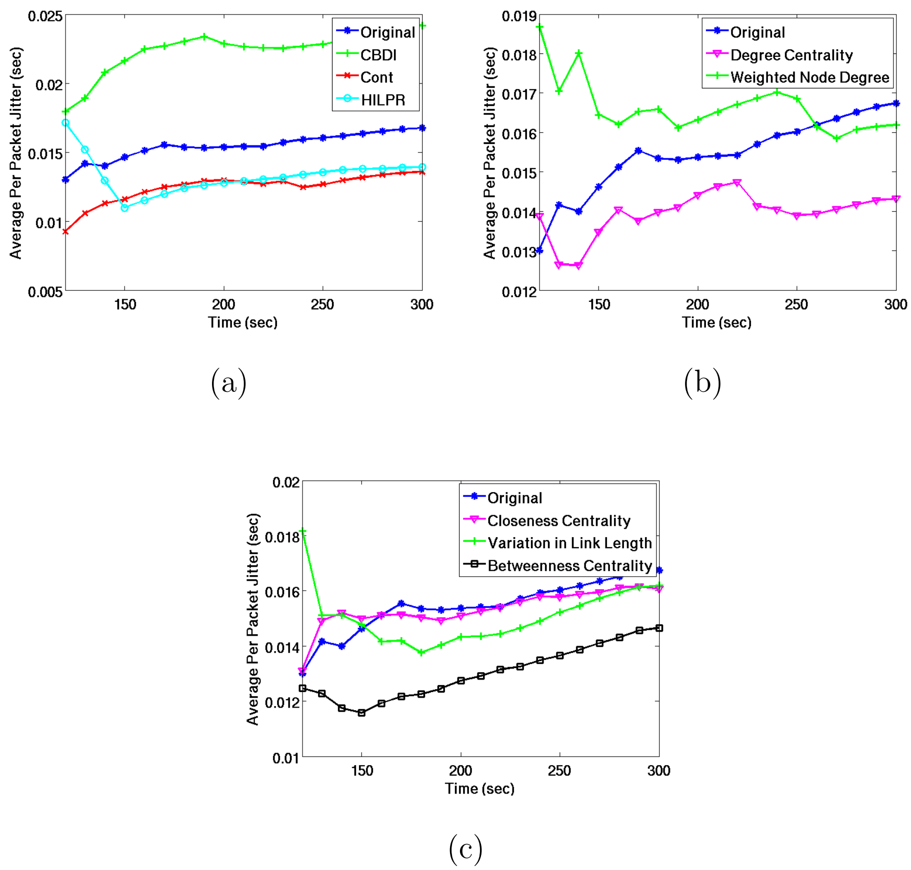


Figure 5.13: Time evolution of the average per packet jitter observed when nodes are removed based on a) *CBDI*, *Cont* and *HILPR*, b) *degree centrality*, *Weighted Node Degree*, c) *closeness centrality*, *betweenness centrality*, *Variation in Link Length*.

outperforming other proposals, when combined, achieve a significant degradation in network performance.

The next performance metric under consideration is the average per packet delay jitter. This is calculated by dividing the total delay jitter observed throughout the simulation experiment with the total number of transmitted packets. The delay jitter is calculated as the variation in packet reception times at the receiver. Increasing delay jitter values indicate increasing congestion within the network, so small delay jitter values are preferable. Fig 6.8 shows the time evolution of the average per packet delay jitter observed in the original network and when nodes are removed according to various criticality metrics. It is observed that the proposed CBDI metric outperforms the other proposals as it manages to significantly increase the delay jitter thus degrading network performance. The same applies for the weighted node degree which is also observed to increase the delay jitter. The picture is different in the case of the variation in link length which is shown to decrease the average delay jitter relative to the original network and the closeness centrality metric. However, as mentioned above, despite individual elements, such as the variation in link length, not outperforming other proposals, when these are combined, cause the proposed CBDI metric to cause major degradation in network performance.

The final performance metric under consideration in this section is the total number of dropped packets. High number of dropped packets in the network due to buffer overflow, is a strong indication of congestion. When nodes are removed from the network, the number of available paths decreases and the remaining paths are forced to accommodate all traffic. This makes them more vulnerable to congestion. When critical nodes are removed, congestion is expected to be more severe and the number of dropped packets is thus higher. The results of the conducted simulation experiments are shown in Fig 6.9. It is observed that, during the whole simulation time the proposed CBDI scheme is able to bring a major increase in the number of dropped packets compared to HILPR and Cont Algorithms. The other two algorithms report packet drops similar to the ones reported prior to node removal. Fig

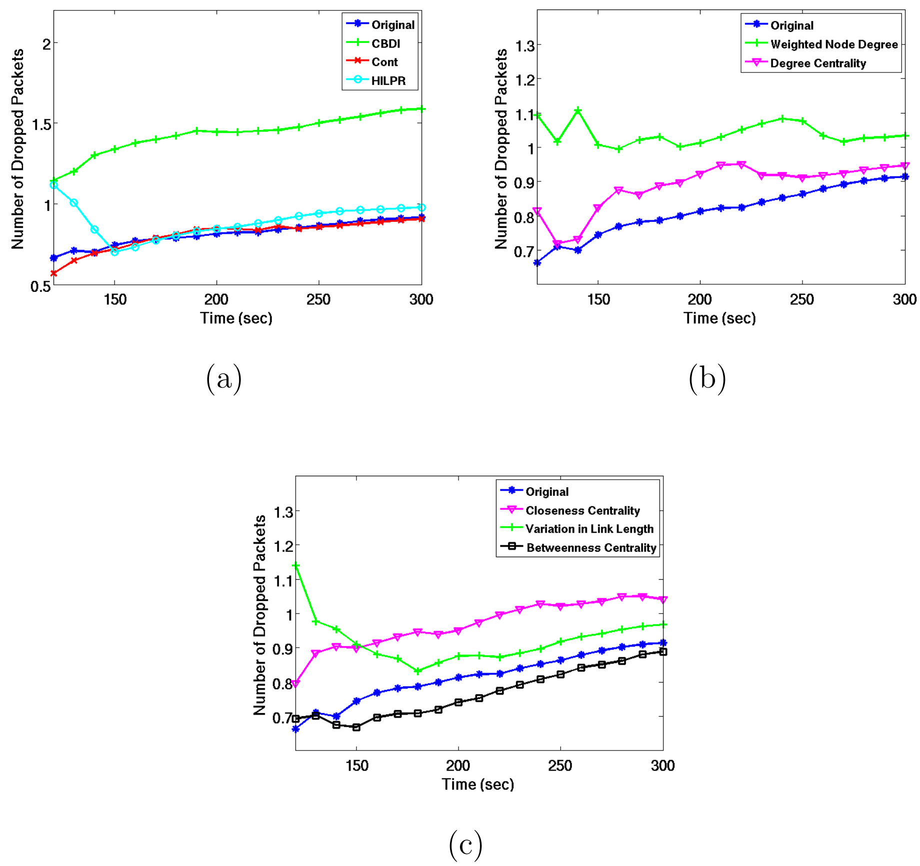


Figure 5.14: Time evolution of the total number of packets dropped when nodes are removed based on a) *CBDI*, *Cont* and *HILPR*, b) *degree centrality*, *Weighted Node Degree*, c) *closeness centrality*, *betweenness centrality*, *Variation in Link Length*.

6.9 also highlights the superiority of the weighted node degree relative to the degree centrality metric. Both cause the number of packets dropped to increase, however the increase achieved by the weighted node degree is higher. The picture for the variation in link length is different. While the variation in link length leads to an increase in the number of dropped packets the closeness centrality metric reports an even higher number. The betweenness centrality metric in fact reports a slight decrease in the number of dropped packets. This is consistent with the throughput performance analysis analyzed earlier. Despite the fact that the closeness centrality exhibits superior performance relative to the variation in link length metric, the superiority of the other constituent elements of the proposed criticality metric render it to be more successful than other metrics proposed in literate. In addition, as mentioned before, the variation in link length requires only local information whereas the closeness centrality requires full network information thus increasing the implementation complexity.

5.5 Summary

This chapter highlights the contribution of critical nodes in network operation and demonstrates how the network reacts when these critical nodes are affected. It proposes a new criticality index which is based on the diversity of node attributes within the network and the participation of each node in forming shortest path routes. It also presents a detailed evaluation of performance of the proposed metric under various network topologies using multiple performance metrics and it is observed that the proposed metric outperforms existing approaches by showing a greater degradation in network performance when the critical nodes, selected using this index, are removed from the network.

Chapter 6

Optimization Based Spectral Partitioning for Node Criticality Assessment

6.1 Introduction

The identification of critical nodes is vital for accessing network vulnerability and security [9]. The failure of a few critical nodes can have an adversarial effect on network performance varying from slight degradation in the Quality of Service up to the complete breakdown of the network [47]. The significance of critical nodes has been highlighted in a number of examples most of which are explained in chapter 1 & 5. Some of these algorithms are based on intuition, whereas others are based on mathematical abstractions of networks of arbitrary topology and are thus characterized by properties which can be verified analytically prior to implementation. This chapter adopts the latter approach and casts the node criticality problem in an optimization based framework. This formulation is divided into two optimization problems: an algebraic connectivity minimization problem, which addresses the topological aspects of node criticality and a min-max aggregate utility problem which addresses the connection oriented nature of the node criticality. The problems are related in depth as the connections can only establish source-destination paths on the underlying topology. However, we treat them as two separate problems and we consider suboptimal solutions for both problems which are combined to yield the proposed criticality identification scheme. The proposed criticality identification scheme is then derived by combining suboptimal solutions for both these problems.

In order to characterize the topological notion of node criticality, a node is considered critical when it contributes mostly to keeping the network connected or alternatively when its removal leads to a minimization of the network connectivity. A popular metric which characterizes the connectivity of a network is the algebraic connectivity. The metric was introduced by Fiedler in [32] and is defined as the second smallest eigenvalue of the Laplacian matrix of the network. It has been established in a number of studies [32][26][63] that algebraic connectivity serves as a good measure of connectivity robustness in the sense that the smallest its value is, the closer the network is in becoming disconnected. So, the first optimization problem under consideration in this chapter is the problem of finding the nodes which, when removed, minimize the algebraic connectivity of the network. A basic but tedious approach to solve the aforementioned problem is to use an exhaustive search over all sub-graphs which result from the removal of each node of the network. This approach assumes knowledge of the entire network topology and can thus become computationally expensive when dealing with large network structures. In addition, when multiple critical nodes need to be found, the approach becomes computationally expensive with the number of subgraphs that need to be considered increasing combinatorially with the network size. For this reason, a number of suboptimal solutions have been proposed in literature [57][96][102][20]. These suboptimal solutions utilize the elements of the Fiedler vector which is the eigenvector associated with the second smallest eigenvalue of the Laplacian of the network. Each element of the eigenvector naturally corresponds to a node in the network. The most popular suboptimal node criticality metric is the aggregate squared difference of Fiedler vector elements between neighbouring nodes [57][96] which has been shown to approximate the optimal solution using both analysis and simulations. Recent advances, which allow the distributed calculation of the Fiedler vector values [14] have enabled the distributed implementation of the proposed criticality metric. However, the main drawback of the distributed implementation is that a global maximisation consensus algorithm must be employed which can be slow and significantly increases the convergence time.

This thesis adopts an alternative approach to obtaining a suboptimal solution of the original algebraic connectivity minimization problem by employing spectral partitioning concepts. It is well known that the elements of the Fiedler vector assume positive and negative values in the range $[-1, 1]$ and that a splitting value s can be used to partition the network in two clusters (the first cluster containing all the nodes with corresponding Fiedler vector values less than s). Different values of s yield different types of cuts such as bisection, ratio cut, sign cut and gap cut [32]. The Fiedler clusters are known to be well connected [14] and in addition it has been shown that for various types of networks [88], which go beyond double community structures, they possess the desired property that they have nearly equal number of vertices with minimum number of edges in-between them [63]. In this chapter, based on the latter property, a node is considered critical if it lies on the boundary of the Fiedler clusters. This is achieved by adopting the sign cut approach which leads to a node being considered critical if it has at least one neighbour with a corresponding Fiedler vector value of different sign. This approach is attractive to be implemented in a distributed manner and allows each node to decide by itself whether it is a critical node. In addition, it is demonstrated here that, this approach is directly related to the approach in [57][96] as the nodes which lie on the boundary of the Fiedler clusters report high values of the aggregate squared Fiedler vector value differences, which is the criticality metric proposed therein. However, when a single critical node is required and a maximization algorithm needs to be employed, the proposed algorithm offers the advantage that it significantly reduces the distributed computational complexity as the maximization algorithm needs to be applied only over a reduced set of nodes, namely the ones which have the same Fiedler vector element sign. It is also demonstrated through simulations that significant reduction in convergence time is achieved, and along with this the solution is near optimal, in the sense that it approximates to a very good extent, a lower bound on the achieved algebraic connectivity which we derive analytically.

As pointed out above, the proposed change of sign method can lead to multiple nodes being detected as critical and so, when a single node is required, a metric must be utilized to decide on the most critical node among the ones which lie on the boundary of the Fiedler clusters. Existing works [8] have adopted metrics presented in [57][96], however, this chapter considers an alternative metric which takes into account the users of the underlying network and their source destination paths. The algebraic connectivity depends only on the topology of the underlying network and the criticality metric must thus be complemented to account for the intuitive notion that the users of the network must also be taken into consideration when assessing the criticality of a node. This complementary information is offered by the second optimization problem that is consider in this chapter. It has been well established in the literature that the rate allocation algorithms of the network users attempt to maximize the aggregate utility of the network over the capacity constraints [49]. So, in this chapter a node is considered critical when its removal degrades the network performance to the greatest extent i.e. they minimize the maximum of the aggregate utility function. This optimization problem requires full network information in order to be solved and in addition the complexity of the exhaustive search solution increases combinatorially with the network size when multiple nodes need to be selected. Thus, in this chapter a suboptimal solution is presented which identifies as critical, the nodes which maximize the square root of the number of active connections at each node multiplied by the aggregate input data rate. The combination of these two suboptimal solutions results in the proposed criticality metric such that it considers as critical the nodes which maximize the latter criticality metric over the nodes which lie on the boundary of the Fiedler clusters.

Performance evaluation of the proposed criticality metric was performed using extensive simulations conducted on Matlab and the NS-3 simulator. Since the criticality metric is obtained by combining suboptimal solutions of two optimization problems therefore, it is first established that these suboptimal solutions are not conservative. When a single critical node is removed, the proposed suboptimal solutions are very close to the optimal ones which are obtained using the exhaustive search approach. When multiple nodes are removed the suboptimal solutions are close to a lower bound which is obtained analytically. Later, the proposed metric was evaluated against other metrics which have been proposed in literature: the betweenness centrality [34], the closeness centrality, the degree centrality [35], the Hybrid Interactive Linear Programming Rounding (HILPR) proposed in [82], the Controllability of complex networks (Cont) in [59], the suboptimal solution of eq 6.15 [102][20] and the suboptimal solution of Eq (6.16) [57][96]. The evaluation is based on the degradation in performance reported when nodes selected using the criticality metrics under consideration are removed from the network. The considered network is a wireless ad-hoc network where the x and y coordinates of the nodes are randomly chosen according to uniform distributions. It is established here that, the proposed criticality metric outperforms the other approaches in terms of the achieved network throughput, the average network delay, the average network jitter and the number of dropped packets.

6.2 Problem Formulation

The proposed method for identifying critical nodes is based on the solution of two optimization problems: the algebraic connectivity minimization problem and a min-max aggregate utility problem. This section, introduces the relevant mathematical framework which is used to formulate these problems mathematically and also present some of the relevant approaches present in the literature.

6.2.1 Algebraic Connectivity Minimization

Algebraic connectivity of a graph is the second smallest eigenvalue of the graph Laplacian and it is a measure of how well a graph is connected. In the Graph $G = (V, E)$ where $|V| = n$ and $|E| = m$ are the number of nodes and edges respectively. The incidence matrix A is the $n \times m$ matrix where the existence of an edge $l \in E$ between node i and j defines the l^{th} column of the matrix with $a_{l_i} = 1$ and $a_{l_j} = -1$. For such a graph the Laplacian matrix can be determined by:

$$L = AA^T = \sum_{l=1}^{m} a_l a_l^T \tag{6.1}$$

The diagonal entries of this Laplacian matrix $L_{i,i}$ denote the degree of the node i and the non diagonal entries denote the existence of a link between two nodes. It is easy to state here that L is positive semi-definite and $L\mathbf{1} = 0$ where $\mathbf{1}$ is the vector of all ones.

Algebraic connectivity has been observed to serve as a connectivity robustness measure in the sense that the lower its value is, the closer the network is in becoming disconnected. The latter property has motivated the use of the algebraic connectivity in assessing node criticality. A node is considered to be critical when it contributes mostly to keeping the network connected. One may thus define as critical, the nodes which when removed minimize the algebraic connectivity of the network. This optimization problem, referred to as optimization problem P, is shown formally below:

$$P: \; CN = \arg \min_{\alpha \in V} \; \mu(G(V-\alpha)) \tag{6.2}$$

One way of solving P when a single node is removed is through exhaustive search. However this approach is computationally expensive. In addition, when multiple nodes are removed, the complexity of the exhaustive search solution increases combinatorially with increasing network size. So, people have sought suboptimal solutions which are simple to implement in a distributed manner. The most popular solutions are inspired from the following characterization of the algebraic connectivity [65] using the Rayleigh quotient of y with respect to L:

$$\mu(L) = min\{\frac{y^T L y}{y^T y} | y \neq 0, \mathbf{1^T} y = 0\} \tag{6.3}$$

If we substitute y with the normalized vector $v = y/||y||$ in eq 6.3 then, it can be written as:

$$\mu(L) = min\{v^T Lv| \; ||v|| = 1, \mathbf{1^T} v = 0\} \tag{6.4}$$

which can also be expressed in the form:

$$\mu(L) = \min\{\sum_{i=1}^{n} \sum_{j \in N_i} (v_i - v_j)^2| \; ||v|| = 1, \mathbf{1^T} v = 0\} \tag{6.5}$$

where N_i is the set of neighbours of node i. The minimum is achieved when v is the Fiedler vector of the Laplacian L. Each Fiedler vector entry naturally corresponds to a node in the graph. It can thus be deduced from eq 6.5 that the node which contributes the most to the algebraic connectivity is the one with the maximum sum of squared Fiedler vector value differences with neighbouring nodes i.e $\sum_{j \in N_i}(v_i - v_j)^2$.

One of the suboptimal solutions that can reduce the computational complexity of solving eq 6.2 is built by substituting the function $G(V - \alpha)$ with L in eq 6.2 where, from eq 6.1. We know that $L = (L_o - uu^T)$ where, $uu^T = (\sum_{k=1}^{m} x_k h_k h_k^T)$. Here, L_o is the Laplacian matrix for the original network and x_k is a boolean variable that is 1 if the edge k is connected to the node α and is zero otherwise. By substituting $G(V - \alpha)$ in eq 6.2 we have:

$$\min \; \mu(L_o - \sum_{k=1}^{m} x_k h_k h_k^T) \tag{6.6}$$

$$s.t. \; x \in \{0, 1\}^m$$

The first order partial derivative of the aforementioned optimization function with respect to x_k gives us the first order approximation of the decrease in $\mu(L)$ if the node α is removed from the graph G.

$$\frac{\partial}{\partial x_k}\mu(L_o - \sum_{k=1}^{m} x_k h_k h_k^T) \tag{6.7}$$

Now we know that if v is the normalized Fiedler vector then we have:

$$\mu(L(x))v = L(x)v \tag{6.8}$$

By multiplying v^T to both sides of eq 6.8 we get:

$$v^T \mu(L(x))v = v^T L(x)v \tag{6.9}$$

Since v is normalized, we have:

$$\mu(L(x))(v^T v) = v^T (L(x))v \tag{6.10}$$

$$\mu(L(x)) = v^T L(x)v \tag{6.11}$$

Now if we take partial derivative of both sides of eq 6.11 we have:

$$\frac{\partial}{\partial x_k}\mu(L(x)) = v^T \frac{\partial L(x)}{\partial x_k} v \tag{6.12}$$

Hence, by substituting eq 6.7 into eq 6.12 we have:

$$v^T \frac{\partial (L_o - \sum_{k=1}^{m} x_k h_k h_k^T)}{\partial x_k} v \tag{6.13}$$

By performing matrix multiplication, we can rearrange eq 6.13 into:

$$v^T \frac{\partial L_o}{\partial x_k} v - v^T \frac{\partial (\sum_{l=1}^{|P|} x_k h_k h_k^T)}{\partial x_k} v \tag{6.14}$$

Now as we know that, L_o is not a function of x_k and that $v^T \frac{\partial L_o}{\partial x_k} v$ is the algebraic connectivity of the original network, thus in order to solve the original optimization problem stated by eq 6.6, we need to determine the node that maximizes the function $v^T (\sum_{k=1}^{m} x_k h_k h_k^T) v$. This can also be illustrated in the form of an optimization problem such as [102] [57] [20]:

$$CN = \arg \max_{i \in V} \sum_{j \in N_i} (v_i - v_j)^2 \tag{6.15}$$

A slight variant of the aforementioned optimization problem has also been proposed in [57] and [96]

$$CN = \arg \max_{i \in V} \frac{\sum_{j \in N_i} v_j (v_i - v_j)}{1 - v_i^2} \tag{6.16}$$

The solutions of eq 6.15 and eq 6.16 constitute suboptimal solutions of the optimization problem P as indicated in [57]. More specifically, in [57] the metrics are derived using approximations of the difference in the algebraic connectivity when a particular node is removed. Bounds on the estimation error are then established which can be used to characterize how conservative these approximations are. The distributed criticality metrics and their analysis are generalized in [58]. Therein, the authors show that under certain conditions the distributed metrics create the same importance order as the approximation based centralized solutions. As a result of recent advances in the distributed calculation of Fiedler vector values [14], these suboptimal solutions are amenable for implementation in a distributed manner. The main drawback of the distributed implementations, as indicated by the authors in [57][20], is that, a maximization consensus algorithm must be employed over the entire set of nodes present in the relevant graph which increases significantly the computational overhead. This chapter offers an alternative suboptimal solution which alleviates the aforementioned problem thus reporting smaller convergence times.

6.2.2 Min-Max Aggregate Utility

The algebraic connectivity, which has so far been used to assess node criticality, only takes into account the topology of the underlying network. However, intuition suggests that apart from the network topology, the network users also have a key role to play when assessing the criticality of a particular node. Nodes which are utilized by many source destination paths, or nodes which accommodate large amounts of data traffic, can be considered more critical than others. This subsection utilizes the Network Utility Maximization (NUM) framework proposed by Kelly in [50] to cast these intuitive notions in a formal optimization based framework.

Consider a network which consists of a set of traffic sources S and a set of links L.

Each network user $s \in S$ injects data into the network with a rate denoted by x_s. The data is transferred from its source $s \in S$ to its destination via a route which comprises of a set of links collected in the set $L(s)$ representing the route. Each link $l \in L$ is characterized by a finite capacity c_l. To each user x_s assign a utility function $U_s(x_s)$ which represents the satisfaction a user gets from a particular sending rate allocation. The utility functions are assumed to be strictly increasing, continuously differentiable and strictly concave. The objective of the network user collaboration is to maximize the aggregate utility function subject to the capacity constraints. Therefore, a node is considered as critical if its removal results in the highest degradation in the aggregate utility function of the network. This is expressed formally below:

$$Q : CN = arg \min_{k \in V_c} \max_{s \in (S \setminus k)} \sum_{s} U_s(x_s) \tag{6.17}$$

$$subject\ to \sum_{s: l \in (L(s) \setminus L(k))} x_s \leq c_l\ \forall l \tag{6.18}$$

$$over\ x_s \geq 0 \tag{6.19}$$

The optimization problem of eq 6.17 is a mixed integer discrete continuous problem, discrete in the minimization over the set of nodes and continuous in the maximization over the sending rates. One may employ the exhaustive search approach to obtain the optimal solution when a single node is removed. However, this approach is computationally expensive and requires full network information. In addition, when multiple nodes are removed the complexity of the exhaustive search approach increases combinatorially with network size. A number of algorithms have been proposed in literature to obtain more efficient optimal and suboptimal solutions [70][105]. This chapter offers, a suboptimal solution which leads to a distributed, simple to evaluate node criticality metric.

6.3 Proposed Algorithm

This section describes the proposed criticality metric which is based on suboptimal solutions of the optimization problems P and Q described in the previous sections. The rationale behind the offered suboptimal solutions is explained.

6.3.1 Algebraic Connectivity Minimization

The proposed suboptimal solution of problem P is based on spectral partitioning considerations. Spectral partitioning, refers to the methodology with which a graph can be partitioned into connected clusters using spectral properties of the graph, namely the elements of the Fiedler vector. As a result of the property $\mathbf{1^T}v = 0$ in eq 6.5 the elements of the Fiedler vector attain both positive and negative values in the range $[-1, 1]$. The following theorem establishes how the Fiedler vector elements can be used to partition the graph into clusters which are well connected [33].

Theorem 1. *Let G be a finite connected graph with N vertices and v_i be the Fiedler vector value corresponding to node i. Then for any $s \geq 0$:*

$$M(s) = \{i \in N | v_i + s \geq 0 \qquad (6.20)$$

the sugbraph $G(s)$ induced by G on $M(s)$ is connected.

A similar theorem exists for $s \leq 0$. Different values of s yield different types of cuts [33]. This chapter adopts the sign cut approach in which case s is equal to 0. The above theorem only establishes the connectivity of the obtained clusters. However, a number of other results indicate that spectral partitioning can produce cuts with a good ratio of cut edges to separated vertices [22]. This implies that spectral partitioning methods yield strongly connected clusters of approximately equal size, loosely connected between them. This property motivates the proposed solution. As the objective here is to identify nodes which when removed minimize the algebraic connectivity and it is expected that if an edge lying in the spectral partitioning cut-set is removed from the network, it will render the clusters even less loosely connected thus significantly decreasing the algebraic connectivity of the network. Therefore, in this chapter, such a node is considered critical whose removal will result in the removal of an edge from the spectral partitioning cut-set. As mentioned above, this chapter adopts the sign cut approach which partitions the network into two well-connected clusters. All the nodes of the first cluster have positive corresponding Fiedler vector elements whereas, all the nodes of the second cluster have negative Fiedler vector elements. The cut-set thus comprises of all the edges which connect nodes with corresponding Fiedler value elements of different sign. Therefore, such a node is considered as critical who has at least one neighbouring node with a Fiedler vector element of different sign. In mathematical terms a node $i \in V$ is critical if it satisfies:

$$sign(v_i) \text{ is +ve and } sign(v_j) \text{ is -ve}$$

or

$$sign(v_i) \text{ is -ve and } sign(v_j) \text{ is +ve} \tag{6.21}$$

where $sign$ is the sign function and $v_i \in V$ are the elements of the Fiedler vector.

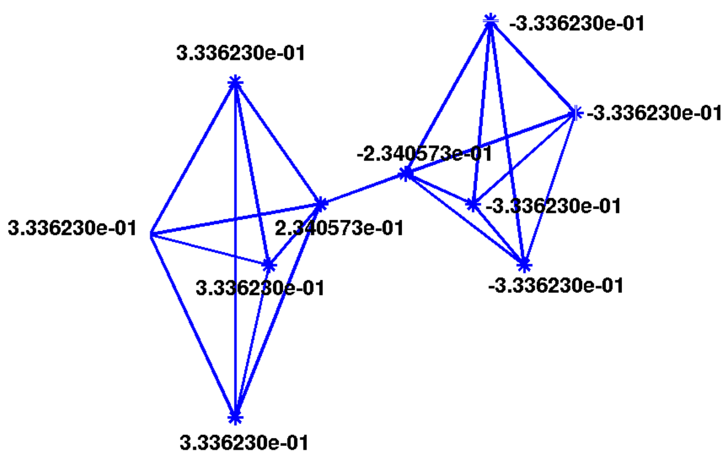
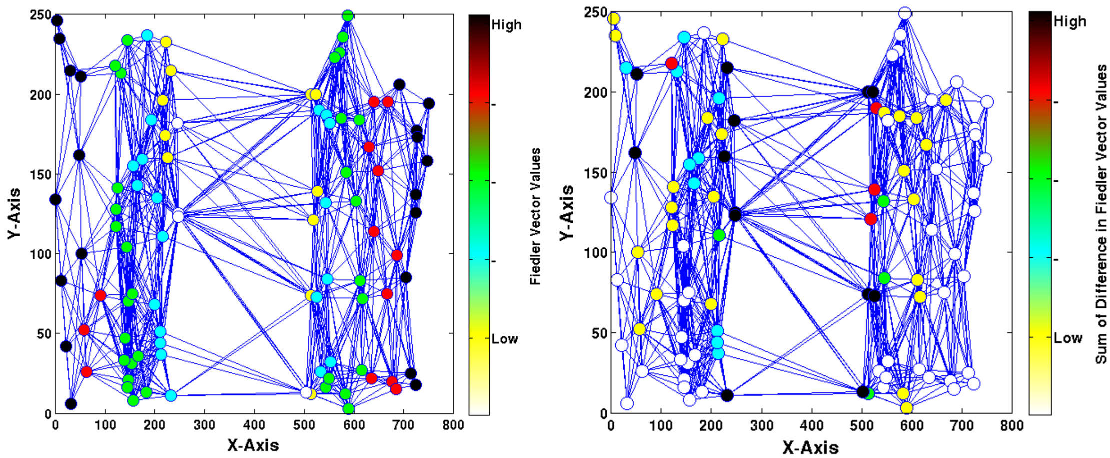


Figure 6.1: Example network where the Fiedler values are indicated at the corresponding nodes.

The aforementioned concept is demonstrated through the sample network of Fig 6.1. The network consists of two well connected subgraphs. These are loosely connected between them by means of a single link. The Fiedler vector values are calculated and indicated on the diagram. It is observed that the Fiedler vector values corresponding to the nodes in the left-hand subgraph have positive values, whereas, the Fiedler vector values corresponding to nodes in the right-hand subgraph have negative values. Intuition suggests that the nodes which are critical are the ones which connect the two subgraphs via the single edge and can be observed in Fig 6.1. The nodes that connect the two subgraphs have Fiedler vector values of different signs.

The question that arises is whether the proposed criterion is indeed a suboptimal solution of the algebraic minimization problem P in eq 6.2. In subsequent sections, the suboptimality of the proposed solution is demonstrated using simulations. This section demonstrates the suboptimality by highlighting its relation to the criticality criterion in eq 6.15 which has been demonstrated [102] to constitute a suboptimal solution. In particular, the nodes which are detected as being critical according to the proposed criterion of eq 6.21 also report high aggregate squared Fiedler difference values $\sum_{j \in N_i}(v_i - v_j)^2$ which implies that they are also critical according to criterion eq 6.15. The analytical verification of this observation is an open problem. This observation is important as it suggests that the maximization of eq 6.15 does not have to be done over the entire set of nodes but only over the ones which have Fiedler element values of the same sign. This can significantly reduce the implementation complexity of eq 6.15.

This relation is demonstrated using the network of Fig. 6.2 which comprises of 80 nodes. The network consists of two well connected subgraphs loosely connected by a small set of edges. Each node is coloured according to the magnitude of the absolute value of the quantity under investigation. Fig. 6.2(a) shows that, at each node i the magnitude of the calculated Fiedler element value v_i whereas, Fig. 6.2(b) shows the magnitude of the aggregate squared difference value $\sum_{j \in N_i}(v_i - v_j)^2$. It is observed that, there is a tendency for the Fiedler elements to attain their lowest value at nodes



(a) (b)

Figure 6.2: Example network where at each node we highlight a) Fiedler vector values, b) Difference in Fiedler vector value across the network.

which lie in the sign cut-set. As one moves away from the sign cut-set the Fiedler values tend to increase. In addition, it is observed that, nodes which lie in the sign cut-set tend to attain large aggregate squared difference values. This demonstrates the relationship between eq 6.21 and eq 6.15.

The proposed change of sign approach is amenable for implementation in a distributed manner. Recent techniques [14], allow the distributed calculation of Fiedler values at each node. Then, the only thing that a node needs to do in order to classify itself as critical is to check whether at least one of its neighbours has a Fiedler value with a different sign than itself. However, this approach leads to multiple nodes being detected as critical. What if a single node needs to be selected? Among the nodes which lie in the sign cut-set how do we choose the one which is the most critical? In our recent work in [8] we have chosen the node which maximizes the sum of squared differences $\sum_{j \in N_i}(v_i - v_j)^2$, whereas, this chapter chooses an alternative criterion which is based on a distributed suboptimal solution of the problem Q in (6.17).

6.3.2 Min-Max Aggregate Utility

Here, the strict concavity of the utility functions is relaxed to assume linear utility functions $U_s(x_s) = x_s$. The proposed criticality metric is obtained using suboptimal solutions of two approaches. The first approach is via the directional derivative along the directions of rate deductions due to link removal. Let $F(x^*) = \sum_s U_s(x_s^*)$ denote the aggregate utility function evaluated at the optimal sending rates at which the maximum is achieved. When a link $l \in L$ is removed from the network then all the sources s which utilize link l denoted by $S(l)$ will be deprived from the ability to send data. This is expected to lead to a reduction in the cost function $F(.)$ along the directions $x_s, s \in S$. Our aim is to remove a link which will cause maximum reduction in the cost function $F(.)$. By employing steepest descent considerations a removal which maximizes the directional derivative is thus sought. We thus investigate the effect of removing link l on F by considering the directional derivative of F along the unit vector $\vec{y_l} = \sum\limits_{s \in S(l)} \frac{1}{\sqrt{n_l}} \vec{i_s}$, where n_l is the cardinality of $S(l)$ and $\vec{i_s}$ is the unit vector along the direction x_s. The directional derivative $D_{\vec{y_l}}F$ evaluated at the equilibrium point x^* is given by

$$D_{\vec{y_l}} F = \vec{y_l}. \bigtriangledown f_{x=x^*} = \tag{6.22}$$
$$\frac{1}{\sqrt{n_l}} \frac{\partial F}{\partial x_1} + \frac{1}{\sqrt{n_l}} \frac{\partial F}{\partial x_2} + ... + \frac{1}{\sqrt{n_l}} \frac{\partial F}{\partial x_n}$$

Since the utility functions are assumed linear:

$$D_{\vec{y_l}} F = \sqrt{n_l} \tag{6.23}$$

Since the objective is to minimize $F(x^*)$ links l are sought which maximize the directional derivative. The other approach is by direct calculation of the reduction in $F(x^*)$ when a link l is removed. Due to the linear utility function assumption, $F(x^*) = \sum_{s \in S} x_s^*$. When a link l is removed, all the sources s which utilize link l will be deprived from the ability to send data. This will result in a reduction in $F(x^*)$ by an amount $\Delta y_l^* = \sum_{s \in S(l)} x_s^*$. Since the objective is to minimize $F(x^*)$, links l are sought which report the highest input data rate Δy_l^*. We combine the aforementioned approaches to classify as critical the links which satisfy:

$$CN = arg \max_{l \in L} \sqrt{n_l} \Delta y_l^* \tag{6.24}$$

Despite the fact that the discussion has so far been made with reference to link removal, the derived criterion of eq 6.24, also applies to node removal. n is the total number of connections traversing the node, whereas Δy^* is the input data rate at the node. The dependence of the criticality metric on n is in line with the well known betweenness centrality criterion. The dependence on the input data rate is in line with the intuitive notion that the more data traverses a node the more critical it is. The input data rate at a particular node is a quantity that can be calculated locally. The number of active connections, however, is readily available locally only in systems which maintain per connection states at each node. When such per connection states are not available, estimates of the active connections can be used instead. Such estimates can be generated online using parameter identification techniques proposed in literature [54].

Algorithm 1: Distributed Critical Node Identification.

Initialization: Every node i shares corresponding Fiedler vector component to its neighbouring nodes and stores a flag bit $f_i = 1$, set $t \leftarrow 0$
Step 1:
if $v_i > 0$ *and* $v_j < 0 \;\forall\; j \in N_i$ **then**
    calculate $\triangle\beta_i(t) = \sqrt{n_i}y_i$. Each node i transmits $\triangle\beta_i(t)$ to its neighbours with $v_j > 0$ and computes: $\triangle\beta_i(t) = max\{\triangle\beta_i(t), \triangle\beta_j(t)\} j \in N_i$
    else
        $f_i = 0$, $\triangle\beta_i(t) = 0$
    end
end
Step 2:
if *(t mod D)*$= 0$ **then**
    each node checks weather $f_i = 1$ or not,
    Critical Node = $arg\ max\{\triangle\beta_i(t), \triangle\beta_j(t)\}$, $j \in N_i$
    else
        At all nodes observing a sign change with $v_i > 0$ and $v_j < 0$, set $f_i = 1$. Each node i transmits $\triangle\beta_i(t)$ to its neighbours with $v_j > 0$ and computes: $\triangle\beta_i(t+1) = max\{\triangle\beta_i(t), \triangle\beta_j(t)\}\ j \in N_i$
    end
end
if $\triangle\beta_i(t+1) \neq \triangle\beta_i(t)$ **then**
    $\triangle\beta_i(t+1) \leftarrow \triangle\beta_i(t)$, $t = t+1$, set $f_i = 0$
end
Return to Step 2

The obtained suboptimal solutions of the two considered optimization problems are then combined to yield the methodology with which the most critical node in the network is identified. The methodology is as follows. The change of sign approach of eq 6.21 is first used to identify all the nodes which lie in the sign cut-set. Among the nodes which lie in the sign cut-set, the most critical is the one which maximizes the cost function of eq 6.24. The proposed approach is amenable for implementation in a distributed manner. Recently proposed techniques [14] allow the distributed calculation of the Fiedler elements at each node. After the Fiedler elements are calculated at each node, the nodes employ beacon message exchange to share their Fiedler elements with their neighbours. If a node detects that the sign of the Fiedler value of one of its neighbours is different than its own sign, then it identifies itself as lying in the sign cut-set of the network graph. All the nodes that lie in the sign cut-set calculate the $\sqrt{n}\Delta y$ cost of eq 6.24 and initiate a blind flooding algorithm to share their cost with all the other nodes lying in the sign cut-set. When a node in the sign-cut set receives a cost initiated from another node in the sign cut-set it compares the two, and if the maximum is its own cost it identifies itself as a critical node and rebroadcasts the maximum of the two. This approach guarantees that when the algorithm terminates, only one critical node is left within the network which is the one which has the highest cost among all the nodes which lie in the sign cut-set. Note that the blind flooding algorithm is implemented only over the nodes which share the same Fiedler element sign. This achieves significant savings in computation effort relative to other approaches. Below, is the pseudocode of the proposed method.

6.4 Analysis

In this section, we derive analytically a lower bound on the algebraic connectivity when a single node is removed from the network and use it iteratively to evaluate how conservative our suboptimal solutions are when multiple nodes are removed from the network.

Theorem 2. *Let $G = (V, E)$ be a graph of n nodes with eigenvalues $0 \leq \wedge_2 \leq \wedge_3 \leq ... \leq \wedge_n$. Then, upon removal of a node w node from the graph, the algebraic connectivity of the resultant graph is lower bounded by:*

$$\lambda \geq \wedge_2 - \frac{u_2^2}{1 + (b_n - u_2^2)/(\wedge_2 - \wedge_n)} \tag{6.25}$$

where

$$u_2 = \sum_{w \in n} \sum_{j \in N_i, i \in w} (v_i - v_j), \tag{6.26}$$

$$b_n = n(tr(A) - u_2) + \sqrt{n(1-n)f(A)} \tag{6.27}$$

and

$$f(A) = tr\left(A - \frac{tr(A)}{2} I\right)^2 - \left(2\left(u_2 - \frac{tr(A)}{2}\right)^2\right) \tag{6.28}$$

with

$$tr\left(A - \frac{tr(A)}{2}I\right)^2 = tr(A^2) - \frac{(tr(A))^2}{2} \tag{6.29}$$

Here, A is the Laplacian matrix defined by the node w that is being removed from the graph.

Proof. We use the eigenvalue decomposition of $L = QDQ^T$ where $D = Diag(0, \wedge_2, ..., \wedge_n)$ is the diagonal matrix of ascending eigenvalues and Q is an orthogonal matrix with corresponding eigenvectors of L in its columns. The eigenvalues of a Laplacian matrix L can be found using $Lv = \lambda v$, therefore, in this expression we substitute L to get [87]:

$$(QDQ^T)v_j = \wedge_j v_j \tag{6.30}$$

Where v_j is the linear combination of the eigenvectors corresponding to the j^{th} eigenvalue $\wedge_j$ of L. The removal of w nodes from the network reduces D by a factor uu^T where $u = Q^T h_l$ and h_l is l^{th} column of the incidence matrix A of the network [38]. Thus we have:

$$Q(D - uu^T)Q^T v_j = \wedge_j v_j \tag{6.31}$$

We know from [41] that, the eigenvalues of eq 6.31 can be obtained by solving $D - uu^T - \lambda I$ for the determinant of the matrix, where I is the identity matrix [41]:

$$det(D - uu^T - \lambda I) = 0 \tag{6.32}$$

$$det(D - \lambda I)det(I - (D - \lambda I)^{-1}uu^T) = 0 \tag{6.33}$$

Eq 6.33 can be reduced to [41]:

$$\prod_{i=1}^{n}(\wedge_i - \lambda)\left(1 - \sum_{i=1}^{n}\frac{u_i^2}{(\wedge_i - \lambda)}\right) = 0 \tag{6.34}$$

This shows that, the eigenvalue of eq 6.31 can be computed by finding the roots of the secular equation:

$$1 = \sum_{i=1}^{n}\frac{u_i^2}{\wedge_i - \lambda} \tag{6.35}$$

We solve eq 6.35 for the the eigenvalue λ of the network that results after the removal of w node from the network. Here, we know that $u_1 = 0$ and $u_2 = \sum_{w \in n}\sum_{j \in N_i, i \in w}(v_i - v_j)$. Therefore we have:

$$\frac{u_2^2}{\wedge_2 - \lambda} = 1 - \sum_{i=3}^{n}\frac{u_i^2}{\wedge_i - \lambda} \tag{6.36}$$

This can be re-arranged into:

$$\lambda = \wedge_2 - \frac{u_2^2}{1 + \sum_{i=3}^{n} u_i^2/\lambda - \wedge_i} \tag{6.37}$$

According to the eigenvalue interlacing theorem, the algebraic connectivity of network that results from the removal of a node is bounded by $0 \leq \lambda_2 \leq \wedge_2$ [42].

Theorem 3. *Let X be a graph with n vertices and let Y be obtained by removing a* *vertex from X then [42]:*

$$\lambda_{i-1}(L(X)) \leq \lambda_i(L(Y)) \leq \lambda_i(L(X))$$

We used Theorem 3 along with the observation in eq 6.37, concludes that, the LHS is a decreasing function whereas the RHS is an increasing function of λ, therefore we obtain the lower bound of λ by using the appropriate substitution of $\lambda = \wedge_2 > \lambda_2$. This gives us:

$$\lambda \geq \wedge_2 - \frac{u_2^2}{1 + \sum_{i=3}^{n} u_i^2/(\wedge_2 - \wedge_n)} \tag{6.38}$$

From [77] it is known that $\sum_{i=1}^{n} u_i^2 \leq b_n$, thus we approximate $\sum_{i=3}^{n} u_i^2$ with the difference $b_n - u_2^2$ to obtain the final expression of eq 6.25, where:

$$b_n = n(tr(A) - u_2) + \sqrt{n(1-n)f(A)} \tag{6.39}$$

and $f(A)$ is:

$$f(A) = tr\left(A - \frac{tr(A)}{2}I\right)^2 - \left(2\left(u_2 - \frac{tr(A)}{2}\right)^2\right) \tag{6.40}$$

In eq 6.40 the square of the matrix can be avoided by using eq 6.41 [77].

$$tr\left(A - \frac{tr(A)}{2}I\right)^2 = tr(A^2) - \frac{(tr(A))^2}{2} \tag{6.41}$$

Here $tr(A^2) = ||A||_f^2$ and $||A||_f$ is the Frobenius matrix norm of A. □

6.5 Performance Evaluation

This section evaluates the performance of the proposed criticality metric using simulations conducted on Matlab [61] and on the Network Simulator (NS-3) [69]. This section first assess how conservative the suboptimal solutions are with reference to the posed optimization problems, and then evaluates the ability of the proposed method to choose the most critical nodes in the network. The criticality of a fixed number of nodes is assessed by evaluating the degradation in performance achieved when these nodes are removed from the network. Here, a comparative study is conducted to investigate the performance of the proposed metric against other approaches that exist in literature such as the Betweenness Centrality [34], the Closeness Centrality, the Degree Centrality [35], the exhaustive search approach, the Hybrid Interactive Linear Programming Rounding (HILPR) metric proposed in [82], the controllability of complex networks (Cont) approach in [59], the suboptimal solution of eq 6.15 which is referred to as the Sum Squared Difference approach (SSD) [102][20], the suboptimal solution of eq 6.16 which is referred to as the Normalized Sum Squared Difference approach (NSSD) [57][96] and a previously proposed approach which is referred to as Spectral Partitioning for Node Criticality approach (SPNC) [8]. The simulation results of this chapter indicate that the suboptimal solutions are not conservative and that the proposed criticality metric chooses the most critical nodes in the network as it achieves the greatest degradation in performance when these nodes are removed.

6.5.1 Algebraic Connectivity Suboptimality

This subsection evaluates based on simulations conducted on Matlab, the ability of the change of sign approach, incorporated in the proposed metric, to serve as a suboptimal solution of the posed algebraic connectivity minimization problem i.e. to identify nodes which when removed achieve algebraic connectivity values which are close to the minimum. It also compares the change of sign approach with other approaches which have been proposed in literature in terms of the algebraic connectivity achieved. As the objective here is to focus on the topological aspects of the proposed criticality metric these simulations do not account for network users. To find a single critical node the proposed approach first employs the change of sign approach to find the set of nodes which lie in the sign cut-set and among these it finds the ones which maximize the $\sqrt{n_l}$ parameter. The parameter n_l at a particular node l is found by calculating the number of times the node l participates in the shortest path, among all shortest paths between all possible source destination pairs.

Here, simulation experiments are executed on an area of $1000 \times 1000m^2$ in which 100 nodes are randomly deployed. The x and y coordinates of the nodes are drawn from a uniform random distribution. The nodes employ wireless communication to form a wireless ad hoc network. In order to evaluate the performance of the considered criticality metrics as a function of the transmission radius of the nodes, the considered transmission radius values are kept in the range $100m$ to $200m$. To avoid random fluctuations due to single simulation run, simulations were conducted for 20 different network topologies and the results were then averaged.

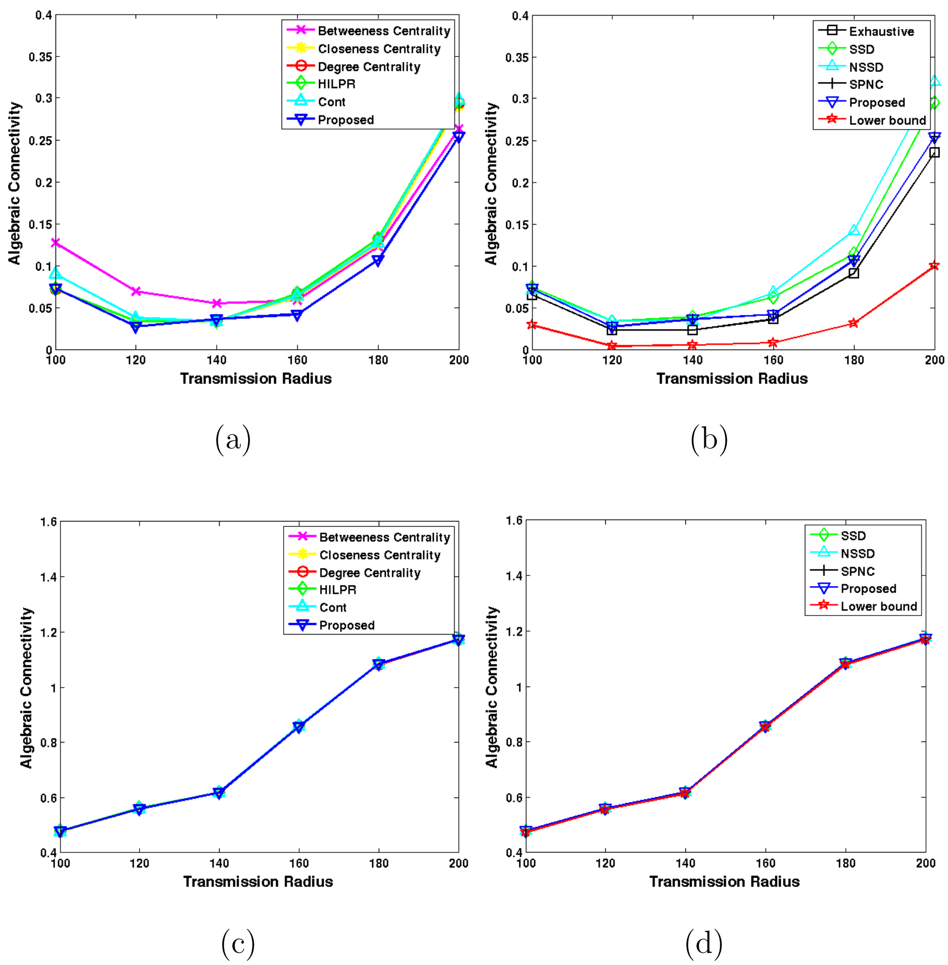


Figure 6.3: Algebraic Connectivity versus the trasnsmission radius when: a) & b) a single node is removed from the network, c) & d) five nodes are removed from the network.

Fig 6.3a & 6.3b show the algebraic connectivity of the aforementioned network as a function of the transmission radius when only one node, the most critical in the network, is removed. In these simulations, the proposed change of sign approach is tested against the exhaustive search approach, the betweenness centrality, the closeness centrality, the degree centrality, the HILPR, the Cont, the SSD and the NSSD. Note that when a single node is removed the optimal algebraic connectivity value can be found using the exhaustive search approach i.e. the algebraic connectivity is calculated when each node is removed from the network and the minimum among all calculated values is recorded.

The first thing to note is that, as expected, the algebraic connectivity increases monotonically as the transmission radius increases. The other thing to note is that at almost all transmission range values, the proposed change of sign approach, manages to yield the smallest algebraic connectivity value which is surprisingly very close to the optimal value calculated using the exhaustive search approach. This demonstrates that the proposed suboptimal solution is not conservative in the sense that it yields algebraic connectivity values which are close to the optimal. A similar study when conducted for the removal of 10 nodes from the network yields that it is computationally expensive to use the exhaustive search approach therefore, in order to evaluate the suboptimality of the proposed approach it is compared with the lower bound calculated in section 6.4. The results are shown in Fig 6.3c & 6.3d. The results indicate that all criticality metrics report similar algebraic connectivity values which are close to the lower bound. This again demonstrates the fact that the proposed suboptimal solution is not conservative.

6.5.2 Network Utility Maximization Suboptimality

The main objective of this set of simulation experiments is to evaluate how conservative the proposed criticality metric is in solving the min-max optimization problem of eq 6.17. Since a suboptimal solution is proposed, it is crucial to evaluate the degree with which the metric identifies nodes which when removed lead to aggregate utility functions which are close to the optimal. The optimal cost function is found by employing an exhaustive search approach i.e. the maximum aggregate utility is calculated, when each node is removed from the network and the minimum is found among all values calculated. The utility function used in this section is logarithmic in nature as it has been observed as common practice in the available literature. The simulations setup for the problem at hand considers an area of $100 \times 100m$ where 50 nodes are deployed with the x and y coordinates drawn from a uniform random distribution. Each node is characterized by a transmission radius of $30m$. At each time instant, a particular number of users inject data into the network along specific data routes. Where the number of users vary from 5 to 20 and the reported results are averaged over 50 experiment repetitions, in order to decrease the inaccuracies due to the random nature of the setting. As the proposed criticality metric incorporates the number of users traversing the node which is related to the betweenness centrality metric, therefore, the proposed approach is not only compared with the optimal but also with the betweenness centrality metric. For each considered number of users, a single node is removed from the network according to the criticality metric under consideration, and results recorded for the the maximum aggregate utility of the resulting network. In order to appreciate the level of the cost function reduction achieved the comparison also includes the maximum aggregate utility value prior to node removal which is referred to as the original network. The incorrect selection of the critical node is reported as the maximum network utility, which in the considered scenario will be a node that creates a bottleneck for the network and thus bounds the maximum aggregate utility, such a node upon removal will render the network with a higher aggregate utility. The results are shown in Fig. 6.4. It is observed that the proposed criticality metric yields smaller maximum aggregate utility values than the betweenness centrality metric which are close to the optimal values. This demonstrates the near optimality of the proposed solution.

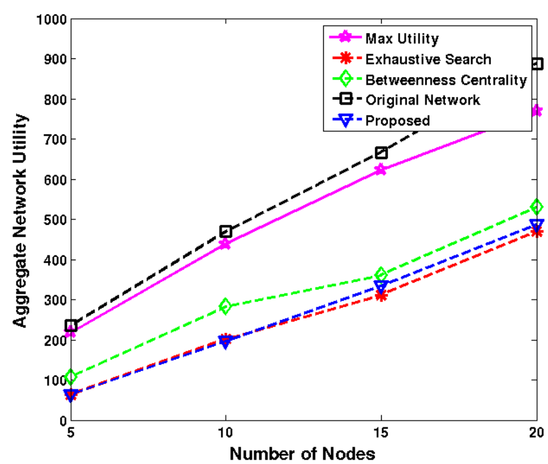


Figure 6.4: Aggregate network utility versus number of node in a network when critical nodes are selected using various approaches.

6.5.3 Computational Complexity

It has been established in section 6.3 that the proposed change of sign approach is related to the sum of squared differences approach of eq 6.15 in the sense that nodes which lie in the sign cut-set report high sum of squared difference values. However, the main benefit of the proposed approach is that the maximization algorithm does not have to be performed over the entire node set but only over the nodes which report the same sign of the Fiedler value element. In order to demonstrate, the significant reduction in computational effort achieved the proposed algorithm in algorithm 1 is compared with the maximization consensus algorithm proposed in [57] in terms of the computational time required for the algorithm to reach an equilibrium. In the simulation experiments that are conducted, nodes are deployed in an area of $1000 \times 1000 m^2$ with their x and y coordinates drawn from a uniform distribution. In order to evaluate the computational effort for different node densities and network sizes we consider number of node values are varied in the range 100 to 1000. Each node is assumed to have a fixed transmission radius of $250m$. The computational time for the two approaches as a function of the number of nodes is shown schematically in Fig. 6.5. It is observed that the proposed approach is able to achieve significant reductions in the computational time. These reductions become larger with increasing network size.

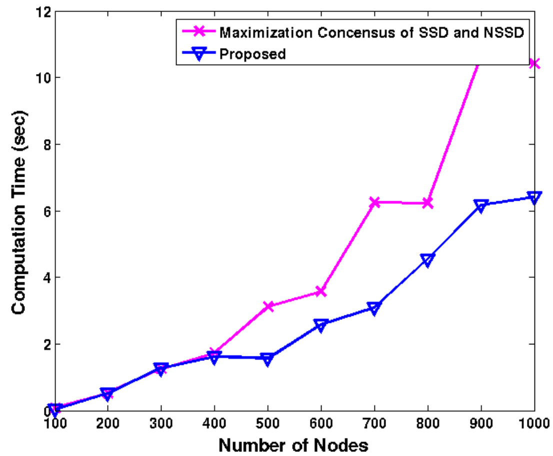


Figure 6.5: Computational time versus the number of nodes for the proposed approach and the maximization consensus algorithm of [57].

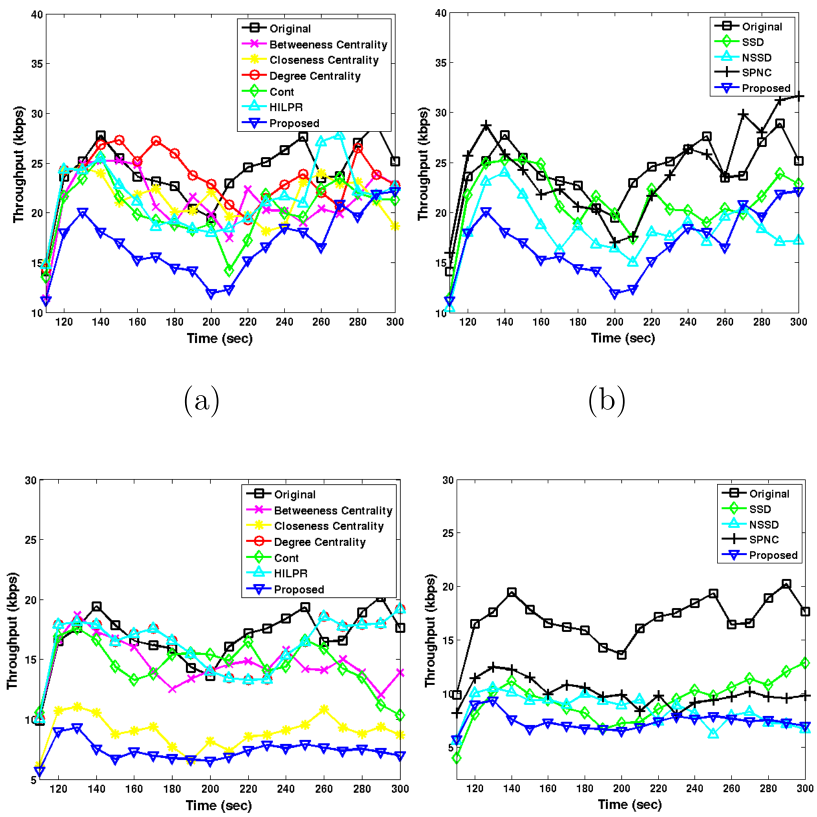
6.5.4 Network Centric Evaluation

Having established the suboptimality of the proposed solutions, and the significant reduction in implementation complexity achieved, in the final set of experiments, performance of the proposed criticality metric is evaluated in a more realistic network scenario. The simulation experiments are conducted on the NS-3 Simulator [69] and the network performance evaluated using network centric performance criteria such as the total network throughput, the average per packet delay, the average per packet jitter and the total number of packets dropped. In all the simulations the performance of the proposed metric is compared against metrics such as, betweenness centrality, closeness centrality, degree centrality, Hybrid Interactive Linear Programming Rounding (HILPR), the Controllability of complex networks (Cont),the Sum Squared Difference (SSD) approach, the Normalized Sum Squared Difference (NSSD) approach and the previously proposed Spectral Partitioning for Node Criticality (SPNC) approach

[8].

The evaluation was conducted on an area of $1500 \times 1500m^2$, where 100 wireless adhoc network nodes were placed using a uniform random distribution. Each node was equipped with a $802.11b$ transceiver with a transmit power of $7.5dbm$. 15% of them had an option of transmitting at a power $1.5 \times 7.5dbm$ [10] thus forming long range communication links. The degradation in signal strength as a function of the distance covered was represented by the Friss loss propagation model. A randomly selected set of 20 source/sink pairs initiate the communication in the network by transmitting packets at a rate of $2.048Kb/s$ each. Packet based transmission was assumed with the packet size set to $64byte$ packets. Routing paths within the network are formed using the OLSR (Optimized Link State Routing) protocol [62]. All measurements are obtained in the interval $100 - 300$ seconds after the start of the simulation. This provides sufficient time for the OLSR algorithm to converge to its equilibrium state. The degradation in network performance is evaluated after 10% of the most critical nodes are removed from the network. This process is repeated 10 times with the results averaged to decrease the stochastic uncertainty of the obtained results.

The first comparison evaluates the performance of the proposed approach against the metrics under consideration in this chapter for the network throughput that is achieved. The throughput of a network is defined as the total number of packets delivered to their destinations within the network per unit time. Fig 6.6a, 6.6b and Fig 6.6c, 6.6d show the achieved throughput after a single and 10% of the most critical nodes are removed from the network respectively. It is observed that, the



(a) (b)

(c) (d)

Figure 6.6: Time evolution of network throughput for the original network, and when a) & b) A single node, c) & d) 10% of the most critical nodes are removed according to betweenness centrality, closeness centrality, degree centrality, Hybrid Interactive Linear Programming Rounding (HILPR), the Controllability of complex networks (Cont),the Sum Squared Difference (SSD) approach, the Normalized Sum Squared Difference (NSSD) approach and the Spectral Partitioning for Node Criticality (SPNC) approach.

proposed approach reports the highest decrease in the achieved throughput relative to the approaches that already exist in literature. This demonstrates that the proposed algorithm is successful in identifying the most critical nodes of a network. The decrease in average throughput observed at certain periods of time is due to the long range link which have a higher transmitter power compared to the rest of the nodes in the network. The increase in power enables them to cover a larger distance for relaying data and thus reserve a larger portion of the network, increasing the probability of collision in the network. This results in a similar trend observed by the original network and all the criticality metrics under consideration of a decrease in throughput at around 200*sec*.

The next experiments were conducted aiming at comparing the proposed criticality metric against other approaches using the average per packet delay of the network. The delay experienced by packets in transit is an important network attribute which describes its performance. Low delays are preferable. In wireless ad hoc networks, such as the one considered in this study, delays are due to a number of reasons: network congestion resulting in queuing delays, poor channel behaviour resulting in re-transmissions and contention resulting in large vacant medium delay times due to the CSMA/CA mechanism. This chapter considers the average per packet delay as the performance metric. This is calculated by dividing the total number of delays observed with the number of packets transmitted throughout the simulation time. Fig 6.7 shows the time evolution of the average per packet delay reported in the original network and when nodes are removed according to approaches that exist in

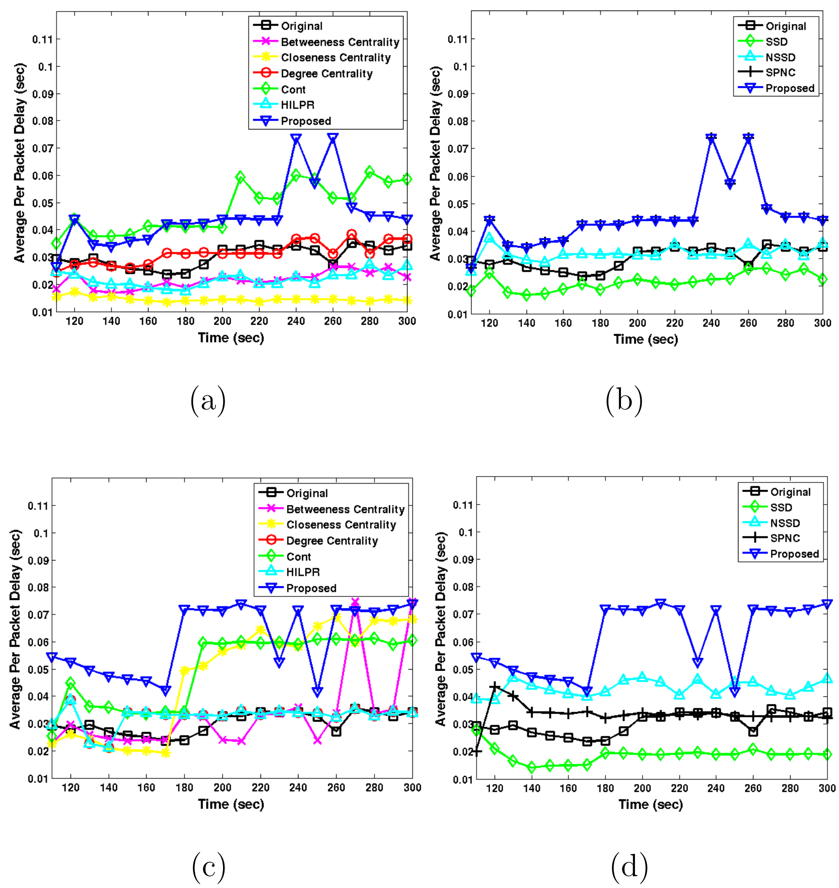
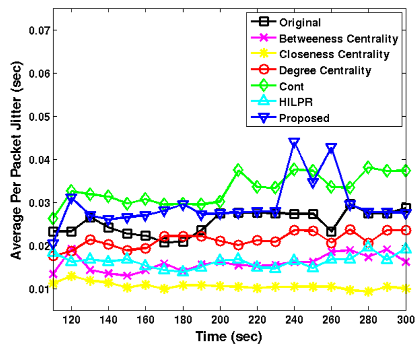


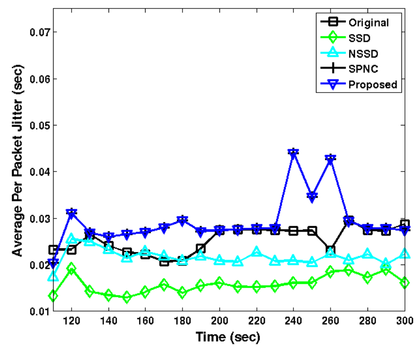
Figure 6.7: Time evolution of the per packet delay for the original network, and when a) & b) A single node, c) & d) 10% of the most critical nodes are removed according to betweenness centrality, closeness centrality, degree centrality, Hybrid Interactive Linear Programming Rounding (HILPR), the Controllability of complex networks (Cont), the Sum Squared Difference (SSD) approach, the Normalized Sum Squared Difference (NSSD) approach and the Spectral Partitioning for Node Criticality (SPNC) approach.

literature and the proposed criticality metric. It is observed that the proposed metric is able to bring a major degradation in performance as the average per packet delay increases significantly when nodes are removed. This is evidence of the fact that the proposed approach is more accurate in identifying the most critical nodes of a network. However, in Fig 6.7a and partly in 6.7c it is observed that in some cases the performance of the proposed metric is comparable to the performance of other metrics such as the Cont and Closeness Centrality, as similar average per packet delay values are reported when nodes are removed. However, it must be noted that even in these cases the proposed metric is the metric of choice, as it has been demonstrated earlier in Fig 6.6, that it outperforms the other proposals in terms of the degradation in throughput achieved.

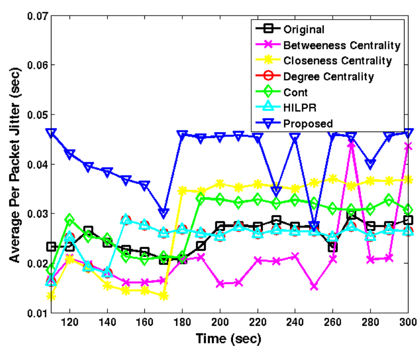
Next, the average per packet delay jitter is conducted as the performance metric. This is calculated by dividing the total delay jitter observed throughout the simulation experiment with the total number of transmitted packets. The delay jitter is calculated as the variation in packet reception times at the receiver. Increasing delay jitter values indicate increasing congestion within the network, so small delay jitter values are preferable. Fig 6.8 shows the time evolution of the average per packet delay jitter observed in the original network and when nodes are removed according to various criticality metrics. It is observed that the proposed metric outperforms other metrics when multiple nodes are removed and it reports a comparable average per packet jitter when a single most critical node is removed. Despite a comparable reduction in average per packet jitter, the proposed approach is considered as the



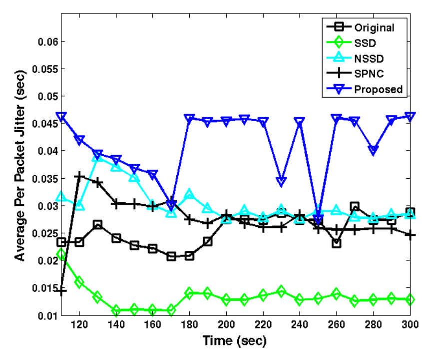
(a)



(b)



(c)



(d)

Figure 6.8: Time evolution of the per packet jitter for the original network, and when a) & b) A single node, c) & d) 10% of the most critical nodes are removed according to betweenness centrality, closeness centrality, degree centrality, Hybrid Interactive Linear Programming Rounding (HILPR), the Controllability of complex networks (Cont), the Sum Squared Difference (SSD) approach, the Normalized Sum Squared Difference (NSSD) approach and the Spectral Partitioning for Node Criticality (SPNC) approach.

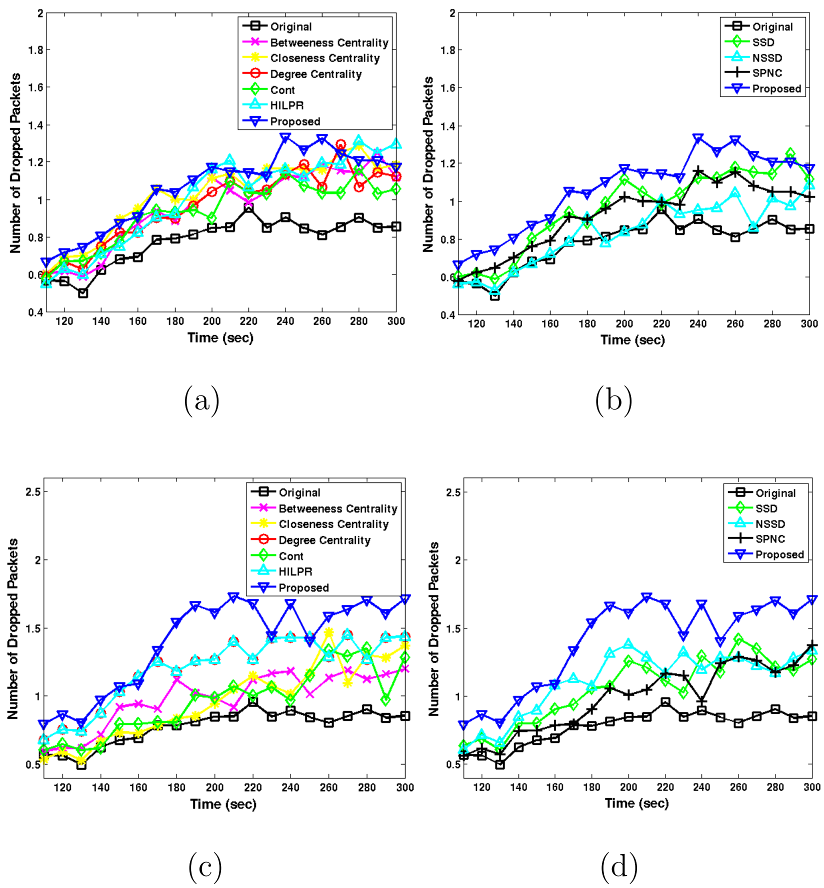


Figure 6.9: Time evolution of the number of dropped packets for the original network, and when a) & b) A single node, c) & d) 10% of the most critical nodes are removed according to betweenness centrality, closeness centrality, degree centrality, Hybrid Interactive Linear Programming Rounding (HILPR), the Controllability of complex networks (Cont), the Sum Squared Difference (SSD) approach, the Normalized Sum Squared Difference (NSSD) approach and the Spectral Partitioning for Node Criticality (SPNC) approach.

better choice for identification of the most critical node in the network due to the prominent reduction in average throughput of the network reported in Fig 6.6.

Finally, the total number of dropped packets is considered as the performance metric. High number of dropped packets in the network due to buffer overflow, is a strong indication of congestion. When nodes are removed from the network, the number of available paths decreases and the remaining paths are forced to accommodate all traffic. This makes them more vulnerable to congestion. When critical nodes are removed, congestion is expected to be more severe and the number of dropped packets is thus higher. The results of the conducted simulation experiments are shown in Fig 6.9. It is observed that, during the whole simulation time the proposed scheme is able to bring a major increase in the number of dropped packets compared to other approaches thus making it a viable option for identifying critical nodes in a network.

6.6 Summary

This chapter proposed a new metric with which critical nodes can be identified in computer networks. The problem is posed in an optimization based framework and a metric is developed by combining suboptimal solutions of two optimization problems: the algebraic connectivity minimization problem which captures the topological aspects of node criticality and the min-max aggregate utility problem which captures its connection oriented nature. It is shown here that, the suboptimal solutions are not conservative and it is demonstrated through extensive simulations that the proposed method is effective and superior relative to the other approaches. The method was evaluated on a wireless ad-hoc network. However, the problem formulation has been general and it thus opens the way for its application in other types of complex networks such as transportation networks, biological networks and water pipe networks. In the future, such extensions will be pursued in parallel with the development of a more efficient distributed algorithm that takes into account the change in the Fiedler vector elements across the network.

Chapter 7

Conclusion and Future Work

This chapter provides the conclusion of the work presented in this thesis along with a brief overview of a future direction of research.

7.1 Conclusion

The change in APL of a network upon removal or addition of a node is among the key considerations when dealing with critical node identification or accessing network vulnerability. This thesis, addressed this critical node identification problem by first identifying the parameters that affect the APL of a network, which is shown in literature to be computed using the complete knowledge of the network, where each nodes computes its distance from every other node in the network. This tedious approach is replaced by a much simpler and computationally less expensive approach in this thesis where, the network is broken down into branch and leaf nodes and then the APL approximated. The proposed approach when tested against existing approaches using extensive simulations has shown to outperform existing approaches in terms of computational complexity.

The APL of a network, as established in this thesis, plays a major role in approximating the average time it takes for a message to be decimated throughout the network and numerous research has been done in order to reduce the APL of a network. Existing approaches achieve this goal by either equipping nodes with special high power antennas that would cover a longer distance, equip nodes with special directed antennas for a directed beam forming or would rely on addition of a dedicated wire, connecting different nodes for increasing the connectivity of the network. This thesis eliminated this requirement of adding special hardware by proposing a new Variable Rate Adaptive Modulation (VRAM) scheme, that changes the modulation schemes to achieve long distance communication. The proposed approach reduces the APL of a network and improves the communication between nodes. It was observed here that, the proposed approach reported an average improvement of 41% in reducing the APL of a network and it reported an average 21% increase in the average node degree of the network when compared to existing approaches. The increase in average node degree is evidence to the fact that more nodes are directly connected with each other and thus message sharing among distant nodes in a network will take a shorter amount of time. This led to the deduction that a critical node will be the one that would increase the APL of a network upon its removal and will therefore increase the time taken for communication between nodes in the network. Numerous approaches exist in literature that work on identifying critical nodes in a network.

A number of approaches that exist in literature mainly deal with the geographic location of nodes or the networks traffic flow pattern to identify these critical nodes of a network whereas, this thesis proposes two approaches, the first being an intuitive approach, that identifies critical nodes of a network (nodes that result in the highest decrease in the performance of the network upon their removal), based on a newly defined diversity index which is combined with an existing Banzhaf power index approach. The newly defined diversity index comprises of the diversity in the link length capability of a node and is referred to as the variation in link length metric and the diversity in weights of the node degree which is referred to as the weighted node degree. The combined affect of the diversity index and the banzhaf power index has been reported to outperform existing approaches in identifying critical nodes in a network. The identification of these critical nodes will aid in timely adaptation of the network so that their influence on the performance of the network can be mitigated. The proposed approach when tested for the affect it has on the topology of a network when nodes are removed based on it, then it was observed that a 7% and 18% percent increase in average path length of the random and WaxMan network topology respectively took place and a total paths elimination for the small world network topology was observed. Furthermore, it reported a $13\%, 28\%$ and 68% decrease in the average node degree for the random, WaxMan and Small World network topologies respectively which means that the identified/removed node was connected to multiple node in the network thus breaking multiple connections upon its removal. The proposed approach also outperformed existing approaches in terms of increasing the number of isolated nodes in a network. The increase in number of isolated nodes is the evidence to the fact that the network has been partitioned into multiple disconnected components. The proposed approach reported a $150\%, 400\%$ increase in the number of isolated nodes in the random and Small World network topologies respectively and a small increase of 0.8% decrease in the number of isolated nodes in a WaxMan network topology. This small increase is negligible when it comes to really large networks. The proposed approach was also tested against other approaches for analysing the connectivity and the affect it had on the performance of the network and it was observed that the critical nodes identified by the proposed approach when removed from the network result in a decrease in the algebraic connectivity of a network by 58% whereas, as for the performance of the network, the Throughput of the network degraded by 22% for the random network topology and it was backed by an increase in the average delay, average jitter and average number of dropped packet by $33\%, 45\%$ and 75% respectively. These all are evidence to the fact that the identified critical node is vital for maintaining normal network functionality and upon its removal the network undergoes major performance degradations.

In order to justify the claims made in the aforementioned work, a mathematical framework was also built which uses suboptimal solutions for two optimization problems, namely the algebraic connectivity minimization and the network utility maximization problem. The resultant solution of these optimization problems when used to identify critical nodes in a network has been shown to outperform exiting work in identifying critical nodes in a network. In this thesis, a lower bound on the algebraic connectivity is also calculated that identifies the affect on the algebraic connectivity of the network when a certain node is removed from the network. The critical node identified using this mathematical abstraction resulted in a reduction in the algebraic connectivity of the network by 22% which denotes that the network is loosely connected and the removal of a few more nodes can easily partition the network. It is also reported in this thesis that, the loosely connected network formed after removing the identified critical node results in a bottleneck close to the center of the network which increases the network congestion, reduces network throughput by 16% and increases the average per packet delay, the average number of dropped packets and the average jitter experienced in the network by 6%, 4% and 6% receptively. The proposed approach is complimented in this thesis with a distributed implementation that is computationally less complex and can be implemented in complex networks. It was observed that the proposed approach reduces the average computation time of a network by 36% when compared to existing approaches in the network. These statistics clearly state that the proposed approach outperforms existing approaches in identifying critical nodes in a network and that these nodes when removed result in a higher degradation in performance of the network, therefore, in order to maintain normal network functionality, it is necessary to timely identify these critical nodes and take appropriate measures.

7.2 Future Direction of Research

This thesis proposes solutions to two major problems, the first being the estimation of the average path length of a network and the second being the identification of critical nodes in a network. In the first problem, the underlying assumption is of reducing an arbitrary network into a tree structure, the elimination of this assumption will lead to multiple open problems and this can be used as a future direction of work.

The second problem that is being addressed by this thesis initiates its own set of problems that can be addressed in the future. The first being that, as a conventional approach the vulnerability of a network is estimated for a particular instance when the most critical node is removed from the network, but in real life scenarios, most of the networks have a recovery mechanism with the aid of which they adapt and change the network structure to regain maximum network utility. A new direction of research in this domain would be of finding a particular critical node, who's removal will have an impact that cannot be recovered by the network with the aid of a conventional recovery mechanism.

Along with this, another open problem that originates from this thesis is the design of an efficient distributed critical node identification mechanism. This thesis also proposes a distributed mechanism for identification of critical nodes but it relies only on the sign of the Fiedler vector elements that correspond to each node in the network. It was observed during this thesis that, the magnitude of the Fiedler values decreases as one moves to a node close to the center of the network (the sign cut region) and it increases as one moves away from this region. As a future direction of research, the use of this change in magnitude along with the change in sign would help in forming a more efficient distributed critical node identification mechanism.

Bibliography

[1] Centrality metrics. *https://cs.hse.ru/data/2015 /05/14/1098547089 /4. Centrality Metrics.pdf*.

[2] Maple homepage. *http://www.maplesoft.com*.

[3] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. Wireless sensor networks: a survey. *Computer networks*, 38(4):393–422, 2002.

[4] Réka Albert, István Albert, and Gary L Nakarado. Structural vulnerability of the north american power grid. *Physical review E*, 69(2):025103, 2004.

[5] K.M. Alzoubi, P.J. Wan, and O. Frieder. Distributed heuristics for connected dominating sets in wireless ad hoc networks. *Journal of Communications and Networks*, 4(1):22–29, 2002.

[6] J.S. Andrade Jr, H.J. Herrmann, R.F.S. Andrade, and L.R. da Silva. Apollonian networks: Simultaneously scale-free, small world, euclidean, space filling, and with matching graphs. *Physical review letters*, 94(1):18702, 2005.

[7] Ashwin Arulselvan, Clayton W Commander, Oleg Shylo, and Panos M Pardalos. Cardinality-constrained critical node detection problem. In *Performance models and risk management in communications systems*, pages 79–91. Springer, 2011.

[8] W. Asif, M. Lestas, H. K. Qureshi, and M. Rajarajan. Spectral partitioning for node criticality. In *Symposium on Computers and Communication (ISCC)*, pages 877–882. IEEE, 2015.

[9] W. Asif, H.K. Qureshi, M. Rajarajan, and M. Lestas. Cbdi: Combined banzhaf and diversity index for finding critical nodes. In *IEEE Global Communications Conference (GLOBECOM)*, pages 758–763, Dec 2014.

[10] Waqar Asif, Hassaan Khaliq Qureshi, and Muttukrishnan Rajarajan. Variable rate adaptive modulation (vram) for introducing small-world model into wsns. In *47th Annual Conference on Information Sciences and Systems*, pages 1–6. IEEE, 2013.

[11] Giorgio Ausiello, Donatella Firmani, et al. Real-time monitoring of undirected networks: Articulation points, bridges, and connected and biconnected components. *Networks*, 59(3):275–288, 2012.

[12] David Bader, Kamesh Madduri, et al. Parallel algorithms for evaluating centrality indices in real-world networks. In *International Conference on Parallel Processing, ICPP*, pages 539–550. IEEE, 2006.

[13] Abhik Banerjee, Rachit Agarwal, Vincent Gauthier, Chai Kiat Yeo, Hossam Afifi, and FB Lee. A self-organization framework for wireless ad hoc networks

as small worlds. *IEEE Transactions on Vehicular Technology*, 61(6):2659–2673, 2012.

[14] Alexander Bertrand and Marc Moonen. Distributed computation of the fiedler vector with application to topology inference in ad hoc networks. *Signal Processing*, 93(5):1106–1117, 2013.

[15] Vladimir Boginski and Clayton W Commander. Identifying critical nodes in protein–protein interaction networks. *Clustering challenges in biological networks*, pages 153–167, 2009.

[16] Phillip Bonacich. Power and centrality: A family of measures. *American journal of sociology*, pages 1170–1182, 1987.

[17] Phillip Bonacich. Some unique properties of eigenvector centrality. *Social Networks*, 29(4):555–564, 2007.

[18] U. Brandes. A faster algorithm for betweenness centrality*. *Journal of Mathematical Sociology*, 25(2):163–177, 2001.

[19] Ulrik Brandes. On variants of shortest-path betweenness centrality and their generic computation. *Social Networks*, 30(2):136–145, 2008.

[20] Pin-Yu Chen and Alfred O Hero. Local fiedler vector centrality for detection of deep and overlapping communities in networks. In *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1120–1124. IEEE, 2014.

[21] Ed H Chi, Peter LT Pirolli, James E Pitkow, Rich Gossweller, Jock D Mackinlay, and Stuart K Card. Usage based methods of traversing and displaying generalized graph structures, January 21 2003. US Patent 6,509,898.

[22] Paul Christiano, Jonathan A Kelner, Aleksander Madry, Daniel A Spielman, and Shang-Hua Teng. Electrical flows, laplacian systems, and faster approximation of maximum flow in undirected graphs. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 273–282. ACM, 2011.

[23] Richard Church and M Paola Scaparra. Analysis of facility systems reliability when subject to attack or a natural disaster. In *Critical Infrastructure*, pages 221–241. Springer, 2007.

[24] F. Clad, A. Gallais, and P. Mérindol. Energy-efficient data collection in wsn: A sink-oriented dynamic backbone. In *IEEE International Conference on Communications (ICC)*, 2012.

[25] S. Cui, A.J. Goldsmith, and A. Bahai. Energy-efficiency of mimo and cooperative mimo techniques in sensor networks. *Journal on Selected Areas in Communications*, 22(6):1089–1098, 2004.

[26] Nair Maria Maia de Abreu. Old and new results on algebraic connectivity of graphs. *Linear algebra and its applications*, 423(1):53–73, 2007.

[27] Inderjit S Dhillon. Co-clustering documents and words using bipartite spectral graph partitioning. In *Proceedings of the seventh ACM SIGKDD inter-*

national conference on Knowledge discovery and data mining, pages 269–274. ACM, 2001.

[28] Thang N Dinh, Ying Xuan, My T Thai, Panos M Pardalos, and Taieb Znati. On new approaches of assessing network vulnerability: hardness and approximation. *IEEE/ACM Transactions on Networking*, 20(2):609–619, 2012.

[29] Jürgen Drews. Drug discovery: a historical perspective. *Science*, 287(5460):1960–1964, 2000.

[30] Pradeep Dubey and Lloyd S Shapley. Mathematical properties of the banzhaf power index. *Mathematics of Operations Research*, 4(2):99–131, 1979.

[31] Leonhard Euler. Solutio problematis ad geometriam situs pertinentis. *Commentarii academiae scientiarum Petropolitanae*, 8:128–140, 1741.

[32] Miroslav Fiedler. Algebraic connectivity of graphs. *Czechoslovak Mathematical Journal*, 23(2):298–305, 1973.

[33] Miroslav Fiedler. A property of eigenvectors of nonnegative symmetric matrices and its application to graph theory. *Czechoslovak Mathematical Journal*, 25(4):619–633, 1975.

[34] Linton C Freeman. A set of measures of centrality based on betweenness. *Sociometry*, pages 35–41, 1977.

[35] Linton C Freeman. Centrality in social networks conceptual clarification. *Social networks*, 1(3):215–239, 1979.

[36] Linton C Freeman. Centered graphs and the structure of ego networks. *Mathematical Social Sciences*, 3(3):291–304, 1982.

[37] A. Fronczak, P. Fronczak, and J.A. Hołyst. Average path length in random networks. *Physical Review E*, 70(5):056110, 2004.

[38] Arpita Ghosh and Stephen Boyd. Growing well-connected graphs. In *45th Conference on Decision and Control*, pages 6605–6611. IEEE, 2006.

[39] P.J. Giabbanelli. Impact of complex network properties on routing in backbone networks. In *GLOBECOM Workshops (GC Wkshps)*, pages 389–393. IEEE, 2010.

[40] P.J. Giabbanelli, D. Mazauric, and J.C. Bermond. On the average path length of deterministic and stochastics recursive networks. *Complex Networks*, pages 1–12, 2011.

[41] Gene H Golub. Some modified matrix eigenvalue problems. *Siam Review*, 15(2):318–334, 1973.

[42] Willem H Haemers. Interlacing eigenvalues and graphs. *Linear Algebra and its applications*, 226:593–616, 1995.

[43] X. Han, X. Cao, E.L. Lloyd, and C.C. Shen. Fault-tolerant relay node placement in heterogeneous wireless sensor networks. *IEEE Transactions on Mobile Computing*, 9(5):643–656, 2010.

[44] Yuan He, Hao Ren, Yunhao Liu, and Baijian Yang. On the reliability of large-scale distributed systems–a topological view. *Computer Networks*, 53(12):2140–2152, 2009.

[45] Petter Holme, Beom Jun Kim, Chang No Yoon, and Seung Kee Han. Attack vulnerability of complex networks. *Physical Review E*, 65(5):056109, 2002.

[46] B.D. Hughes. Random walks and random environments: Volume 2: Random environments (vol 2). 1996.

[47] Muhammad Imran, Mohamed A Alnuem, Mahmoud S Fayed, and Atif Alamri. Localized algorithm for segregation of critical/non-critical nodes in mobile ad hoc and sensor networks. *Procedia Computer Science*, 19:1167–1172, 2013.

[48] A Jamakovic and Piet Van Mieghem. On the robustness of complex networks by using the algebraic connectivity. In *NETWORKING 2008 Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet*, pages 183–194. Springer, 2008.

[49] Frank Kelly. Charging and rate control for elastic traffic. *European transactions on Telecommunications*, 8(1):33–37, 1997.

[50] Frank P Kelly, Aman K Maulloo, and David KH Tan. Rate control for communication networks: shadow prices, proportional fairness and stability. *Journal of the Operational Research society*, pages 237–252, 1998.

[51] Valdis Krebs. Uncloaking terrorist networks. *First Monday*, 7(4), 2002.

[52] Stefan S Krishna, P Krishna Gummadi, and Steven D Gribble. A measurement study of peer-to-peer file sharing systems. *Multimedia Computing and Networking, San Jose, CA, USA*, 2002.

[53] Mukkai S Krishnamoorthy and Narsingh Deo. Node-deletion np-complete problems. *SIAM Journal on Computing*, 8(4):619–625, 1979.

[54] Marios Lestas, Andreas Pitsillides, Petros Ioannou, and George Hadjipollas. A new estimation scheme for the effective number of users in internet congestion control. *IEEE/ACM Transactions on Networking (TON)*, 19(5):1499–1512, 2011.

[55] Yu-Shuai Li, Da-Zhong Ma, Hua-Guang Zhang, and Qiu-Ye Sun. Critical nodes identification of power systems based on controllability of complex networks. *Applied Sciences*, 5(3):622–636, 2015.

[56] Donggang Liu, Peng Ning, and Wenliang Du. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. In *25th IEEE International Conference on Distributed Computing Systems*, pages 609–619, 2005.

[57] Hao Liu, Xianghui Cao, Jianping He, Peng Cheng, Jiming Chen, and Youxian Sun. Distributed identification of the most critical node for average consensus. *IFAC Proceedings Volumes*, 47(3):1843–1848, 2014.

[58] Hao Liu, Xianghui Cao, Jianping He, Peng Cheng, Chunguang Li, Jiming Chen, and Youxian Sun. Distributed identification of the most critical node for average consensus. *IEEE Transactions on Signal Processing*, 63(16):4315–4328, 2015.

[59] Yang-Yu Liu, Jean-Jacques Slotine, and Albert-László Barabási. Controllability of complex networks. *Nature*, 473(7346):167–173, 2011.

[60] László Lovász and József Pelikán. On the eigenvalues of trees. *Periodica Mathematica Hungarica*, 3(1):175–182, 1973.

[61] MathWorks. Matlab 2013. *http://www.mathworks.com /support /sysreq /sv-r2013a/*.

[62] Consolee Mbarushimana and Alireza Shahrabi. Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. In *21st International Conference on Advanced Information Networking and Applications Workshops*, volume 2, pages 679–684. IEEE, 2007.

[63] Russell Merris. Laplacian matrices of graphs: a survey. *Linear algebra and its applications*, 197:143–176, 1994.

[64] S. Milgram. The small world problem. *Psychology today*, 2(1):60–67, 1967.

[65] Bojan Mohar and Y Alavi. The laplacian spectrum of graphs. *Graph theory, combinatorics, and applications*, 2:871–898, 1991.

[66] Ramasuri Narayanam. A game theoretic approach to identify critical components in networked systems. In *SRII Global Conference*, pages 515–524. IEEE, 2012.

[67] ABM Nasiruzzaman and HR Pota. Critical node identification of smart power system using complex network framework based centrality approach. In *North American Power Symposium (NAPS)*, pages 1–6. IEEE, 2011.

[68] Mark EJ Newman. A measure of betweenness centrality based on random walks. *Social networks*, 27(1):39–54, 2005.

[69] NSNAM. Network simulator 3. *https://www.nsnam.org/*.

[70] Daniel P Palomar and Mung Chiang. Alternative distributed algorithms for network utility maximization: Framework and applications. *IEEE Transactions on Automatic Control*, 52(12):2254–2269, 2007.

[71] Charles Pandana and KJ Ray Liu. Robust connectivity-aware energy-efficient routing for wireless sensor networks. *IEEE Transactions on Wireless Communications*, 7(10):3904–3916, 2008.

[72] The Opte Project. Originally from the english wikipedia; licensed under cc by 2.5 via wikimedia commons, 2006.

[73] Hassaan Khaliq Qureshi, Sajjad Rizvi, Muhammad Saleem, Syed Ali Khayam, Muttukrishnan Rajarajan, and Veselin Rakocevic. An energy efficient clique-based cds discovery protocol for wireless sensor networks. In *44th Annual Conference on Information Sciences and Systems (CISS), 2010*, pages 1–6. IEEE, 2010.

[74] Hassaan Khaliq Qureshi, Sajjad Rizvi, Muhammad Saleem, Syed Ali Khayam, Veselin Rakocevic, and Muttukrishnan Rajarajan. Evaluation and improvement of cds-based topology control for wireless sensor networks. *Wireless Networks*, 19(1):31–46, 2013.

[75] H.K. Qureshi, S. Rizvi, M. Saleem, S.A. Khayam, V. Rakocevic, and M. Rajarajan. Poly: A reliable and energy efficient topology control protocol for wireless sensor networks. *Computer Communications*, 2011.

[76] Sajjad Rizvi, Hassaan Khaliq Qureshi, Syed Ali Khayam, Veselin Rakocevic, and Muttukrishnan Rajarajan. A1: An energy efficient topology control algorithm for connected area coverage in wireless sensor networks. *Journal of Network and Computer Applications*, 35(2):597–605, 2012.

[77] O Rojo, R Soto, and H Rojo. Bounds for sums of eigenvalues and applications. *Computers & Mathematics with Applications*, 39(7):1–15, 2000.

[78] S. Schnettler. A structured overview of 50 years of small-world research. *Social Networks*, 31(3):165–178, 2009.

[79] M.Á. Serrano and M. Boguná. Topology of the world trade web. *Physical Review E*, 68(1):015101, 2003.

[80] Gaurav Sharma and Ravi Mazumdar. Hybrid sensor networks: a small world. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 366–377. ACM, 2005.

[81] Z. Shelby, C. Pomalaza-Raez, H. Karvonen, and J. Haapola. Energy optimization in multihop wireless embedded and sensor networks. *International journal of wireless information networks*, 12(1):11–21, 2005.

[82] Yilin Shen, Nam P Nguyen, Ying Xuan, and My T Thai. On the discovery of critical links and nodes for assessing network vulnerability. *IEEE/ACM Transactions on Networking (TON)*, 21(3):963–973, 2013.

[83] Yilin Shen, Nam P Nguyen, Ying Xuan, and My T Thai. On the discovery of critical links and nodes for assessing network vulnerability. *IEEE/ACM Transactions on Networking*, 21(3):963–973, 2013.

[84] L. Sitanayah, K.N. Brown, and C.J. Sreenan. Fault-tolerant relay deployment for k node-disjoint paths in wireless sensor networks. In *Wireless Days (WD), IFIP*, pages 1–6. IEEE, 2011.

[85] M.E. Smoot, K. Ono, J. Ruscheinski, P.L. Wang, and T. Ideker. Cytoscape 2.8: new features for data integration and network visualization. *Bioinformatics*, 27(3):431–432, 2011.

[86] M. Soltan, I. Hwang, and M. Pedram. Modulation-aware energy balancing in hierarchical wireless sensor networks. In *3rd International Symposium on Wireless Pervasive Computing,ISWPC*, pages 355–359. IEEE, 2008.

[87] Daniel A Spielman and Nikhil Srivastava. Graph sparsification by effective resistances. *SIAM Journal on Computing*, 40(6):1913–1926, 2011.

[88] Daniel A Spielman and Shang-Hua Teng. Spectral partitioning works: Planar graphs and finite element meshes. *Linear Algebra and its Applications*, 421(2):284–305, 2007.

[89] E. Stai, V. Karyotis, and S. Papavassiliou. Socially-inspired topology improvements in wireless multi-hop networks. In *International Conference on Communications Workshops (ICC)*, pages 1–6. IEEE, 2010.

[90] S.H. Strogatz. Exploring complex networks. *Nature*, 410(6825):268–276, 2001.

[91] Godfried T Toussaint. The relative neighbourhood graph of a finite planar set. *Pattern recognition*, 12(4):261–268, 1980.

[92] Mario Ventresca and Dionne Aleman. Efficiently identifying critical nodes in large complex networks. *Computational Social Networks*, 2(1):1, 2015.

[93] Chetan Kumar Verma, Bheemarjuna Reddy Tamma, BS Manoj, and Ramesh Rao. A realistic small-world model for wireless mesh networks. *Communications Letters, IEEE*, 15(4):455–457, 2011.

[94] P.J. Wan, K.M. Alzoubi, and O. Frieder. Distributed construction of connected dominating set in wireless ad hoc networks. In *Twenty-First Annual Joint Conference of the Computer and Communications Societies, INFOCOM*, volume 3, pages 1597–1604. IEEE, 2002.

[95] P. Wang and I.F. Akyildiz. Spatial correlation and mobility-aware traffic modeling for wireless sensor networks. *IEEE/ACM Transactions on Networking (TON)*, 19(6):1860–1873, 2011.

[96] Takamitsu Watanabe and Naoki Masuda. Enhancing the spectral gap of networks by node removal. *Physical Review E*, 82(4):046102, 2010.

[97] D. Watts and S. Strogatz. The small world problem. *Collective Dynamics of Small-World Networks*, 393:440–442, 1998.

[98] D.J. Watts. Networks, dynamics, and the small-world phenomenon 1. *American Journal of Sociology*, 105(2):493–527, 1999.

[99] Duncan J Watts and Steven H Strogatz. Collective dynamics of small-worldnetworks. *nature*, 393(6684):440–442, 1998.

[100] Bernard M Waxman. Routing of multipoint connections. *IEEE Journal on Selected Areas in Communications*, 6(9):1617–1622, 1988.

[101] WT Webb and R. Steele. Variable rate qam for mobile radio. *IEEE Transactions on Communications*, 43(7):2223–2230, 1995.

[102] Peng Wei and Dengfeng Sun. Weighted algebraic connectivity: An application to airport transportation network. In *Proceedings of the 18th IFAC World Congress, Milan, Italy*, 2011.

[103] P.M. Wightman and M.A. Labrador. A3: A topology construction algorithm for wireless sensor networks. In *Global Telecommunications Conference, GLOBECOM*, pages 1–6. IEEE, 2008.

[104] J. Wu, M. Cardei, F. Dai, and S. Yang. Extended dominating set and its applications in ad hoc networks using cooperative communication. *IEEE Transactions on Parallel and Distributed Systems*, 17(8):851–864, 2006.

[105] X Xiaochun and W Xiaoyan. A simple rate control algorithm for maximizing total user utility. In *Proceedings of the International Conference on Communication Technology*, pages 135–138, 2003.

[106] Ning Xu, Sumit Rangwala, Krishna Kant Chintalapudi, Deepak Ganesan, Alan Broad, Ramesh Govindan, and Deborah Estrin. A wireless sensor network for structural monitoring. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 13–24. ACM, 2004.

[107] P Yu and H Van de Sompel. Networks of scientific papers. *Science*, 169:510–515, 1965.

[108] Z. Yuanyuan, X. Jia, and H. Yanxiang. Energy efficient distributed connected dominating sets construction in wireless sensor networks. In *Proceedings of the international conference on Wireless communications and mobile computing*, pages 797–802. ACM, 2006.

[109] Z. Zhang, L. Chen, S. Zhou, L. Fang, J. Guan, and T. Zou. Analytical solution of average path length for apollonian networks. *Physical Review E*, 77(1):017102, 2008.

[110] Zhongzhi Zhang, Lili Rong, and Chonghui Guo. A deterministic small-world network created by edge iterations. *Physica A: Statistical Mechanics and its Applications*, 363(2):567–572, 2006.

[111] Z. Zinonos, V. Vassiliou, C. Ioannou, and M. Koutroullos. Dynamic topology control for wsns in critical environments. In *4th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5. IEEE, 2011.