ON ROBUSTNESS IN HIGH LOAD MOBILE AD HOC NETWORKS

BY

PAUL EDWARD ROGERS

BS, Binghamton University, 1998
MS, Binghamton University, 1999

DISSERTATION

Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science in the Graduate School of Binghamton University
State University of New York
2005
Submitted in partial fulfillment of the requirements for
the degree of Doctor of Philosophy in Computer Science
in the Graduate School of
Binghamton University
State University of New York
2005

December 2, 2005

Nael B. Abu-Ghazaleh, Department of Computer Science, Binghamton University

Kenneth Chiu, Department of Computer Science, Binghamton University

Michael J. Lewis, Department of Computer Science, Binghamton University

Douglas H. Summerville, Department of Electrical and Computer Engineering,
Binghamton University
Abstract

Mobile Ad hoc Networks (MANETs) are increasing in popularity as an approach for cost-effective and fast deployment of wireless connectivity. As their use increases in the context of mesh networks, sensor networks, as well as for traditional ad hoc networks, applications that use them are emerging. Thus, protocols for MANETs must mature beyond the idealized assumptions made in their evaluation towards protocols that are robust and effective in real-world deployments.

In this work, it is first shown that MANETs experience erratic and unpredictable behavior under high loads even in the absence of mobility. Some of the causes of the behavior are identified by analysis of problematic scenarios. Two contributing problems are isolated and then analyzed. The major focus of the work (the first problem considered) is the poor robustness of Network Wide Broadcast (NWB) algorithms. NWBs provide an important primitive operation that underlies many routing and group communication operations. It is shown that NWBs do not provide a high amount of coverage in a network that is prone to losses (due to interference under high load, or losses due to signal fading), and therefore are not robust when faced with losses in the network.

Most existing NWB algorithm research focuses on reducing the overhead of these algorithms. The work in this dissertation focuses on increasing their robustness. The root of the robustness problem is the unreliability of the Medium Access Control (MAC) level broadcast primitive. This component of the work first classifies NWB according to their features that influence robustness. These algorithms are studied experimentally to evaluate their robustness.

In order to improve the robustness of a NWB, the potential solution space for NWB algorithms is reviewed. Solutions that use implicit feedback, explicit feedback, and solutions that provide a fixed level of redundancy based on factors such as the network quality are examined. Protocols that improve the coverage of a NWB in each sector of the solution space are proposed.

First, to improve NWB robustness, a selective rebroadcast approach is evaluated. This network level solution leads to a leads to considerable improvement in NWB coverage, with only a small increase in overhead. This solution, which relies on implicit feedback, can be added to virtually all NWB approaches in order to improve their reliability.

Second, a new MAC level primitive is proposed, which significantly improves the reliability of link level broadcast. In particular, this solution that uses explicit feedback is especially suited for optimized NWB algorithms that build a virtual backbone because it
allows full reliability for the messages as they cross the backbone.

Lastly, this work proposes a new CDS algorithm that assigns qualities to links between nodes, and builds a tree to cover these nodes that takes the qualities into account. Existing CDS algorithms view the connections between nodes as boolean values; the nodes are either connected or not. By making use of the state of the network, more robust protocols can be designed which provide some fixed level of redundancy, based on external factors.

The second problem examined in this dissertation is the problem of unpredictable hop-level interactions under high load. More specifically, it is observed that destructive interactions occur in some scenarios that allow certain transmitters to capture the medium. While unfairness is a known problem with some solutions in MANET MAC, these solutions were not successful in significantly improving the observed effect. It is hypothesized that the effect occurs due to the different interaction relationships that arise among nodes depending on their relative location to one another (influencing the interference level, the carrier sense and Request to Send/Clear to Send (RTS/CTS) reception capabilities). Such micro-level studies have not been conducted in the past.
For Danielle. I love you.
Acknowledgements

My thanks and appreciation go to a large number of people.

First, to Nael Abu-Ghazaleh, for serving as my advisor these past few years. It has been a long road, and I appreciate your guidance along the way. You’ve helped me learn about an interesting topic and provided me with assistance as needed.

Thanks to the members of my committee: Ken Chiu, Mike Lewis, and Doug Summerville. The time you spent working with me and giving advice is greatly appreciated.

I appreciate the guidance of the researchers in the field that I have spoken with, especially Dr. Tracy Camp, from the Colorado School of Mines, and Dr. Wei Lou, from Florida Atlantic University.

I thank all of the professors and teachers I’ve had over the course of my education. You have helped nurture a hunger for knowledge and have taught me the skills to obtain it.

Thanks to all of my friends who provided a constant stream of support. I consider myself fortunate to have so many friends that consistently checked in on my journey that I can not name them all here.

Thanks to all of my family for their unending support and love as I worked on my Ph.D. The encouragement you provided as I worked towards my degree was always appreciated.

Lastly, thanks to Danielle for your unwavering support through these past few years. You helped me keep going on so many days. Thank you.
Contents

Abstract v
Dedication vii
Acknowledgements ix
List of Tables xv
List of Figures xvii

Part I: Introduction 1

1 Introduction 1
1.1 Motivation: MANET Behavior under High Loads 2
1.2 Research and Contribution Overview 2
1.2.1 Robust Network Wide Broadcast 3
1.2.2 Preliminary Characterization of Micro-level MAC Interactions 6
1.3 Contribution Summary 6
1.4 Dissertation Structure 8

2 Introduction to MANETs 11
2.1 Wireless Propagation Basics 12
2.1.1 Propagation Models 12
2.2 Medium Access Control 14
2.2.1 Node Interactions 17
2.3 Routing 19
2.3.1 Routing Protocols 20

Part II: Literature Survey 23

3 Literature Review 23
3.1 Overview and Classification of NWB Algorithms 24
3.1.1 Topology-Independent (Flooding) Approaches 24
3.1.2 Topology Sensitive Approaches 25
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2 MAC Level Solutions to NWB Robustness</td>
<td>27</td>
</tr>
<tr>
<td>3.3 NWB Algorithms Targetting Robustness</td>
<td>31</td>
</tr>
<tr>
<td>3.4 MAC Fairness</td>
<td>32</td>
</tr>
<tr>
<td>3.5 Capacity</td>
<td>34</td>
</tr>
<tr>
<td>3.6 Quality of Service</td>
<td>36</td>
</tr>
<tr>
<td>3.7 Summary</td>
<td>38</td>
</tr>
<tr>
<td>Part III: Problem Definition/Hypothesis</td>
<td>41</td>
</tr>
<tr>
<td>4 Motivating Scenario and Problem Identification</td>
<td>41</td>
</tr>
<tr>
<td>4.1 Analysis of a Representative Scenario</td>
<td>42</td>
</tr>
<tr>
<td>4.2 Problem Statement</td>
<td>48</td>
</tr>
<tr>
<td>Part IV: Evidence</td>
<td>51</td>
</tr>
<tr>
<td>5 Network Wide Broadcast Robustness</td>
<td>51</td>
</tr>
<tr>
<td>5.1 Broadcast Robustness</td>
<td>52</td>
</tr>
<tr>
<td>5.1.1 Losses Due To Self-Interference</td>
<td>52</td>
</tr>
<tr>
<td>5.1.2 Losses Due To Shadowing</td>
<td>53</td>
</tr>
<tr>
<td>5.2 Preliminaries and Experimental Setup</td>
<td>53</td>
</tr>
<tr>
<td>5.3 Evaluated Algorithms</td>
<td>55</td>
</tr>
<tr>
<td>5.4 Grid Topologies</td>
<td>57</td>
</tr>
<tr>
<td>5.5 Random Topologies</td>
<td>58</td>
</tr>
<tr>
<td>5.5.1 Controlled Drop</td>
<td>58</td>
</tr>
<tr>
<td>5.5.2 Signal Fading Losses</td>
<td>60</td>
</tr>
<tr>
<td>5.6 Cluster Topologies</td>
<td>61</td>
</tr>
<tr>
<td>5.6.1 Controlled Drop</td>
<td>61</td>
</tr>
<tr>
<td>5.6.2 Signal Fading Losses</td>
<td>62</td>
</tr>
<tr>
<td>5.7 Mobile Topologies</td>
<td>63</td>
</tr>
<tr>
<td>5.7.1 Random Waypoint</td>
<td>63</td>
</tr>
<tr>
<td>5.7.2 Probabilistic Random Walk</td>
<td>65</td>
</tr>
<tr>
<td>5.8 Summary</td>
<td>67</td>
</tr>
<tr>
<td>Part V: Solutions</td>
<td>69</td>
</tr>
<tr>
<td>6 Robustness Control – Solution Space</td>
<td>69</td>
</tr>
<tr>
<td>6.1 NWB Robustness Control – Solution Space</td>
<td>70</td>
</tr>
<tr>
<td>6.1.1 Explicit Feedback Algorithms</td>
<td>70</td>
</tr>
<tr>
<td>6.1.2 Implicit Feedback Algorithms</td>
<td>71</td>
</tr>
<tr>
<td>6.2 Classifying Existing Solutions</td>
<td>72</td>
</tr>
<tr>
<td>6.3 Summary</td>
<td>73</td>
</tr>
</tbody>
</table>
### 7 Selective Additional Rebroadcast

7.1 Selective Additional Rebroadcast .................................................. 75
7.2 Experimental Evaluation ............................................................... 80
  7.2.1 Preliminaries ................................................................. 80
  7.2.2 Evaluation of SAR Approaches ............................................. 81
  7.2.3 Adaptive SAR Evaluation .................................................. 83
7.3 Summary ..................................................................................... 85

### 8 Directed Broadcast

8.1 Overview .................................................................................... 87
8.2 Related Work .............................................................................. 89
8.3 Improving NWB Reliability with DB ........................................... 90
8.4 Experimental Evaluations ......................................................... 91
  8.4.1 Preliminaries ................................................................. 91
  8.4.2 Base Case ................................................................. 92
  8.4.3 Directed Broadcast Evaluation ........................................... 93
  8.4.4 Dense Network Evaluation .............................................. 94
8.5 Summary ..................................................................................... 96

### 9 Link-Quality Sensitive Connected Dominating Set NWB

9.1 Background ................................................................................. 98
9.2 Link Quality Sensitive CDS .......................................................... 101
9.3 Experimental Evaluation ............................................................. 105
  9.3.1 Preliminaries ................................................................. 105
  9.3.2 Base Case ................................................................. 106
9.4 LQ-CDS Evaluation ................................................................. 107
9.5 Summary ..................................................................................... 109

Part VI: Microanalysis

10 Micro-Analysis ........................................................................... 111
10.1 Overview and Methodology ....................................................... 111
10.2 Experimental Study ................................................................. 112
10.3 Fairness ................................................................................... 116
10.4 Throughput .............................................................................. 118
10.5 Effect of Packet Size ............................................................... 118
10.6 Collision Analysis .................................................................. 119
10.7 General Scenario Applicability .................................................. 119
10.8 Enumerating Interaction Cases ................................................ 120
10.9 Summary ................................................................................... 123

Part VII: Conclusion ...................................................................... 125
11 Future Work 125
12 Conclusion 127
Appendices 131
A Topology Samples 131
B Micro-Analysis Layouts 133
C Curriculum Vitae 137
D Bibliography 139
List of Tables

3.1 Neighbor Knowledge NWB Approaches ........................................ 32

4.1 RREQ Failures ................................................................. 47

10.1 Scenario Criteria ............................................................ 113
10.2 Standard 802.11, RTS/CTS enabled, % potential packets sent successfully ........................................ 114
10.3 Standard 802.11, RTS/CTS disabled, % potential packets sent successfully ........................................ 115
10.4 MILD, RTS/CTS enabled, % potential packets sent successfully ........................................ 115
10.5 MILD, RTS/CTS disabled, % potential packets sent successfully ........................................ 116
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Transmission with Omni-Directional Antenna</td>
<td>16</td>
</tr>
<tr>
<td>2.2</td>
<td>The Hidden Terminal Problem</td>
<td>17</td>
</tr>
<tr>
<td>2.3</td>
<td>The Exposed Terminal Problem</td>
<td>17</td>
</tr>
<tr>
<td>4.1</td>
<td>Three Competing FTP Connections</td>
<td>42</td>
</tr>
<tr>
<td>4.2</td>
<td>Scenario Depiction</td>
<td>43</td>
</tr>
<tr>
<td>4.3</td>
<td>Three Competing CBR Connections</td>
<td>45</td>
</tr>
<tr>
<td>4.4</td>
<td>Two Competing CBR Connections</td>
<td>45</td>
</tr>
<tr>
<td>4.5</td>
<td>Two Competing CBR Connections (MILD)</td>
<td>45</td>
</tr>
<tr>
<td>5.1</td>
<td>Coverage of Flooding (Grid Deployment, Controlled Drop)</td>
<td>58</td>
</tr>
<tr>
<td>5.2</td>
<td>Coverage of Flooding (Grid Deployment, Fading)</td>
<td>58</td>
</tr>
<tr>
<td>5.3</td>
<td>Coverage (Random Deployment, Controlled Drop, Flooding)</td>
<td>59</td>
</tr>
<tr>
<td>5.4</td>
<td>Coverage (Random Deployment, Controlled Drop, 30 Nodes)</td>
<td>59</td>
</tr>
<tr>
<td>5.5</td>
<td>Overhead (Random Deployment, Controlled Drop, 30 Nodes)</td>
<td>59</td>
</tr>
<tr>
<td>5.6</td>
<td>Coverage (Random Deployment, Controlled Drop, 60 Nodes)</td>
<td>60</td>
</tr>
<tr>
<td>5.7</td>
<td>Overhead (Random Deployment, Controlled Drop, 60 Nodes)</td>
<td>60</td>
</tr>
<tr>
<td>5.8</td>
<td>Coverage (Random Deployment, Fading)</td>
<td>61</td>
</tr>
<tr>
<td>5.9</td>
<td>Overhead (Random Deployment, Fading)</td>
<td>61</td>
</tr>
<tr>
<td>5.10</td>
<td>Coverage (Cluster Deployment, Controlled Drop)</td>
<td>61</td>
</tr>
<tr>
<td>5.11</td>
<td>Overhead (Cluster Deployment, Controlled Drop)</td>
<td>61</td>
</tr>
<tr>
<td>5.12</td>
<td>Coverage (Cluster Deployment, Fading)</td>
<td>62</td>
</tr>
<tr>
<td>5.13</td>
<td>Overhead (Cluster Deployment, Fading)</td>
<td>62</td>
</tr>
<tr>
<td>5.14</td>
<td>Coverage (RW, Controlled Drop, 30 Nodes)</td>
<td>63</td>
</tr>
<tr>
<td>5.15</td>
<td>Overhead (RW, Controlled Drop, 30 Nodes)</td>
<td>63</td>
</tr>
<tr>
<td>5.16</td>
<td>Coverage (RW, Controlled Drop, 60 Nodes)</td>
<td>64</td>
</tr>
<tr>
<td>5.17</td>
<td>Overhead (RW, Controlled Drop, 60 Nodes)</td>
<td>64</td>
</tr>
<tr>
<td>5.18</td>
<td>Coverage (RW, Fading)</td>
<td>64</td>
</tr>
<tr>
<td>5.19</td>
<td>Overhead (RW, Fading)</td>
<td>64</td>
</tr>
<tr>
<td>5.20</td>
<td>Coverage (PRW, Controlled Drop, 30 Nodes)</td>
<td>65</td>
</tr>
<tr>
<td>5.21</td>
<td>Overhead (PRW, Controlled Drop, 30 Nodes)</td>
<td>65</td>
</tr>
<tr>
<td>5.22</td>
<td>Coverage (PRW, Controlled Drop, 60 Nodes)</td>
<td>66</td>
</tr>
<tr>
<td>5.23</td>
<td>Overhead (PRW, Controlled Drop, 60 Nodes)</td>
<td>66</td>
</tr>
</tbody>
</table>
A.1 30 nodes ......................................................... 131
A.2 40 nodes ......................................................... 131
A.3 50 nodes ......................................................... 131
A.4 60 nodes ......................................................... 131
A.5 5x5 grid ......................................................... 132
A.6 6x6 grid ......................................................... 132
A.7 7x7 grid ......................................................... 132
A.8 8x8 grid ......................................................... 132
A.9 Cluster ......................................................... 132

B.1 Scenario 1 ...................................................... 133
B.2 Scenario 2 ...................................................... 133
B.3 Scenario 3 ...................................................... 133
B.4 Scenario 4 ...................................................... 133
B.5 Scenario 5 ...................................................... 134
B.6 Scenario 6 ...................................................... 134
B.7 Scenario 7 ...................................................... 134
B.8 Scenario 8 ...................................................... 134
B.9 Scenario 9 ...................................................... 134
B.10 Scenario 10 .................................................... 134
B.11 Scenario 11 .................................................... 134
B.12 Scenario 12 .................................................... 134
B.13 Scenario 13 .................................................... 135
B.14 Scenario 14 .................................................... 135
Chapter 1

Introduction

A Mobile Ad hoc Network (MANET) is a network made up of mobile nodes without a fixed infrastructure [1]. Nodes in a MANET participate in forwarding traffic throughout the network, creating multi-hop wireless connections. MANETs are useful whenever infrastructure is unavailable or expensive, and quick deployment is desired. MANETs have been used for many applications such as military operations, search-and-rescue operations, and in providing on-the-fly connectivity in conference settings. They have also been used to extend the range of last hop networks [2, 3]. MANETs are becoming more useful and important with the emergence of sensor networks and smart environments [4]. In addition, Mesh networks and Community Area networks (both forms of Ad hoc Networks) are emerging technologies that are forecast to play an important role for reliable and cost-effective approaches for broadband Internet access [5]. For example, several companies are field-testing wireless networks to expose communities to broadband Internet access for the first time [6, 7].
1.1 Motivation: MANET Behavior under High Loads

Since MANETs are becoming more common, applications that use them are emerging. However, it can be shown that under high load, MANET operation is erratic and unpredictable. More specifically, in the presence of high load, or unreliable wireless channels, unpredictable behavior, loss of efficiency and severe unfairness arises, with some connections suffering prolonged periods of little or no connectivity. Clearly, such behavior significantly impacts the utility of MANETs.

Despite the large amount of research in the area, this problem has not been studied in detail; most studies use limited scenarios and a “black-box” approach to performance analysis that does not deeply investigate the causes of the observed behavior. This is an important problem because MANETs need to be able to support high loads gracefully in order to be viewed as a viable networking option. While some of the underlying causes have been identified (e.g., congestion and interactions between routing and Medium Access Control (MAC) layers [8]), the problem is not completely understood.

1.2 Research and Contribution Overview

In this work, first some of the causes of the erratic and unpredictable behavior observed in MANETs under high loads are identified by analysis of problematic scenarios. The first observed problem is that Network Wide Broadcast (NWB) algorithms, which are used to propagate routing information as the topology changes due to mobility, are not robust. It is shown that NWBs do not provide acceptable coverage in a network that is prone to losses (due to interference under high load, or losses due to signal fading on a wireless channel). As a result, when routes are lost (due to mobility, or persistent packet loss that can occur under high load), some connections cannot discover alternative routes because their route discovery NWB fails to reach the destination. While most existing NWB algorithm
research focuses on reducing the overhead of these algorithms, the problem targeted in this dissertation is that of their robustness. Note that NWB algorithms are not only important for routing, but also for group communication operations such as multicast, anycast, and GeoCast [9, 10, 11, 12, 13].

The second observed problem is that unfairness exists in MANETs in a way that is different from the unfairness effects studied in MANET literature. While short term unfairness is well known and has been studied in-depth, long term unfairness due to network topologies has not previously been examined.

The precise problem of unfairness is defined and explored later on in this work in Chapter 3. Some cases arise that exhibit unfair behavior for connections, both with the standard 802.11 MAC protocol as well as with the Multiplicative Increase/Linear Decrease (MILD) fairness algorithm. The study used to locate the areas of unfairness and the knowledge gained from this research will also prove to be useful in understanding and quantifying MANET behavior in general.

1.2.1 Robust Network Wide Broadcast

The first contribution in this area is to classify existing NWB algorithms with respect to robustness and validate this classification using a detailed study of representative algorithms from the identified classes. The overhead of these NWB algorithms is tracked as well, in order to see how coverage is related to the number of broadcasts used in a NWB. In general, it can be observed that reducing the overhead of NWB algorithms results in increasing their vulnerability to losses. In addition, distributed algorithms that take forwarding decisions locally are found to be more robust because they can dynamically compensate for some losses.

The second contribution in this area is to introduce and examine several solutions to increase the robustness of NWB algorithms without excessively increasing their overhead.
There are many potential solutions in the solution space for NWB robustness. Full reliability requires explicit feedback from all nodes in the network, and is too expensive. Implicit feedback solutions attempt to predict losses based on the observed behavior of the network. Explicit feedback solutions require selected notes to provide feedback, in order to achieve NWB robustness. Finally, other solutions can monitor the state of the wireless channel, in order to create more effective strategies for robust NWBs. Solutions in each category of the solution space are as follows:

- Selective Additional Rebroadcast (SAR): In key places, when performing a NWB, perform an additional rebroadcast in order to raise the probability that a packet is heard at neighboring nodes. This protocol uses implicit feedback to locally infer the probability of a loss, and compensates by generating an additional rebroadcast if a loss is predicted. As many NWB protocols reduce on overhead by sacrificing redundancy, NWBs are more prone to failure if a single NWB packet is lost due to collision. One challenge is to raise this level of coverage without raising overhead significantly. Thus, the key challenge with this approach is to estimate when it is likely that a broadcast has been lost, and that there are not other broadcasts that can compensate for it.

- Directed Broadcast (DB): When sending NWB data, a new MAC-level primitive is used in order to guarantee packet delivery to a single neighbor. The key difficulty with making MAC level broadcast reliable is that it is a one-to-many operation; carrying out handshaking for reliability with multiple receivers concurrently is difficult. In this approach, this difficulty is solved by electing a single neighbor as the partner in the handshake. Neighboring nodes who did not participate in the handshake can still receive the packet and process it as if it came in as a broadcasted packet. This has a challenge of deciding which neighbor or neighbors to perform a hand-
shake with. Essentially, this approach implements explicit feedback but only from a selected neighbor.

DB has attractive properties compared to existing MAC solutions to improve broadcast reliability. For example, the ability to control the neighbor that receives the packet reliably is essential for improving the reliability of a class of NWB algorithms that relies on a virtual backbone; DB allows packets to reliably be delivered to the backbone nodes, significantly improving robustness. Furthermore, DB can be adapted to perform the handshake and send the packet multiple times, ensuring that more neighbors receive the packet. Initial studies indicate this solution yields coverage near flooding for a single handshake, and results above flooding for two handshakes. Both of these approaches yield overheads below flooding, as well.

- Link Quality Sensitive Connected Dominating Set (LQ-CDS) Algorithm: The problem of constructing a CDS when considering link quality (which varies due to shadowing and possibly interference) is formulated. Existing CDS algorithms consider node coverage as a boolean value – a node is either covered or not. In reality, link qualities are a value that fluctuates between 0 and 1, with some links being more stable than others (e.g., due to the proximity of the nodes). The quality can vary due to the distance between the nodes, the amount of traffic near the nodes, and the potential bandwidth of the link. In this solution, the CDS is formulated in the presence of variable quality links. This approach illustrates how feedback based on the wireless channel can be used to optimize NWB operations. However, the approach requires the ability to track link quality [14, 15] and then compute a CDS backbone that provides coverage probabilistically.
1.2.2 Preliminary Characterization of Micro-level MAC Interactions

The second problem examined is that unfairness issues arise in MANETs that are not the typical unfairness problem studied in the MANET literature. While short term unfairness is a known problem in MAC protocols such as IEEE 802.11, long term unfairness with regards to relative node locations has not been studied in depth to our knowledge. To study possible MAC level interaction modes, two single hop connections are examined in different configurations to see what interaction patterns occur.

In order to demonstrate that the unfairness issues are not related to the well known unfairness problems in MANETs, the IEEE 802.11 protocol is studied in conjunction with one of the published MANET fair MAC algorithms. The results indicate that fairness problems exist in both protocols. In addition, the effect of the Request to Send/Clear to Send (RTS/CTS) handshake is studied. It can be seen that by disabling this handshake, fairness and overall throughput are improved. The observations made in these studies should fuel interest in solutions that are able to address the roots of the exposed effects.

1.3 Contribution Summary

The major contributions of this work to the MANET research community are as follows:

1. An analysis of existing NWB protocols with respect to robustness: Existing studies of NWB algorithms focus on the coverage to overhead tradeoffs under idealized low-load settings. In contrast, this work classifies these algorithms with respect to properties that influence their robustness. In general, it can be observed that reducing the redundancy in NWBs harms robustness. Moreover, it is shown that protocols which do dynamic forwarding decisions outperform those whose decisions are static because of their ability to compensate for losses.
2. Evaluation of the NWB robustness solution space: The potential solutions for NWB robustness management are evaluated. Examples of these are implicit feedback solutions, which require no extra data on the channel, explicit feedback solutions, which leverage data from select nodes in the network to achieve higher robustness, and solutions that monitor the network channel, and create NWB protocols that make use of this data. From this solution space, example protocols of interest are developed and evaluated.

3. A network level mechanism for increasing node coverage of NWB protocols: The mechanism of selectively adding an additional rebroadcast of NWB data is shown to increase coverage without greatly increasing overhead. Different metrics can be used to control the number of additional rebroadcasts, allowing the solution to be blind, not-blind, or adaptive.

4. A MAC level mechanism for increasing node coverage in a NWB: A new MAC level primitive called Directed Broadcast is introduced. This MAC layer solution leverages the reliability of a unicast packet, while providing the function of a broadcast packet.

5. A new network level NWB protocol that considers varying link qualities: Most NWB protocols only consider shadowing at a basic level when performing a NWB- a packet is either received or it is not. In reality, link quality under signal fading is more than a boolean value- it is a metric that indicates the probability of a packet being propagated successfully. This protocol takes into consideration each link’s distance, and weights it with a probability. When performing a NWB, a CDS is built that attempts to cover all nodes in the network with a given probability.

6. A study of micro-effects in a MANET: Existing research today does not examine the interaction between flows in general scenarios, and tends to focus on single connections. With many protocol layers, the behavior of a MANET is difficult to quantify.
The contribution presented here serves as a building block for understanding what happens in a large-scale MANET with multiple connections.

1.4 Dissertation Structure

The structure of the remainder of this work is as follows:

- Chapter 2: This section provides an introduction to MANETs. Key concepts of mobile computing such as physical limitations, MAC layer protocol, and routing protocols are overviewed.

- Chapter 3: This section gives an overview of related work. Work dealing with broadcasts in a MANET is studied. Additionally, areas such as MAC capacity and fairness are explored.

- Chapter 4: This section provides a hypothesis on why MANETs do not perform well under high loads. Potential reasons as to why they do not perform well are refuted, and a set of claims are made, which serve as the problem statement for this dissertation.

- Chapter 5: This section characterizes NWB unreliability with respect to robustness. Overhead and node coverage are examined for a number of protocols, and it can be seen that coverage is impacted as the overhead is reduced.

- Chapter 6: This section overviews the potential NWB robustness solution space. Existing solutions are classified with respect to the space, along with the solutions presented in this dissertation.

- Chapter 7: This section explains the details of the SAR protocol. Its value is presented by comparing present day NWB algorithms to the modified versions that use
• Chapter 8: This section covers the details of the DB protocol. Evidence of its value is presented by comparing present day NWB algorithms against modified versions that use DB.

• Chapter 9: This section explores the implementation of a link quality-aware CDS-based protocol.

• Chapter 10: This section examines the interactions of two single hop connections. Different topologies of the connections are analyzed in order to better understand the behavior of a general scenario MANET.

• Chapter 11: This section describes future work that can be done, using the ideas presented in this work as a base.

• Chapter 12: This section summarizes the entire dissertation and presents some concluding remarks.
Chapter 2

Introduction to MANETs

In this chapter, basic Mobile Ad hoc Network (MANET) operation principles are presented to provide the necessary background for understanding the research in this dissertation. The chapter is organized into three sections: the first two discuss Medium Access Control (MAC) and routing issues, while the final section overviews basic wireless propagation and channel models.

A MANET is a collection of wireless nodes that form a network. This network has no fixed infrastructure and is self-configuring and dynamic. In such a network, nodes cooperate in routing packets among each other. MANETs characteristics present challenges to several aspects of networking protocol design. First, since the nodes are mobile, existing links may break as nodes move away from each other and new links appear as they move in range with each other. As a result, route searching algorithms are needed to track the dynamic network topology in the presence of mobility. Due to their wireless nature, MANET nodes are constrained in terms of resources and available bandwidth. Effective protocols take these limitations into account to produce energy efficient and bandwidth efficient operation.
2.1 Wireless Propagation Basics

For nodes to receive data, packets must be transmitted wirelessly. This section presents a brief overview of wireless propagation, in order to describe some of the challenges that are present, namely the loss of data that can occur during packet transmission.

The wireless channel is a complex time-variant, space-variant entity that is extremely difficult to model in practice. To abstract the details of wireless propagation and to focus on its implications on simulation based experimental evaluation, this section discusses propagation with an emphasis on packet level simulation models. A more formal treatment of wireless propagation can be found in wireless propagation literature (e.g., [16]).

A wireless signal is propagated a number of ways, depending on the environment it is being transmitted in. In free space, and with no obstructions, the receiver is in line of sight and the signal attenuates with $\frac{1}{r^2}$ where $r$ is the distance between the sender and receiver. In more realistic settings, the signal between two points may reflect and refract off of multiple objects during transmission. This phenomenon results in multiple waves being received, and is referred to as multipath. When the signals are out of phase, the signal strength can diminish, resulting in what is referred to as multipath fading [17].

2.1.1 Propagation Models

For simulation studies to be accurate and valid, the wireless propagation model should be realistic [18]; however, significant challenges remain and most of the MANET community accepts the use of idealized models [19].

Different propagation models are used to model the signal power of an incoming packet at a node. If the signal power of the inbound packet is below the node’s receiving threshold, the packet is marked as an error and dropped by the MAC layer. Moreover, if the ratio of the received signal power to the total interference power (from noise and concurrent
transmissions) falls below the capture threshold (typically 10–20), the packet is lost due to interference – otherwise, capture can occur even in the presence of interference.

The simplest model of wireless propagation study is known as the Free Space model. In this model, the power of a signal is the inverse proportion of the square of the distance between two nodes. The received signal power is shown as:

\[ P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \]

In this function, \( P_t \) is the transmitted signal power, \( G_t \) and \( G_r \) are the antenna gains for the transmitting and receiving nodes, \( L \) is the system loss, \( \lambda \) represents the signal wavelength, and \( d \) is the distance between two nodes.

The Free Space model is unrealistic given the effects found in real wireless channels. Therefore, in many simulations of MANETs, the propagation model known as the Two Ray Ground model is used. This model uses the reflection of a signal off of the ground, as well as the directly propagated signal. At short distances, the directly propagated signal is used, while longer distances use the reflected signal. The received signal power is calculated as:

\[ P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \]

In this function, \( h_t \) and \( h_r \) are the antenna heights (other variables are the same as in the Free Space model). The crossover distance \( d_c \) is represented as:

\[ d_c = \frac{4\pi h_t^2 h_r^2}{\lambda} \]

The crossover distance represents the point where the Free Space model is used for short distances.

As both models are unrealistic for real world environments, another model has started
to be used, called the signal fading propagation model. This model simulates losses due
to reflection and refraction of the wireless signal, due to obstacles and movement in the
networks. The shadowing propagation model uses a random variable with a log normal
distribution to simulate losses. This variable is combined with the functions in the Two
Ray Ground model to determine whether a packet is captured or lost. The overall model is
represented as:

\[
P_r(d) = \frac{P_r(d_0)}{d_0} - 10\beta \log \left( \frac{d}{d_0} \right) + X_{dB}
\]

In this model, the power received at some distance \(d\) is denoted as \(P_r\), and \(X_{dB}\) is a Gaus-
sian random variable representing the shadowing deviation. \(d_0\) is a reference distance that
is a function of antenna height. \(\beta\) represents the ideal path loss exponent, which varies
depending on the network environment (such as indoor, outdoor, and obstructed).

It should be noted that this is only a statistical model and is limited in that it does
not capture time correlation aspects of the signal power (it assumes that signal power is
independent from previous values of the signal). Aspects of operation that are sensitive to
time correlation would benefit from an even more realistic model that implements time-
correlation artifacts such as block fading. Since the signal fading model is idealistic, more
research is being done to define more realistic propagation models.

2.2 Medium Access Control

The IEEE 802.11 WLAN MAC/PHY specification [20] is a recommended international
standard used in MANETs. This standard contains implementation details for the MAC and
Physical (PHY) layer used in communications in a Wireless Local Area Network (WLAN).

MAC is the distributed protocol used to manage access to a shared communication
medium. The properties of the physical wireless channel pose significant challenges to
MAC design. Even under idealized channel assumptions, significant challenges exist. Due
to the fast attenuation of signal power, the state of the channel at the receiver is different from that at the sender – this makes techniques such Carrier Sense Multiple Access inaccurate and give rise to the known hidden and exposed terminal problems. For the same reason, Collision Detection is difficult. The MAC layer provides a number of services, including collision avoidance and fairness for nodes in the network.

The MAC protocol uses a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism. This mechanism requires nodes that wish to transmit data to sense the wireless medium, in order to ensure that it is not in use. Once it is determined that the medium is idle, nodes delay sending their transmissions with a random backoff, in order to avoid collisions that would result if all nodes transmitted at the same time. Note that the carrier sense is done at the sender to estimate the state of the channel at the receiver; it is possible that the channel appears idle at the sender but is not at the receiver (hidden terminal), or vice versa (exposed terminal).

To augment the carrier sense, when sending a packet, a node can optionally send a Request To Send (RTS) packet in advance. Nodes that observe the RTS packet should cease transmissions for the duration specified in the RTS packet, which is about the amount of time needed to fully transmit the packet. The destination node, upon hearing a RTS packet, responds with a Clear To Send (CTS) packet, indicating to the source node that it is ready to receive a packet transmission. Once the destination node receives a data packet, it responds with an acknowledgement (ACK) packet, indicating a successful packet transmission. An advantage of using these short control packets for arbitrating access is that collisions on them are not costly (in light of the difficulty in detecting collisions, this is an important factor).

Two communication functions exist in the 802.11 standard for unicast transmissions: the Point Coordination Function (PCF) and the Distributed Coordination Function (DCF). The PCF approach uses a polling technique by base stations to ask network nodes for traffic
that is waiting to be sent. The DCF mechanism lets nodes compete for use of the wireless channel. As MANETs are a group of nodes without a fixed infrastructure, the DCF mode is used for communications. In fact, the trend has been to use DCF almost exclusively even for last hop networks.

A node in a MANET is typically equipped with an omni-directional antenna. This antenna provides a nominally uniform transmission range in a circular area around the node, with the node at the origin of the circle. In practice, this assumption does not hold due to antenna lobe coverage patterns, and signal propagation and interaction with the surrounding environment. The transmission range is the area around the node where a packet can be successfully received. The wireless radios of the nodes can sense an area typically twice the size of the transmission range in what is known as the interference range, as shown in Figure 2.1. A node that is receiving a packet may be unable to capture the inbound packet if a nearby unrelated node is transmitting. This range is referred to as the interference range. There is also a carrier sense range around the node. This range is determined by antenna sensitivity, and a node only starts transmission when it determines the wireless medium is free.

![Figure 2.1: Transmission with Omni-Directional Antenna](image-url)
To improve reliability in the face of losses, MAC protocols like IEEE 802.11 [20, 21] use two mechanisms: (1) Collision Avoidance (CA): the nodes exchange small handshaking packets, the well known RTS/CTS/DATA/ACK exchange [22], to attempt to acquire the channel and block hidden terminals from interfering. Unfortunately, this mechanism is of limited success because it only blocks nodes in the reception range, but not those in the much larger interference range; and (2) Carrier Sense (CS): carrier sense is conducted aggressively, with a very low power threshold, enabling the sender to detect transmissions that are more than twice its range away. While this reduces the effect of the hidden terminal problem, it significantly increases the exposed terminal problem.

### 2.2.1 Node Interactions

A hidden terminal is an interfering node out of reception range of the sender, but in interference range with the receiver; such a transmission is not detected by the sender (it is hidden to it), causing a potential collision at the receiver. This can be seen in Figure 2.2. If node C is sending a packet to node B, node A can not detect this. Node A may transmit during node C’s transmission, resulting in a collision at node B.

![Figure 2.2: The Hidden Terminal Problem](image)

![Figure 2.3: The Exposed Terminal Problem](image)

An exposed terminal is a node that is forced to delay transmission due to another transmission nearby. The exposed terminal senses that a transmission is occurring; however the receiving node of this transmission is outside its transmission range. Since the exposed terminal backs off, it results in underutilization of the wireless channel. This can be seen in
Figure 2.3. Node B may wish to send a packet to node C. However, node B can sense that node A is transmitting, and does not send its packet, even though a collision will not occur at node C.

Situations arise where two nodes (A and B) are transmitting within collision range of a third node (C). In these cases, if the packet sent from A and the packet sent from B have similar signal power, node C will not be able to differentiate the two packets, and both will be marked as a collision and dropped. However, if one of the two packets has a signal power significantly higher than the other packet, node C will receive the stronger packet, regardless of whether it arrives slightly before or after the weaker one [23]. This situation is often referred to as a capture scenario, where C was able to capture one of the packets, due to its relatively higher power.

Despite CA and CSMA, not all collisions are prevented [24]. Neither approach can prevent all collisions. CA is limited to nodes in reception range (a subset of possible hidden terminals), while CS, which is applied at the sender, can not accurately detect the state of the channel at the receiver. Furthermore, collisions resulting from concurrent transmissions while the medium is idle can not be easily prevented. As an attempt to improve reliability, unicast MAC packets are retransmitted if the full packet exchange is not completed successfully. Up to 7 retries are attempted before the sender notifies the upper network layers of a failure.

Because of the broadcast nature of the channel when using omni-directional antennas, it is possible to support efficient link level broadcast. No handshaking is done in a broadcast, and only one attempt is made. While broadcasting allows a node to reach many other nodes at a minimal cost, it is an unreliable communication mechanism. Consequently, in order for a broadcast message to be heard by all of the nodes, multiple attempts may have to be made. When this is used in an application such as finding routing information, it introduces a large amount of latency.
A MAC level broadcast relies only on carrier sense to try and mitigate collisions. It does not use CA because that requires a single receiver that acts as a partner in the RTS/CTS/DATA/ACK exchange; CA cannot be applied to broadcast where multiple nodes concurrently receive a packet. In fact, it is possible for the broadcast packet to be received correctly at some nodes and not at others.

2.3 Routing

A MANET has no fixed infrastructure, hence the term ‘ad hoc’. There is no central authority responsible for keeping track of needed data, such as node locations. Further, the network does not have an address hierarchy or fixed network locations as is the case with traditional routing protocols. Routing is further complicated with mobility, which necessitates tracking topology changes at fairly small time scales.

To determine the path from one node to another in a MANET, routing protocols are used. These protocols allow the nodes to cooperate with each other in order to provide connectivity throughout the network via different paths. The paths used are often a chain of multiple nodes, in what is known as a multi-hop path. In order for data to flow between the two nodes, not only does the path have to be viable physically, but all nodes along the path must know their neighboring nodes. Each link in the path may vary in quality, due to distance between the nodes, the amount of traffic in the network, and the amount of energy being used for packet transmissions. Furthermore, each node in a path may move out of range from each other, depending on the mobility pattern that is present in the network. For instance, if the nodes are travelling along a freeway, it is likely that they will stay near each other for a long period of time. However, if the nodes are moving about randomly, the length of time that the nodes will stay in range is often below 100 seconds [25]. Other work has shown that as the chance of link failures increase, the chance of overall path
failure increases as well [26].

2.3.1 Routing Protocols

Traditionally, the routing protocols are categorized as either proactive or reactive (on demand) routing protocols. The former protocols attempt to keep up to date data on the network, while the latter protocols only gather data when needed. It is this data that is needed in order to repair a the path. When the nodes in a path move out of range, a link is broken and an alternative path must be found. Similarly, when new links appear, they may be used to create more efficient routes between nodes. The routing protocols differ in how they track such changes.

Ideally, a routing protocol should have a low overhead (in terms of the number of packets sent, as well as the energy used), but return optimal routes (in terms of the quality and stability of the routes, and perhaps the number of routes discovered). Furthermore, the protocol should scale from sparse networks to dense networks, and be able to recover from failed paths quickly.

Proactive protocols maintain tables that track routing information for the full network continuously; they are similar to traditional Internet routing protocols. If topographic changes are detected, updates are propagated throughout the network. As a result, they have substantial overhead. An example of a proactive protocol is the Destination Sequenced Distance Vector (DSDV) [27] protocol.

In contrast, reactive protocols invest in routing only when a path to a destination is needed. When a packet is generated to an unknown destination, a path discovery phase is initiated. This approach introduces a delay when an application wishes to send data, as the path information must be obtained, but cuts down on the amount of constant overhead in the network that is present with proactive protocols.

In a typical reactive protocol, when a path needs to be found, a Network-Wide Broad-
cast (NWB) is sent throughout the network. These NWBs are traditionally implemented via flooding, a process in which a node that receives a packet that was sent via a MAC layer broadcast resends that packet, also using MAC layer broadcasts. This allows the data packet to be propagated throughout the network. Since MAC layer broadcasts are used, there is no overhead or latency present that is typically associated with unicast transmission. As a result, losses due to congestion, collisions, or propagation errors result in the NWB potentially not reaching portions of the network and not discovering available paths. Consequently, the route search must be performed again at a great cost, and after a significant backoff delay, in order to collect the appropriate path information.

The Dynamic Source Routing (DSR) protocol [28] is an example of a reactive protocol. Each packet sent contains the full routing information for the packet. Conversely, the Ad hoc On-Demand Distance Vector Routing Protocol (AODV) [29] contains only next-hop information for the packet being sent. Each node in the network using AODV contains tables with data on which node is the next hop in order to reach a node. Both protocols rely on flooding with MAC broadcasts to obtain path information.
Chapter 3

Literature Review

This chapter describes important work in Mobile Ad hoc Networks (MANETs) that is related to robust operation. First, Network Wide Broadcasts (NWB) are examined, and areas for potential losses are explained. Existing solutions, both in the Medium Access Control (MAC) layer and in the network layer are reviewed. Since broadcasts are used in routing and multicast operations, any loss of these packets results in overall degradation for a flow or series of flows in the network. The existing MAC layer solutions have a high cost to implement, and are not fully optimized. The existing network layer solutions work on cutting down the number of broadcasts, resulting in lower redundancy, but also expose a higher chance of overall failure if a critical broadcast is lost.

MAC fairness is then reviewed. If the MAC layer is unfair, one or more flows in a network may suffer, as they are not granted fair access to the wireless medium. If fair access is not granted throughout the network, overall robustness throughout the network can not be achieved. Most existing fairness algorithms create fairness by cutting down overall throughput. Since less traffic exists in the network, there is less chance for losses due to collisions and congestion. These solutions are not ideal, because the overall throughput is lowered, resulting in less of the network capacity being used.
Issues of channel capacity are examined next. The overall network capacity must be understood in order to decide whether or not multiple high load flows can be effectively supported in a MANET. Lastly, existing Quality of Service (QoS) schemes are reviewed. These are network wide approaches to sharing the wireless medium among many nodes and many traffic types. They represent a complimentary approach to contention based approaches that attempt to support fairness after the fact. These solutions often require substantial changes to the MAC protocol. A guaranteed level of QoS is difficult to achieve in a MANET due to its dynamic nature.

3.1 Overview and Classification of NWB Algorithms

In this section, NWB approaches are overviewed and classified with an emphasis on robustness. The primary characteristics of interest are: (1) overhead; (2) resilience to mobility; and (3) robustness to losses.

3.1.1 Topology-Independent (Flooding) Approaches

Flooding is a brute force approach that has high overhead, especially in dense networks [30]. Most NWB algorithms target this problem. Because no topology knowledge is needed, these algorithms are resilient to mobility and do not require an on-going overhead to discover neighbors/topology. Flooding is thought to be resilient to MAC losses due to the high redundancy generally present. However, this may not be true: in low density areas of networks, the available redundancy is low. Moreover, the amount of available redundancy is fixed – it may be too high for some cases and too low for others.

One approach to reducing overhead is to have nodes determine locally whether their
rebroadcast is likely to be redundant. Ni et al [30] suggest several criteria for deciding whether to rebroadcast, including: (1) probabilistically; (2) based on the number of rebroadcasts already heard (if several were heard, an additional one is probably not needed); or (3) based on the distance or location of the nearest heard rebroadcast (if it is too close, it is likely that little additional coverage is obtained from another broadcast). These approaches reduce the overhead without appreciably harming coverage. Like flooding, they are resilient to mobility. Because each node locally determines whether its rebroadcast is likely to be needed, the approach dynamically adapts to transmission losses.

Haas, et al., propose [31] gossiping, where each node forwards a packet based on some probability $p$. The main concept is that in large networks, many broadcasts are redundant, and by dropping a small percentage of them, no coverage is lost. This approach exhibits a bimodal behavior in that their goal is achieved some times, but in other networks, the broadcast dies out quickly, as one of the first nodes, or a node along a critical path, opts not to rebroadcast the packet.

3.1.2 Topology Sensitive Approaches

Topology-sensitive protocols explore alternative broadcasting approaches that attempt to proactively construct a “virtual backbone” that can be used to optimize NWBs. Under these protocols, only backbone nodes rebroadcast NWB packets. Under ideal assumptions, all the nodes can be covered with an asymptotically optimal overhead; they have been proposed to replace flooding in routing algorithms [32, 33]. A popular approach is using a Connected-Dominating Set (CDS) – a connected subset of the nodes from which all other nodes are one-hop reachable. If the CDS nodes broadcast, all the nodes in the network are covered. While finding the optimal CDS is NP-complete, algorithms have been developed to construct them distributedly, and near-optimally in terms of the size of the CDS and the
overhead to construct it (e.g., [34, 35]).

In order to build a virtual backbone, nodes exchange information about neighbors; this is an ongoing process. As a result, topology sensitive approaches degrade (in terms of overhead and/or coverage) with increasing mobility since the neighborhood information becomes stale more quickly.

One of the most basic topology-sensitive algorithms is known as Flooding with Self Pruning [36]. A node keeps track of all of its one-hop neighbors, which is obtained through periodic ‘HELLO’ broadcasts. When broadcasting, a node includes its list of neighbors in the sent packet. A node receiving this packet examines the incoming neighbor list against its own. If no new nodes would be covered by a rebroadcast, the packet is not resent. This algorithm is beneficial in some scenarios, but is inefficient in others.

The Dominant Pruning algorithm uses 2-hop neighbor knowledge for routing decisions [36]. When broadcasting, a node proactively chooses some of its 1-hop neighbors as rebroadcasting nodes. Only those nodes may rebroadcast the packet. When one of these nodes receives the broadcast data, it uses a Greedy Set Cover algorithm [37] to determine which neighboring nodes should rebroadcast. This algorithm for neighbor selection is not as efficient as other algorithms.

Another example of a topology sensitive approach is the Optimized Link State Routing (OLSR) protocol. This protocol preselects a set of multi-point relays that forward flood information to cut down on overhead [32]. In the Ad Hoc Broadcast Protocol (AHBP) [38], nodes track two hop neighbor information and use this information to explicitly select a set of 1-hop neighbors to rebroadcast the packet such that all the 2-hop neighbors are covered. Pagani and Rossi proposed a protocol for reliable broadcast that builds a hierarchical cluster backbone and reliably unicasts messages to cluster heads for delivery to leaf nodes [39]. Maintaining the underlying cluster and tree structure is impractical in dynamic networks.

In terms of vulnerability to losses, an important distinction between topology sensitive
approaches is whether the forwarding responsibilities are statically or dynamically determined. In static approaches, the topology information is used to determine forwarding responsibilities. Static approaches allow more optimized forwarding, however, this approach becomes especially vulnerable to losses: if a loss of a packet to a node with forwarding responsibilities occurs, the remainder of the backbone reachable through it and the nodes they cover will not receive the NWB.

In dynamic approaches [36, 40], each node locally determines whether it needs to be part of the CDS based on already heard transmissions. For example, in the Scalable Broadcast Algorithm (SBA) [40], each node tracks its two hop neighbors. This enables a node A to determine which of its neighbors a node B are covered by previous retransmissions by checking the two hop neighbor information without requiring B to transmit its neighbor list. The dynamic localized decisions makes this class of algorithms significantly more resilient to losses; however, lacking a central view, they generally do not use to the most efficient CDS, even when no losses occur.

The Lightweight and Efficient Network-Wide Broadcast (LENWB) protocol [41] also uses 2-hop neighbor knowledge. Each node decides to rebroadcast based on its knowledge of its neighbors and the likelihood of those neighbors to rebroadcast. Each node is assigned a priority, based on the number of neighbors the node has. Nodes that are more strongly connected have a high priority and are expected to broadcast. However, the authors of this protocol show that this protocol performs poorly in conditions that are common to MANETs.

### 3.2 MAC Level Solutions to NWB Robustness

Since MAC broadcast is at the root of NWB robustness issues, improving its reliability benefits all NWB algorithms that use it. There have been multiple solutions proposed for
modification at the MAC level in order to increase MAC broadcast reliability; these are reviewed in this section.

Tang and Gerla proposed a MAC protocol where a broadcast is acknowledged by all receivers [42]. They assumed any noise heard on the channel during the expected acknowledgement timeframe was due to a collision. If a single acknowledgement or noise (multiple acknowledgements) are received, the broadcast is considered successful, otherwise it is retransmitted. Thus, this approach leads to at least one of the neighbors receiving the broadcast correctly. It is not clear how accurate the assumption regarding noise on the channel during the expected acknowledge period is with other traffic in the network. Furthermore, while this approach does guarantee that at least one node received the broadcast, it does so at the expense of generating an acknowledgement from all receiving neighbors. This overhead increases self-interference and contention of a network, if it is already under high load.

Chaporkar et al. propose a MAC level mechanism that uses dual channels [43]. In this scheme, a broadcast sender sends an RTS on the message channel. Receivers that are ready respond with a CTS on a busy tone channel. The sender estimates the number of ready receivers by measuring the power on the busy tone channel. In addition to requiring significant changes to the MAC protocol (a separate busy tone channel), this approach presumes complete knowledge of neighbors location in order to estimate their busy tone power. Furthermore, if the difference in distances between neighbors is large, the differences in power (which drops exponentially) makes far nodes indistinguishable from shadowing and other power fluctuations. The authors propose an alternative MAC implementation in another work, but that also requires substantial changes to the MAC layer and is quite complex [44].

Similarly, Park et al. propose a solution for use in sensor networks that guarantees the delivery of a packet [45]. In this scheme, when a node has a packet to send reliably, it emits a series of pulses with unique periods and amplitudes that receiving nodes can detect even
while they are transmitting. After a short period of time, the data packet is sent. Nodes that did not receive the packet are aware that one was sent out, due to the pulses, and can perform requests for retransmission. This approach also requires substantial changes in the MAC layer, including an additional channel for the pulses. Furthermore, this solution makes assumptions suitable for a sensor network environment relative to a single sender, however these assumptions make it unsuitable for general ad hoc operation.

Goassain et al. [46] propose a MAC extension to allow support for reliable multicast. When a node wishes to broadcast a multicast packet, the data packet is augmented with a list of nodes that are to ACK the received packet. The MAC duration field is increased to allow each listed in the DATA packet to send an ACK back to the sending node. To prevent ACK collisions, the nodes wait and send an ACK in a slot corresponding to their location in the node list in the packet. If an ACK is not received, it can be because the node did not receive the packet because of a collision or because it moved out of range. The sending node will then send out a Multicast RTS packet (MRTS), to which each node listed in the packet would send a CTS back to the source. While this approach is thorough, it does increase latency in the network. Waiting for an ACK from all nodes that are part of the multicast group prevents other data from being sent. Their results support this fact; coverage goes up, but the average delay does as well.

In the context of last-hop wireless networks, the problem of reliable broadcast from the basestation to the hosts it is managing has been observed and studied. This is a much simpler setting than a multihop ad hoc network because there is one predetermined source and everything occurs in a single cell without concern to interference with other nodes. Kuri and Kasera propose a leader election MAC level mechanism similar to directed broadcast for use in last hop networks [47]. The receiving nodes that are a member of a multicast group elect a leader responsible for responding to the basestation’s broadcast. The leader responds if it receives the broadcast correctly. Other nodes that do not receive the broadcast
can send a Negative Acknowledgement (NACK) packet that collides with the ACK, invalidating it. Thus, a packet should be retransmitted if any of the receivers does not receive it. While this approach avoids receiver collision problems by having a single responder, it makes many assumptions that are unsuitable for a MANET environment. Furthermore, it does not give the flexibility of choosing the receiver to the sender. Although this mechanism is similar to directed broadcast in that it requires only a single node to respond solving the handshake collision problem, it makes many assumptions that do not hold in ad hoc environments.

Bharghavan [48] proposes the idea of a token-based scheme for multicast access to the MAC in wireless LANs. In this scheme, the base station of the wireless LAN passes tokens to neighboring nodes. When the base stations wishes to multicast, it does not send out tokens for acquiring access to the channel. This scheme is not entirely applicable in a MANET, since all nodes in a MANET contend for the channel. This token passing scheme also only deals with obtaining the wireless channel, but does not address its use afterwards.

Garcia and Zhang propose [49] a flooding based reliable broadcast protocol that allowed nodes to forward the broadcast packet without further notice from the sender. Alagar and Venkatesan also propose a flooding-based reliable broadcast protocol [50]. This protocol requires nodes that receive a flooded message to respond with an ACK if it is a new message. This leads to an ACK explosion problem in conjunction with the broadcast storm problem.

A drawback of all MAC based approaches is the high deployment barrier associated with modifications to the MAC layer. For deployment, it requires a change to the MAC standard, as well as all wireless cards, resulting in a high barrier to cross for adoption. However, the modifications required by the approaches presented in this work require no additional physical capabilities or resources.

Other MAC solutions exist to increase NWB robustness. Those will be reviewed in
Chapter 6, as they are most relevant to the work presented in this dissertation.

### 3.3 NWB Algorithms Targetting Robustness

Pagani et al. [39] and Lipman et al. [51] propose a fully reliable unicast-based NWB algorithm. These approaches have a much higher overhead than broadcast-based approaches. Due to the broadcast storms present in a single flood, losses of broadcasted packets may occur. This situation becomes even worse if multiple NWBs are currently in progress within the network. Some solutions have been provided to schedule the broadcasts with a CDS approach in order to cut down on the amount of self-contention [34].

Lou and Wei recently identified the effect of transmission losses on CDS based approaches [52]. To counter that effect, they proposed a modified CDS algorithm, called Double Coverage Broadcast (DCB). DCB ensures that every node is covered twice (not just once as per the CDS requirement). While DCB is more resilient to the NWB unreliability problem than basic CDS algorithms, the set of forwarding nodes is statically determined, and therefore, the approach remains vulnerable to losses. However, upon detecting a loss, there are 3 algorithms that can be used to recalculate the set of neighboring nodes, providing a more dynamic and resilient NWB approach. Their work is different to the ideas presented in this dissertation since they try to cover each node twice, resulting in more traffic in the MANET. The approach presented by this dissertation uses an additional broadcast selectively, resulting in double coverage only when necessary.

Hyper-flooding [53] is used in MANETs with high levels of mobility, where reliability is needed. Each node in the network broadcasts at least once. Periodically, nodes exchange ‘HELLO’ messages, in order to allow local neighbor node lists to be built. Upon packet reception, the packet is rebroadcasted and locally cached. If a ‘HELLO’ packet comes in from a new neighbor, the packet is rebroadcasted again, allowing the new node to receive
Table 3.1: Neighbor Knowledge NWB Approaches

<table>
<thead>
<tr>
<th>Approach</th>
<th>Protocols</th>
<th>Value</th>
<th>Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pruning</td>
<td>Flooding with Self Pruning</td>
<td>Simple implementation</td>
<td>Not always beneficial</td>
</tr>
<tr>
<td></td>
<td>Dominant Pruning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clustering</td>
<td>Cluster-based backbones</td>
<td>Lowers overhead</td>
<td>Impractical to obtain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lowers redundancy</td>
<td>in dynamic MANETs</td>
</tr>
<tr>
<td>Static CDS</td>
<td>OLSR</td>
<td>Optimized forwarding</td>
<td>Losses due to outdated</td>
</tr>
<tr>
<td></td>
<td>AHBP</td>
<td></td>
<td>neighbor knowledge</td>
</tr>
<tr>
<td>Dynamic CDS</td>
<td>SBA</td>
<td>Higher forwarding costs</td>
<td>More resilient to losses</td>
</tr>
<tr>
<td></td>
<td>DCB</td>
<td></td>
<td>and mobility</td>
</tr>
<tr>
<td>Data Caching</td>
<td>Hyper-gossiping</td>
<td>Provides reliability</td>
<td>Requires storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in mobile scenarios</td>
<td>Adds to contention</td>
</tr>
</tbody>
</table>

Hyper-gossiping, proposed by Khelil [54], is an extension to hyper-flooding that uses gossiping instead of flooding, as described earlier. The combination attempts to increase reliability without increasing overhead in highly mobile scenarios. The criteria for retransmission here is not sensitive to losses; rather a fixed amount of redundancy is added probabilistically.

A summary of these approaches is presented in Table 3.1. A few key positive effects of each approach is listed, as well as a few drawbacks of each approach.

### 3.4 MAC Fairness

The second problem targeted in this dissertation is understanding low-level interactions that cause unpredictable behavior in high load scenarios. In order to show that the observed effects are not due to the well-known fairness issues in MANETs, and to understand the relationship between the two, this section reviews work that examined MAC fairness.

A flow of data in a MANET is said to be unfair when it is preventing another flow of data from achieving a similar rate of transfer. When fairness is studied, the data paths often
have the same number of hops, and the same potential data rate, however the two flows do not behave similarly.

The unpredictable behavior of MANETs has been studied by many. Xu and Saadawi discuss [8] how the 802.11 MAC layer causes problems with TCP in MANETs by examining multiple connections in a string formation. They concluded that the MAC layer still has a hidden node problem, despite the attempts to deal with the issue, as well as the exposed node problem. They also state that the Binary Exponential Backoff (BEB) scheme used in 802.11 favors the last successful node, which leads to unfairness in the network.

Xu and Saadawi also did research regarding fairness issues in MANETs with the Transmission Control Protocol (TCP) [8] and multiple flows. Their first unfairness experiment, the “neighboring node one-hop fairness” issue focused on two TCP flows in a chain of nodes. One flow was started, and proceeded as normal. When the second flow was started, the first flow had no more progress for the remainder of the experiment. In their second unfairness experiment, the “TCP incompatibility problem”, they demonstrated that two flows with the same path length do not successfully send data packets at the same time. This experiment was again done with a chain of nodes.

There have been many studies done to attempt to achieve fairness in a MANET. Most approaches sacrifice throughput for a better level of fairness throughout the network. Multiple algorithms have been proposed for adjusting the Congestion Window (CW), in order to achieve a better sense of fairness. The Multiplicative Increase/Linear Decrease (MILD) scheme was proposed in [55]. In this scheme, the contention window was multiplied by 1.5 for each backoff, rather than doubling it as in the BEB scheme. When a packet is successfully transmitted, the CW is decreased by one, rather than resetting it. A value of the current CW is included in each RTS packet, so that nodes adjust their CW to the value of the sending node’s CW. This scheme has been shown to suffer when the CW value enters an area of the network with a different CW [56]. Other fairness algorithms have been
examined, but are beyond the scope of this research.

An extension to the MILD scheme, Linear/Multiplicative Increase and Linear Decrease (LMILD) has been proposed [57] to utilize overhead collisions at each node. This is done instead of copying the CW value sent in the MILD scheme. In the LMILD scheme, nodes that have colliding transmission increase their CW values multiplicatively, while nodes that only overheard the collision increase their CW values linearly. All nodes decrease their CW values linearly after a successfully sent transmission.

The Estimation Based Fairness Algorithm was proposed as an algorithm that has each node estimate its fair share of the network bandwidth. By observing the packets that are successfully received from the channel, a node can weight the data it must send against the data that other nodes are sending. The CW is adjusted according to the weight values in order to achieve a sense of fairness. A node that had more data to send than what it observed in the channel would have a smaller CW, as it would be weighted towards what it had to send.

Vaidya et al. proposed [58] the Distributed Fair Scheduling (DFS) protocol. This algorithm schedules packets to be sent such that the bandwidth required is proportional to the weight assigned for a given set of paths for packets to be sent on.

Other approaches include extreme MAC changes and hardware changes. For instance, Singh and Singh proposed [59] a slotted MAC approach with directional antennas to increase overall throughput.

3.5 Capacity

Work has been done to examine the capacity of wireless networks. The capacity of a MANET needs to be fully understood in order to quantify how many flows can exist in a network simultaneously as well as how much data can be sent on those flows.
Gupta and Kumar [60] derived a geometric formula giving the end-to-end throughput theoretically available to each node in a wireless network. This throughput is roughly $O\left(\frac{1}{\sqrt{n}}\right)$. Using a global scheduling scheme, they were able to obtain this throughput.

Li et al. [61] examine the interactions of the 802.11 MAC and packet forwarding on the overall capacity of a MANET. Chain configurations are studied in detail, and are shown to have a throughput of around $\frac{1}{7}$ of the channel capacity, compared to the ideal value of $\frac{1}{4}$ of the channel capacity. Their investigation notes that nodes early in the chain cause interference and send packets that will later be dropped, leading to starvation in the later nodes.

Holland and Vaidya examined TCP-Reno behavior for a single connection [62]. They derived a formula for expected throughput for a chain of nodes. The degradation of the throughput increased rapidly as the number of nodes increased, and stabilized as the number of nodes in the chain became larger. Gerla et al noted [63] that end to end throughput decays exponentially with the number of nodes in the path of a flow. It should be highlighted that all of these works deal with throughput for a single connection in a network, without taking into account other potential connections in the same region of the network.

Nandagopal et al. introduced [64] an algorithm which gives each flow in a MANET a fair allocation of capacity of the network. This allocation is given despite how much contention is observed within a flow and is proportional to the other flows in the network.

De Couto et al. [65] present evidence that many MANET protocols opt for using shortest path routes for transmissions, and do not take the quality of those routes into account. As a result, the shortest paths tend to be congested and of poorer quality, while a longer route with more capacity is available and unused.
3.6 Quality of Service

802.11 is designed for best-effort delivery of packets, making Quality of Service (QoS) demands for real-time applications difficult. QoS is a challenging task due to the dynamic nature of the network topology. Flows may break due to nodes moving out of range, causing delays while new paths are established. Furthermore, link states change continuously, effecting the overall state of the flow, making state metrics difficult to keep accurately. This results in inprecise metrics for measuring the quality of a flow. In addition, in a MANET, there is no central control, so nodes must interact with each other to balance and schedule the real-time flows. Lastly, there are limited resources available to each node in a MANET, including bandwidth and power. To combat these challenges, multiple approaches have been proposed, including bandwidth reservation, service differentiation, and link adaptation.

In service differentiation, one of two methods is traditionally followed. Either flow types are given a priority, allowing applications higher preference to the channel, or scheduling algorithms are introduced to allow traffic classes access to the channel in proportion to each other. In the 802.11e standard [20] Enhanced Distributed Coordination Function (EDCF) is introduced. It gives different traffic flows a different priority based on a number of parameters. Each traffic flow still uses the traditional DCF channel access method, but has a different chance of winning the channel contention based on the parameters.

In the Distributed Weighted Fair Queuing (DWFQ) model, proposed by Banchs and Perez [66], two different algorithms can be used. In one, the backoff window size can be adjusted based on the difference between the actual and expected throughputs. If the actual throughput is lower than the desired throughput, the backoff window is made smaller, in order to raise the priority of a flow. In the other algorithm, a ratio of actual throughput to weight of the node is computed for each node in a flow. By comparing the ratios, a node
can adjust its backoff window appropriately.

In the Distributed Deficit Round Robin (DDRR) scheme [67], each traffic class is given a priority, and counters are created representing each node and traffic class pairing. As packets are sent, the counters are decreased by the packet length, and the counters are incremented at the rate expected per traffic class. The counter is then inversely proportionate to the interframe space (IFS), which is the wait time before transmissions occur. A larger counter results in a smaller IFS, resulting in a better chance of obtaining access to the channel.

Service differentiation schemes are useful in that bandwidth is shared evenly among nodes and types of traffic. However, this fairness comes at the cost of substantial modifications to the existing 802.11 standards. Typically, scheduling algorithms require more modifications than priority-based mechanisms. Bandwidth reservation schemes are designed to perform better under high traffic loads. Li et al. [68], introduce such a framework which is designed to optimize the usage of high priority resources. Liu et al. [69] present a group of reservation-based MAC protocols with multi-channel support. These protocols use the RTS/CTS on the channel purely for reservation purposes. Once the channel is obtained, a station transmits uninterrupted in the reserved channel.

Since the 802.11 specification leaves the rate adaptation open, potential exists to modify the link adaptation mechanism in order to increase the throughput when the channel is changing dynamically. Many link adaptation models use existing information contained in the Physical Layer Convergence Protocol (PLCP) header, resulting in not having to modify existing standards. Pavon and Choi [70] use the received signal strength (RSS) as a metric, assuming that the transmission power is fixed. A linear relationship is assumed between the average RSS and Signal to Noise Ratio (SNR). Their algorithm maintains 12 RSS thresholds, and dynamically changes the transmission rate accordingly. Lampe et al. [71] keep track of the packet error rate (PER). Depending on the PER, the transfer rate is adjusted.
In addition to true QoS models, “soft” QoS models have been proposed. These models facilitate “soft” real-time traffic, where a best effort is made to send real-time traffic. However, due to mobility issues or congestion overload at wireless relay points, QoS is not guaranteed. One example of this is the Service Differentiation for Real-Time and Best Effort Traffic in Stateless Wireless Ad Hoc Networks (SWAN) model, proposed by Ahn et al. [72]. SWAN, limits the potential drops more than standard MANET protocols, while still using best effort MAC technology, rather than requiring a QoS dedicated MAC.

The Insignia model [73], designed explicitly for MANETs, is useful for multimedia applications, where some loss is acceptable. With Insignia, any MAC protocol can be used, and any routing protocol can be used, however route maintenance mechanisms will affect the QoS. In-band signalling is used, meaning messages for reserving and releasing resources are sent with the traffic, resulting in lower overhead. Packets are scheduled with a weighted round robin approach for different flows. Since the MAC and routing protocols are up to the network, absolute QoS is not guaranteed.

### 3.7 Summary

This chapter reviewed some of the key areas in MANET research that relate to the work in this dissertation. While much work is being done on minimizing NWB overhead, very little emphasis is being placed on NWB robustness. As a result, when key broadcasts are lost, the NWB can become completely useless. This phenomenon will be discussed in Chapter 5. This section classified NWB algorithms, and reviewed works that targets improving robustness. In Chapter 6 a finer classification of the solution space is undertaken and existing solutions are classified relative to that space.

Also presented in this chapter was research done on MAC level fairness and capacity. These studies focus mainly on short-term unfairness, and do not analyze fairness issues
that arise over a long period of time. The problem of long term unfairness due to low-level interactions among links is examined in Chapter 10.
Chapter 4

Motivating Scenario and Problem Identification

The behavior of MANETs, under high load and in lossy environments, is unpredictable and poorly understood. Most existing work in characterizing MANET performance focuses on single connections, and does not address general scenarios. With non-linear interference and complex interactions between multiple protocol layers, the behavior is extremely difficult to quantify and understand. In this chapter, representative scenarios of Mobile Ad hoc Network (MANET) operation under high load are analyzed to show examples of the observed behavior. Analysis of these scenarios is used to motivate the need for Network Wide Broadcast (NWB) robustness. Further, the scenarios demonstrate the need for a better understanding of the low level interactions that arise between contending transmissions with different interference relationships with each other. This evidence to motivate the research conducted in the remainder of this dissertation.
4.1 Analysis of a Representative Scenario

All experiments use the Network Simulator NS-2 [74], a discrete event simulator with detailed packet-level models of networking protocols. NS-2 incorporates models for wireless propagation and the IEEE 802.11 protocol. In all scenarios, nodes are randomly deployed in a fixed area of 1000 by 1000 meters. The 802.11 Medium Access Control (MAC) implementation in NS-2 was used for experimentation with default parameters that represent a WaveLAN wireless card. The idealized two-ray ground propagation model was used with a transmission range of 250 meters. After a detailed study of many scenarios, the problems discussed in this chapter were isolated. For purposes of illustration a representative scenario is analyzed in detail; the behavior in this scenario is typical of observed behavior arising frequently in most scenarios that were studied.

![Figure 4.1: Three Competing FTP Connections](image)

As described in Chapter 3, the expected throughput of a connection decreases as the number of hops in the connection increases. In a scenario with 3 connections, one being 1 hop long, one being 3 hops long, and one being 5 hops long, the natural expectation would be for the throughput to be inversely proportional to the hop count; this effect is the expected behavior of a chain connection with no outside interference [62, 63]. However, the observed behavior shows that the effect of interference can be counterintuitive and unexpected.
An example of a high load MANET behaving in an undesirable manner can be seen in Figure 4.1, where 3 competing File Transfer Protocol (FTP) connections distributed randomly in a random topology are all active simultaneously. Each connection will attempt to grow its sending rate per Transmission Control Protocol’s (TCP’s) congestion management algorithm [75, 76]. It can be seen that two connections (connections 1 and 2) are not achieving a high transfer rate and are completely idle for long periods of time. The third connection achieves a high throughput, and its progress is not fully charted in order to provide graph clarity. The scenario is illustrated in Figure 4.2.

To better understand why the starvation is occurring, deeper analysis of the simulation traces is necessary. Connection 1 has a length of 3 hops, Connection 2 has a length of 5 hops, and Connection 3 has a length of 1 hop. While the shortest path correlates strongly with the overall scenario throughputs [61, 62], it does not explain the behavior entirely. As was explained in Chapter 3, the capacity of a connection drops with the number of hops because of their self interference. However, the first connection only manages to send a few packets, while the second connection sends far more, despite being two hops longer. In high load environments, we also expect unfairness issues to arise because each hop contends independently for bandwidth making it more difficult to deliver packets across
Connections with more hops.

Connections 1 and 2 had very little progress for the first 200 seconds, and only marginal progress later in the simulation. Ideally, it would have forward progress consistently, with no extended “dead times”, where the FTP connection was not transferring data successfully.

Further study of this scenario indicates that there were 8 “no route available” errors. These errors indicate that packets were dropped because the routing agent did not know about any route. Since packets were previously sent on routes between nodes, these failures indicate that the routes failed due to congestion (many MANET protocols assume that failure to deliver packets at the MAC level after all the retransmission retries is an indicator of mobility; this has been shown to be problematic under heavy load situations [8]) or mobility, and that new routes were unable to be established within the required time for the routing protocol. The scenario being examined is a static scenario, so no routing losses are due to mobility. The first connection sent out 140 route requests from the source node, the second connection sent out 172 route requests from the source node, and the third connection sent out 3 route requests from the source node.

The observed unpredictable behavior can be caused by the following factors:

1. TCP reaction to dropped packets: When packet loss occurs due to congestion, TCP invokes congestion management algorithms. This results in reducing the congestion window (sending rate) and doubling the retransmission backoff. These effects can lead to temporary idle times on connections (for example, waiting for a backed off retransmission timer to expire).

As described earlier in Chapter 3, Xu and Saadawi researched TCP issues in MANETs [8]. The scenario described above indicates there are additional issues than what they present. Since the idle times in the FTP scenario presented above are temporary, it differs from the “neighboring node one-hop fairness” issue characterized by Xu and Saadawi.
To eliminate all side-effects of TCP, Constant Bit Rate (CBR) connections were used to generate traffic, with a transfer rate of one packet every millisecond. Although this transfer rate is unachievable in real world applications, it does ensure the network is saturated and under high load. The same network topography as the FTP connections was used, with connection lengths of 3, 5, and 1 for each of the three connections. In the 3 connection scenario, 1668, 10036, and 19470 packets were sent over the three connections, as can be seen in Figure 4.3. In the 2 connection scenario, 3286 and 17142 packets were sent by the connections, shown in Figure 4.4. As expected, the 1 hop connection had little trouble. However, removing it did not increase throughput substantially for the other two connections. More importantly, the 5 hop connection again fared better than the 3 hop connection, both with and without the 1 hop connection.
connection being active. Since the CBR scenarios performed similarly to the FTP scenarios, in that the 5 hop connection had a higher throughput than the 3 hop connection, TCP is not the sole cause of the issues being seen by the FTP applications. Some “dead times” still exist in the network, where the number of CBR packets sent on a connection does not increase for an extended period of time.

2. Route search failures: The route request operation did not succeed, resulting in failure to find paths. While no path to the destination is known, packets cannot be delivered. The route request search is typically implemented using a network wide broadcast operation. The NWB operation is often optimized, most often using replies from caches (although these are of questionable value [77, 78, 79, 80]). Other route search optimizations include query scope limitation [81, 82]. NWB relies on MAC level broadcast operations which are unreliable.

As shown in Table 4.1, there were 315 route requests within the scenario for the 3 FTP connections. Since the simulation was 500 seconds long, a route request was sent out every 1.5 seconds, on average. Of those, 186 were unsuccessful in returning a single route. This means that 59% of the route requests were wasted. Consistent with that, there were 938 MAC layer broadcasts related to routing that were dropped due to collisions.

Moreover, optimizations to NWB that attempt to reduce its overhead, harm its robustness. Improving the robustness of NWB is a major component of the research in this dissertation. In addition to benefitting route request searches, improving the robustness of NWB is beneficial for other algorithms that rely on NWB such as Multicast [83, 84] and Geocast [85, 86].

3. Congestion: Many packets are dropped due to failed retransmissions. Recall from Chapter 2 that a packet retransmission failure (after multiple retries) at the MAC level
<table>
<thead>
<tr>
<th>Flow</th>
<th>RREQ Sent</th>
<th>RREQ Unanswered</th>
<th>Percentage Lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP3 Conn. 1</td>
<td>140</td>
<td>96</td>
<td>68.6%</td>
</tr>
<tr>
<td>FTP3 Conn. 2</td>
<td>172</td>
<td>90</td>
<td>52.3%</td>
</tr>
<tr>
<td>FTP3 Conn. 3</td>
<td>3</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>CBR2 Conn. 1</td>
<td>753</td>
<td>154</td>
<td>20.5%</td>
</tr>
<tr>
<td>CBR2 Conn. 2</td>
<td>159</td>
<td>29</td>
<td>18.2%</td>
</tr>
<tr>
<td>CBR3 Conn. 1</td>
<td>1027</td>
<td>344</td>
<td>33.5%</td>
</tr>
<tr>
<td>CBR3 Conn. 2</td>
<td>310</td>
<td>68</td>
<td>21.9%</td>
</tr>
<tr>
<td>CBR3 Conn. 3</td>
<td>167</td>
<td>31</td>
<td>18.6%</td>
</tr>
</tbody>
</table>

Table 4.1: RREQ Failures

is used to trigger route failure in many routing protocols. Retransmission failure is used as indication of node mobility. However, under high load, retransmission failures can occur due to consecutive collisions. Moreover, in lossy environments, retransmission failure can occur due to signal fading as well. To address this effect, more effective congestion management techniques are needed. In addition, under heavy load, more effective discrimination of mobility losses from congestion/fading losses are needed.

In order to discard traditional unfairness problems as a reason for the surprising behavior of the above scenarios, the 2 connection CBR scenario was run again with the Multiplicative Increase/Linear Decrease (MILD) algorithm [57]. This algorithm sacrifices throughput in the network in order to achieve fairness. As depicted in Figure 4.5, the longer 5 hop connection did better than the 3 hop connection. With an overall sacrifice in throughput, the level of congestion present in the network is decreased significantly. Even with low congestion, a well-known fairness algorithm, and no side effects from TCP, the longer connection does better than the shorter one.

4. Persistent unfairness due to asymmetric interference patterns: Unfairness is due to the nodes’ geographical location to each other, making one connection dominate, and no packets (routing or data) can get through for the other.
As described earlier in Chapter 3, the throughput of a connection is expected to decrease as the number of hops in the connection increases. This previous research makes the results obtained here seem counter-intuitive, as the longer connection of 5 hops achieves better throughput than the shorter connection of 3 hops. In addition to this, existing research does not explain why having 3 CBR connections yields more data packets sent successfully than only having 2 CBR connections (31174 packets compared to 20428 packets, a difference of 8274 packets).

The remainder of this chapter focuses on the effect of the two major problems addressed in this research.

### 4.2 Problem Statement

It can be seen that MANETs are not robust under high loads. In this work, two contributing factors to this problem are identified: (1) NWB robustness, and (2) unexpected unfairness that arises in a manner that is sensitive to the interference relationship of the nodes to each other. The first effect was observed independently by other researchers but not studied in detail [52]; furthermore, the solutions investigated here differ significantly from theirs. The second effect has not been identified by other researchers. It should be noted that there are other contributing factors as to why MANETs do not function well under high loads, but the isolated problems are important and represent an essential component of an overall understanding and solution to the problem. In response to the above problems, the following solutions are undertaken:

1. Network-Wide Broadcast Robustness: In a MANET, the ability to send an NWB is crucial to the operation of critical services such as routing. Fundamentally, the lack of structure in MANETs as nodes move requires mechanisms that can disseminate information without relying on a routing structure (e.g., for routing itself, when the
structure is unknown or invalid). NWBs fill this void, by allowing all nodes to be reached in a way that is resilient to mobility and stale/invalid routing information. To work effectively, an NWB should reach a large percentage of the nodes in the network at an acceptable overhead. Since NWBs are typically done with unreliable communications, this is a difficult problem. NWBs are used in routing algorithms, in order to find paths to nodes for unicast transmissions. They are also used heavily in many group communication algorithms, in order to pass data from one node to many nodes in the network.

Most NWB research focuses on reducing the overhead needed to cover all the nodes under idealized and low load assumptions. In contrast, this work focuses on increasing robustness under high load. In the solution space for NWB robustness, there are many approaches for solutions. Implicit feedback solutions attempt to predict losses based on the observed behavior of the network. Explicit feedback solutions require selected notes to provide feedback, in order to achieve NWB robustness. Finally, other solutions can monitor the state of the wireless channel, in order to create more effective strategies for robust NWBs. The following solutions for each category of the solution space are studied:

(a) Selective Additional Rebroadcast: In NWB algorithms that reduce redundancy by preventing nodes from rebroadcasting, apply an algorithm that causes broadcasting nodes to perform a second rebroadcast, if they can locally determine that the packet is likely to have been lost, and that its loss will lead to loss of coverage. This solution is an implicit feedback solution, as the loss is detected without explicit feedback from receiving or neighboring nodes.

(b) Directed Broadcast: Create a new MAC level primitive that allows neighbor-knowledge NWB algorithms to perform a RTS/CTS handshake and reliably
send out a broadcast to another node. Neighboring nodes that overhear this message can treat it as a broadcast packet, rather than as a traditional unicast packet. This solution is an explicit feedback solution, as receiving nodes provide data back to the transmitting nodes.

(c) Link Quality Sensitive CDS: Instead of building a traditional CDS tree to span the entire network, ensure that nodes in the MANET are going to be covered with some guaranteed level of probability. This solution of fixed redundancy monitors the state of the network, allowing for more effective strategies for NWB robustness.

2. Complex Interactions: In addition to cross-interference between connections, self-interference within the connections is also an issue. Most existing work in MANET research assumes that the state of a wireless channel can be characterized by essentially the number of contending transmissions. However, this is not sufficient to explain the types of interactions that were observed experimentally in the scenarios above. Moreover, two contending transmissions sometimes share the medium gracefully, but in other times persistent unfairness results. The second part of this dissertation attempts to expose the low-level interactions that give rise to these inconsistencies. The approach taken is to study the behavior of two interfering single hop connections in detail. By changing their relative geometry, it can be shown that there are a number of possible relationships that produce different patterns of sharing the medium. Some of these configurations are effective, but others have fairness and efficiency problems. Although short term unfairness is a well known problem in ad hoc (that due to exponential backoffs and medium capture), the fairness problems identified in this dissertation are different: they are due to the low-level interactions between contending transmissions.
Chapter 5

Network Wide Broadcast Robustness

In this chapter, the effect of the MAC broadcast unreliability on the performance of NWB algorithms is characterized to demonstrate their lack of robustness. NWB coverage is affected primarily by two factors: the redundancy of the NWB operation and the probability of MAC transmission loss. A dense network allows some NWB algorithms to use redundant paths providing loss-tolerance without losing coverage. This available redundancy is lower in sparse networks, or for algorithms that control redundancy to improve overhead, making NWBs less robust under such conditions.

Neither interference nor transmission occur uniformly across the links of a network. More specifically, interference results in losses in areas closest to the interfering traffic, while transmission errors are affected by the surroundings (which determine the signal fading effects, doppler effect, as well as the path loss exponent which defines how fast the signal attenuates with distance) and increase with the distance between the sender and the receiver.
5.1 Broadcast Robustness

This section outlines the reasons that cause NWB algorithms to lack robustness. Wireless communication channels are unreliable for two primary reasons: (1) Transmission errors: signal propagation effects and interaction with the surrounding environment can cause deep fades in the received signal power (20dB, or 100x changes in signal power are common [87]). These fades can occur in small scales in time and space. This effect leads to a large number of transmission errors, especially when the two communicating nodes are far from each other; and (2) collisions: the wireless channel is non-uniformly shared, giving rise to the well known hidden terminal problems [22].

Transmission errors and collisions makes MAC level broadcast operations susceptible to losses. The lack of higher level reliability mechanism (e.g., as is present in unicast operations via acknowledgements and retransmission) exacerbates the problem. As a result, NWB operations which rely on MAC level broadcast suffer from loss of coverage: the NWB robustness problem.

To address NWB robustness, two general approaches are used: (1) MAC broadcast changes: changes to the MAC layer are introduced to make NWB operations more reliable; and (2) NWB algorithm changes: NWB are done with a smaller set of nodes to cut down on overhead. Both of these approaches are studied later.

5.1.1 Losses Due To Self-Interference

In addition to losses in the network from various application traffic flows, losses can occur with self-interference. In self-interference, a NWB operation results in two nodes broadcasting at the same time, resulting in collisions at receiving nodes. Since any node can issue a broadcast at any time, this can be problematic in a NWB operation. As a result, many NWB algorithms attempt to cut down on the number of broadcasts needed for a NWB.
Ni et al. studied the effect of all nodes in the network performing a broadcast in [30]. They labeled this phenomenon as the broadcast storm problem. Rebroadcasts carried out by nodes in the network were found to be redundant, as many neighbors had the broadcasted information already. Furthermore, the additional rebroadcasts caused contention in the network to go up, as the broadcasts interfered with each other. Lastly, since there is no backoff mechanism or reliability mechanism built into MAC level broadcasts, the number of collisions in the network went up.

5.1.2 Losses Due To Shadowing

In a realistic wireless channel, signals are subject to reflection, refraction and dispersion as they interact with the surrounding environment. Further, the transmissions may undergo Doppler shifts due to mobile objects, and the received signal components will have different delays and power levels. These fluctuations are what is known as signal fading [16]. An idealized signal fading propagation model (that does not model time correlation) was previously described in Chapter 2 and is used in experiments that simulate fading effects.

5.2 Preliminaries and Experimental Setup

The primary performance metrics of interest are: (1) node coverage: percentage of nodes that receive the NWB; (2) overhead: number of retransmissions. Raw overhead is difficult to interpret independently of the network size, and the coverage success. Therefore, normalized overhead, defined as the number of retransmissions per receiving node, was tracked. For flooding, normalized overhead is always one regardless of the topology or the coverage success: every receiving node retransmits the packet once. Optimized NWBs target lowering the overhead while maintaining coverage which should result in a normalized overhead smaller than 1.
To simulate losses in the network, two approaches are used. First, packets are probabilistically dropped at receiving nodes; a similar approach to modeling losses was used in other works [52]. While this approach is somewhat unrepresentative (transmission errors are typically not uniform across all links), it provides a controllable approach to varying the loss rate. The second approach involves introducing fading to the network. Fading models allow for more realistic transmission behavior, but vary depending on the distance between nodes. As a result, the best way to judge the effect of fading is by comparing NWB behavior in networks of different densities. Previous work has been done using Constant Bit Rate (CBR) traffic flows in order to increase the level of contention present in the network. These flows often interfere with each other, preventing a consistent level of contention in the network. As a result, data gathered from these studies is not as controlled as what is presented below.

All experiments in this chapter use the Network Simulator NS-2 [74]. NS-2 is a discrete event simulator with detailed models for the network protocol stack, including the IEEE 802.11 MAC protocol. NS-2 includes simplified models for wireless propagation. In all scenarios, nodes are randomly deployed with a uniform distribution in a fixed area of 1000 by 1000 meters. The 802.11 MAC implementation in NS-2 was used for experimentation with the default parameters (range of 250 meters). In each experiment, one NWB is generated per node. The NWBs are timed to ensure that successive operations do not interfere. Each data point represents an average of 20 scenarios with different random seeds. While the confidence intervals are not presented in the graphs to avoid clutter, they were tracked; the average is narrowly bound (95% confidence intervals within 1% of the mean).

For the signal fading propagation model, the pathloss exponent is set to 2.65, which is representative of a very lightly shadowed urban area. The shadowing deviation is set to 7.5, which is in the middle of the outdoor range for the shadowing model [88].
5.3 Evaluated Algorithms

In addition to flooding, the following NWB algorithms were evaluated, in order to provide representatives of the different classes of solutions discussed in Section 3:\(^1\)

- **Location Based Algorithm (LBA) [30]:** In this algorithm, a node includes its location in the rebroadcasted packet. Upon reception of a broadcasted packet, the receiving node notes its current location in comparison with the location of the sending node, obtained from the packet header. This information is then used to calculate the additional area which would be covered with an additional broadcast. Based on this information, a node decides whether its rebroadcast provides sufficient coverage to be worth sending. This is a dynamic flooding based approach (not topology sensitive). Recall from Section 3.1.1 that flooding typically leads to higher overhead in dense networks. By including location information in each packet, the overhead is not raised quite as high as a traditional flood.

- **Ad Hoc Broadcast Protocol (AHBP) [38]:** Nodes track two hop neighbor information via ‘HELLO’ packets and use this information to explicitly select a set of 1-hop neighbors to rebroadcast the packet such that all the 2-hop neighbors are covered. Only nodes marked as Broadcast Relay Gateway (BRG) nodes perform a broadcast. The node selection algorithm of AHBP is as follows:

  1. Locate all 2-hop nodes that can only be reached by a single 1-hop node. Mark those 1-hop nodes as BRG members.
  2. Calculate the set of nodes that will be covered by the BRG nodes.
  3. For all remaining 1-hop neighbors, find the neighbor that will cover the most uncovered 2-hop neighbors, and mark it as a BRG node.

\(^1\)Code for LBA, SBA, and AHBP provided by Tracy Camp’s group at Colorado Mines. Code for DCB provided by W. Lou.
4. Repeat steps 2 and 3 until all 2-hop neighbors are covered.

Within a NWB packet, the set of BRG neighbors is kept in the packet header. As a result, upstream neighbors calculate which downstream neighbors will rebroadcast the packet, making this a static CDS-based approach. Recall from Section 3.1.2 that static CDS algorithms can suffer greatly if a node with forwarding responsibilities does not receive a packet. In such a situation, the propagation of the NWB is halted, and the NWB is often worthless.

When a BRG node receives a broadcast, it uses its current 2-hop neighbor information to calculate which 1-hop neighbors received the transmission. These neighbors are then removed from the neighbor set used in the BRG selection algorithm described above.

- Scalable Broadcast Algorithm (SBA) [40]: This algorithm is essentially a dynamic version of AHBP where nodes locally determine if all their 2-hop neighbors have been covered based on overhead broadcasts. The 2-hop neighbor information is obtained via ‘HELLO’ packets.

  If node A sends a packet, and it is received at node B, node B calculates if it has neighbors that are not covered by node B. If there are uncovered neighbors, it will retransmit the packet.

  Recall from Section 3.1.2 that dynamic CDS algorithms adapt to losses far better than their static CDS counterparts. As a result, a loss at one node typically does not halt the NWB broadcast. This function comes with a tradeoff of higher forwarding costs than the static CDS approaches, but is more resilient to poor network conditions.

- Double-Covered Broadcast (DCB) [52]: This is a static topology-sensitive CDS-based algorithm with fixed built-in redundancy (CDS developed to provide double-coverage for every node). Neighbor information is tracked via ‘HELLO’ packets. A
node wishing to send a NWB will follow the following algorithm:

1. Select a subset of 1-hop neighbors that cover all 2-hop nodes. Each of these neighbors must be covered by at least two transmissions, one from the sending node, and one from the 1-hop neighbor set. The nodes selected serve as forwarding nodes.

2. Each forwarding node follows the previous step and broadcasts the packet.

3. The transmission of the forwarding nodes serves as an acknowledgement for the upstream sending nodes. If a sender does not detect rebroadcasts from all forwarding nodes, it recalculates the forwarding node set, and repeats the process.

While this algorithm has built in redundancy, it has a higher overhead, due to the double-coverage. Furthermore, when recalculating the forwarding node set, the latency of the NWB is increased, as a node must wait for a series of ‘HELLO’ messages to be sent.

5.4 Grid Topologies

Grid topologies consist of nodes that evenly deployed in a two-dimensional grid throughout the simulation area. This configuration may be representative of static pre-planned networks such as mesh network [6]. Grids also provide a level of control to experiments, due to the uniform density present throughout the network. The coverage of flooding for different density grids inside of a 1000m by 1000m area were studied. Depictions of these grids can be seen in Figures A.5, A.6, A.7, and A.8.

Figure 5.1 plots the coverage achieved by flooding in different densities, using the controlled drop mechanism described earlier. As expected, grids that are more dense achieve a
higher level of coverage. This is due to the fact that denser grids provide more redundancy for the flood. In a sparse grid, the loss of a few packets can result in loss of coverage to significant portions of the network. Figure 5.2 charts the coverage of flooding in an environment with fading. The results are similar—denser grids have a higher coverage ratio than the sparser grids.

5.5 Random Topologies

This section describes studies done with nodes that are randomly deployed in a 1000m by 1000m area. Samples of these topologies can be seen in Figures A.1, A.2, A.3, and A.4.

5.5.1 Controlled Drop

Figure 5.3 charts the coverage obtained for flooding in different densities of networks. Similar to the density study done for grid scenarios (Figure 5.1), as the density increases, the overall coverage increases. This is because the redundancy built into the network has increased.

Figures 5.4 and 5.5 plot the coverage and overhead for various NWB protocols in a sparse 30 node environment. As the loss rate is increased, the overall coverage of the
protocols decreases. This is particularly true for CDS-based approaches, where the loss of one packet in the CDS tree can stop the progression of the NWB.

The coverage of flooding and LBA is very similar. However, LBA optimizes the number of rebroadcasts needed based on location, resulting in a slightly lower overhead. SBA, being a dynamic CDS algorithm, adapts to losses in the network, resulting in coverage near flooding. Furthermore, as the loss rate increases in the network, the number of broadcasts performed by SBA increases as well. This demonstrates the adaptive nature of the SBA protocol. For the static CDS approaches, DCB has a higher coverage level than AHBP. This behavior is expected, as each node is covered twice, as presented earlier.

The controlled drop experiments were repeated in a denser, 60 node environment (Figures 5.6 and 5.7). As the network is more dense, the protocols are generally more tolerant
to losses in the network, resulting in higher coverage. This is especially true of flooding and LBA. The CDS-based approaches make a sparse network out of a dense network, and therefore lose some of the built in redundancy of a dense network. At high loss levels, the static approaches of AHBP and DCB drop off when compared to the dynamic approach of SBA and the flooding algorithms.

In terms of overhead, since more nodes are covered per broadcast, the overall normalized overhead tends to be less than that of a sparser network. The gain of using LBA over flooding is larger in a dense network, since less nodes rebroadcast per region of the network.

5.5.2 Signal Fading Losses

The coverage for the NWB protocols in an environment with signal fading is depicted in Figure 5.8. In this graph, the X axis varies according to density, and the fading parameters are kept constant. As the density increases, the coverage for all of the protocols increases. The overhead for the NWB protocols in a fading environment is shown in Figure 5.9.
5.6 Cluster Topologies

Cluster topologies are networks that have groupings of nodes in specific areas, rather than randomly scattered throughout the network. A cluster scenario was studied with 4 clusters equidistant from each other, connected by a single node. The resulting shape was that of a “plus”. This scenario can be seen in Figure A.9. This shape is representative of multiple groups of nodes, connected by a single ‘command center’.

5.6.1 Controlled Drop

Figure 5.10 plots the coverage achieved by the different protocols in the cluster scenarios. The results roughly mirror the results of the random topologies, with flooding
achieving the highest level of coverage. Figure 5.11 plots the overhead of the different protocols. The results of the cluster experiments have lines that are not as smooth, as a loss of a NWB transmission has a high chance of preventing the rest of the network from receiving the broadcast. The results are somewhat similar to the results found in the 30 node random deployment environment (Figures 5.4 and 5.5). This is because a 30 node environment in a 1000m square area is very sparse and loosely connected. The loss of a transmission along one of the links has a high probability of terminating the NWB propagation. As the network density increases, this probability is lowered. By the same logic, if the clusters were made larger, with more nodes, the coverage results would increase proportionally.

### 5.6.2 Signal Fading Losses

![Graph 1](image1.png) ![Graph 2](image2.png)

Figure 5.12: Coverage (Cluster Deployment, Fading)  
Figure 5.13: Overhead (Cluster Deployment, Fading)

Figures 5.12 and 5.13 show the results of the protocol evaluation in an environment with signal fading. SBA slightly outperforms flooding, and the static approaches of AHBP and DCB lag significantly far behind in coverage. AHBP and DCB suffer as a result of being static CDS algorithms. Losses upstream are not adapted to downstream, resulting in lower coverage. The overhead of LBA is significantly lower than flooding, due to the fact that only one node per cluster performs a broadcast.
5.7 Mobile Topologies

This section presents the coverage and overhead studies for various NWB protocols in a few different mobile environments. Topologies containing nodes within a 1000m by 1000m area were used for these studies.

5.7.1 Random Waypoint

The Random Waypoint Mobility Model is a model commonly used in MANET research. In this mobility model, nodes move in varying directions and speeds, with a pause time between each movement and direction change.

Figure 5.14: Coverage (RW, Controlled Drop, 30 Nodes)

Figure 5.15: Overhead (RW, Controlled Drop, 30 Nodes)

Figure 5.14 shows the tests using the random waypoint model with a pause time of one second between movements, and a maximum speed of 15 meters per second. This figure represents the coverage achieved for different NWB protocols. Similar to the static scenarios, flooding and LBA do better than the neighbor knowledge protocols. This behavior is noticed even more in a mobile environment, because the mobility causes neighbor knowledge to become stale. When Figure 5.14 is contrasted with the static 30 node results shown previously in Figure 5.4, the staleness of the neighbor knowledge data can easily be seen. Figure 5.15 shows the overhead of the protocols in a 30 node environment. The trends seen
here are similar to those seen in the static scenarios.

Figures 5.16 and 5.17 show the coverage and overhead obtained in a 60 node environment, using the random waypoint model (1 second pause time, 15 meters/sec maximum movement). These results again show that dense networks are more robust and resilient to losses. The overall coverage increases, and the overhead goes down, as more nodes are reached with the broadcasts that are sent.

Figures 5.18 and 5.19 show the coverage and overhead obtained for simulations of different densities in a fading environment. The protocols that do not use neighbor knowledge, along with the dynamic CDS algorithm do better than the static CDS algorithms. Again, the trend that denser networks have higher coverage occurs here.
5.7.2 Probabilistic Random Walk

The probabilistic version of the random walk model uses a set of probabilities to determine the next position of a node. This model also uses random directions and speeds, but makes use of a matrix in order to determine the node position for the next time slot. Since the movements are probabilistic, the movements of nodes tend to be more realistic than purely random movements [89]. An interval of 0.5 was chosen for these studies.

This mobility model was chosen for study since there have been studies that have shown the random waypoint mobility model is not always an accurate representation of mobility [90]. Their studies have shown that the general speed of the network slows over time. Bettstetter and Wagner have also shown [91] that the nodes tend to converge on the center of the network over time, when using the random waypoint model.

Figure 5.20: Coverage (PRW, Controlled Drop, 30 Nodes)

Figure 5.21: Overhead (PRW, Controlled Drop, 30 Nodes)

Figure 5.20 shows the coverage obtained with the probabilistic random walk in a 30 node environment. The dropoff is much sharper, when compared with the random waypoint graphs presented earlier (Figure 5.14). This is due to the effects mentioned earlier; that the random waypoint mobility model tends to slow down over time and converge towards the middle. As the network converges, and the neighbor information data is less likely to be out of date, the redundancy of the network is increased.

Figure 5.21 shows the overhead for the probabilistic random walk in a 30 node environ-
ment. Again, overall overhead is higher with this model, when compared with the random
waypoint data (Figure 5.15).

As one would expect, the coverage obtained for a 60 node environment is higher than
that of the 30 node environment, as can be seen when contrasting Figures 5.22 and 5.20.

The trends in coverage and overhead in a fading environment are similar to those in a
controlled drop environment. Figure 5.24 plots the coverage of the different protocols at
different densities. Finally, Figure 5.25 charts the overhead of the protocols.
5.8 Summary

This chapter presented the NWB unreliability problem. The coverage of a NWB was shown to be affected by two primary factors: the overall density of the network and the chance of a MAC transmission loss. Within a dense network, there are redundant paths between nodes, which provide an inherent tolerance for broadcast losses. If one node’s rebroadcast is lost, a neighboring node’s broadcast will cover a large portion of the same area. Transmission losses occur in areas near interfering traffic, or when propagation factors, such as surroundings and fading, come into effect. The following chapters describe solutions related to NWB reliability.
Chapter 6

Robustness Control – Solution Space

Increasing NWB reliability requires increasing the probability of the reception of the NWB rebroadcast operations. This is especially true in situations where their loss is likely and the redundancy in the network is low. The goal of the solutions presented in this dissertation is to improve the reliability of the NWB, rather than ensure complete reliability; guaranteed reliability requires too much overhead (for example, neighbor discovery and the use of unicast packets).

With solutions for robustness control, NWB algorithms can now be thought of in two parts: (1) Redundancy control: this phase of the algorithm targets reducing the redundancy in the rebroadcasts; and (2) Robustness control: this phase of the algorithm attempts to recover from losses occurring in the transmissions necessary to cover the nodes. The focus of most existing solutions is redundancy control; in contrast, our focus here is on robustness control.
6.1 NWB Robustness Control – Solution Space

There are several possible approaches for redundancy control which are classified in the remainder of this chapter. Please note that even though robustness control is discussed separately from the remainder of the NWB and redundancy control aspects of the algorithm, often the most appropriate choice is influenced by the structure of the underlying algorithm. Examples of such inter-dependence will be discussed as different points in the solution space are examined in more detail in the following three chapters.

Approaches to robustness control can be classified along multiple axes, including the following. First, we distinguish solutions according to how they trigger robustness control responses (typically additional rebroadcasts). Fixed redundancy approaches incorporate a fixed degree of redundancy in their coverage, beyond the minimum necessary, to leave a safety margin against broadcast losses. In contrast, loss sensitive approaches, trigger additional redundancy (typically in the form of additional rebroadcasts) only when losses are detected or predicted.

Among loss-sensitive approaches, there is a number of solutions possible based on the approaches for detecting/predicting losses and how redundancy is built in response. Broadly, losses detection/prediction can be accomplished by explicit or implicit feedback.

6.1.1 Explicit Feedback Algorithms

In explicit feedback algorithms, the receivers inform the senders of whether the broadcast was received successfully using an explicit transmission. Explicit feedback solutions face the following problem: if multiple receivers of a MAC broadcast have to provide acknowledgements, collisions occur. However, its possible to randomize/stagger the responses or require feedback from a subset of the receivers only.

With explicit feedback, the granularity of the feedback can be adjusted. The simplest
scheme is to provide feedback on every NWB transmission. This has the cost of immediate latency in a NWB operation. Another approach that can be used is to provide feedback about NWB successes is to inform the sending node periodically. This requires nodes to cache previously sent data, in case a failure situation arises. Depending on the granularity and the subset of receivers responding, explicit feedback may also increase latency and load on the network (due to the acknowledgement traffic).

### 6.1.2 Implicit Feedback Algorithms

Schemes that use implicit feedback attempt to judge the success of a NWB transmission based on locally observed behavior and without requiring addition control packets to be exchanged. Briefly, this approach hypothesizes that the behavior of the neighbors will be different in the case that they receive a broadcast from the case where they don’t. Thus, by observing the behavior of nearby nodes, the loss probability can be predicted. A simple example of such implicit feedback is for a node to observe the channel and see if the NWB packet was retransmitted by neighboring nodes. If enough retransmissions are overhead, the original transmission to the neighbor was likely received successfully.

Implicit feedback solutions can improve their decision by factoring in other criteria that can improve the loss prediction. For example, each node can measure the utilization of the channel; the higher the utilization the higher the probability of a loss. However, this approach is imprecise because the local state at the sender may not match that at the receivers. An additional metric of interest is the expected number of rebroadcasts (a function of density and NWB algorithms) the knowledge of which can help refine the prediction made by the implicit feedback mechanism.

An interesting hybrid approach uses explicit feedback to estimate the probability of success of a broadcast and perhaps the criticality of it; this approach is termed *state-aware*. This approach is similar to the utilization and density estimation discussed above. However,
because those estimates are created based on the imprecise source view, they may not be valid at the destination where losses occur. Further, link utilization is only one of the factors that influences the quality of the wireless channel; other factors cannot be assessed without feedback from the receiver [14].

State-awareness can be combined with implicit feedback or fixed redundancy algorithms. Most NWB solutions view the link quality as boolean - links either exist or they do not. The quality of links differs due to many variables, including the distance between the nodes, the power of transmissions between the nodes, and the overall traffic nearby [14]. NWB solutions can leverage this data in order to provide NWB robustness, for example, by building in more redundancy for nodes that are covered only by weak transmissions in a fixed redundancy NWB algorithm.

6.2 Classifying Existing Solutions

Full reliability for NWBs is an expensive operation. Using the 802.11 Medium Access Control (MAC) layer, the only mechanism for a reliable transmission is with unicast packets, which have an optional Request To Send/Clear To Send (RTS/CTS) handshake, followed by the data transmission, followed by an acknowledgement (ACK) packet. If the ACK is not received by the sending node, the process is retried, up to 7 times.

Tang and Gerla proposed a full reliability MAC protocol to deliver NWB data [92]. This protocol requires all nodes to maintain a neighbor list, a queue of previously sent broadcast packets, and a queue of previously received broadcast packets. Nodes maintain 1-hop neighbor lists by periodically sending out ‘HELLO’ packets. When performing a NWB, a source node selects a neighbor, and performs a RTS/CTS handshake. When sending the RTS, the packet also contains a piece of data indicating which NWB sequence number is about to be transmitted. The neighboring node replies with a CTS message, containing
the last successfully received NWB id. The source node is then responsible for sending all NWB packets between the two values. This process continues in a round-robin fashion throughout the network.

This solution is an example of an explicit feedback algorithm. Their solution has a level of overhead, due to the extra packets that must be exchanged with each node, as well as a high amount of latency, if packets are dropped.

The solutions of Hyper-flooding [53] and Hyper-gossiping [54] are more examples of explicit feedback algorithms. When nodes come into range, ‘HELLO’ packets are sent, indicating that they are a new node, and that the NWB data should be resent.

Lou and Wei’s Double Covered Broadcast (DCB) [52] solution is one that is an implicit feedback solution. Sending nodes keep track of which neighbors rebroadcast the NWB packet. If that retransmission is not heard, it is assumed that the first transmission failed.

6.3 Summary

This chapter overviewed the potential solution space for increasing NWB robustness. Many possible approaches were overviewed, along with the intuitive tradeoffs that result from these approaches. The existing solutions were classified in terms of this solution space. In the next three chapters, three new solutions are presented: (1) Selective Additional Re-broadcast (SAR): A network layer implicit feedback solution; (2) Directed Broadcast (DB): A MAC layer explicit feedback solution; and (3) Link Quality Sensitive Connected Dominating Set: A state-aware fixed redundancy protocol.
Chapter 7

Selective Additional Rebroadcast

Improving Network Wide Broadcast (NWB) robustness requires increasing the probability of the reception of the NWB rebroadcast operations. This requirement is especially true in situations where the broadcast loss is likely and the redundancy in the network is low. This chapter presents and analyzes the Selective Additional Rebroadcast (SAR) solution introduced earlier in this dissertation. SAR represents a network level solution that uses implicit feedback to predict losses and compensates by selectively rebroadcasting when losses are predicted.

7.1 Selective Additional Rebroadcast

In the class of network level solutions, the redundancy of the NWB is increased to attempt to improve robustness. An existing example of this approach is the Double Coverage Broadcast (DCB) [52] which was discussed earlier Chapter 3. In DCB, a Connected Dominating Set (CDS) is constructed such that every node is covered twice. While DCB improves coverage relative to regular CDS algorithms, it remains vulnerable to losses since the forwarding set is determined statically. Further, the degree of redundancy that is built
DCB does not attempt to detect losses either implicitly or explicitly; thus, in cases where the level of built in redundancy is lower than that needed, it is unable to recover. Further, in cases where the redundancy is not needed, it incurs a higher overhead than algorithms that are sensitive to losses.

The protocol introduced here is Selective Additional Rebroadcast (SAR): an approach where NWB packets are selectively rebroadcast an additional time if they are suspected to have been lost. Ideally, lost broadcast packets would be recovered via explicit feedback in a manner similar to Automatic Repeat Request (ARQ), where the receiving node requests a retransmission if a timeout or error occurs. However, since this is not possible for broadcast operations due to multiple receivers, the protocol attempts to detect losses based on locally available information. SAR can be added to any existing NWB algorithm to recover from losses. Accordingly, starting from an NWB optimized for overhead, SAR can be added to provide additional robustness.

It is important to note that these approaches do not simply restore some of the redundancy that is available in flooding. They key to their operation is being able to locally predict whether a rebroadcast has been lost and retransmitting if necessary. The additional rebroadcasts are not generated blindly; they are only generated when they are predicted to be needed – in sparse areas of the network when a loss is likely to have happened. Further, the redundancy is not along a different path; rather, it is simply a rebroadcast of the packet on the same path.

SAR is a dual to the local solutions to the broadcast storm problem [30]. Those solutions selectively eliminate rebroadcasts of the flood packet if it is suspected to be redundant to cut down on the flood overhead. In contrast, this protocol selectively rebroadcasts packets an additional time if it is suspected to be lost in order to improve reliability.

SAR should be applied judiciously. In dense regions of the network topology, the available redundancy is high and the broadcast algorithm should cut down on the number of
rebroadcasts, especially if interference is low. However, in sparse regions of the network topology, and in the presence of interference, SAR can significantly improve the reliability of the NWB. Thus, SAR as the robustness control approach, should be tightly integrated with the redundancy control aspect of the NWB algorithm.

SAR differs from the solutions of Hyper-gossiping [54] and Hyper-flooding [53], presented earlier in Chapter 3 for a number of reasons. The criteria used for rebroadcasting in Hyper-gossiping and Hyper-flooding is not sensitive to losses. Instead, a fixed amount of redundancy is added probabilistically to the NWB algorithm. In addition, the SAR solution can be applied to NWB algorithms besides flooding.

Several criteria can be explored to decide when to rebroadcast a packet an additional time. SAR is designed to provide NWB robustness implicitly. No explicit feedback is used to predict whether a NWB transmission has been lost. This prediction can be based on recently observed behavior such as recent loss rates and the utilization of the channel. In addition, the prediction metrics can take into account the subsequent behavior of nearby nodes (which may differ based on whether the rebroadcast was received or not). For SAR, the following triggers are considered:

1. Probabilistic Solution: a packet is rebroadcast with a fixed probability. In general, this solution is problematic because it does not adapt to the density or loss rates in the network. Therefore, it may result in large increases in the overhead when it is not needed (e.g., in dense areas and/or when interference is low). This solution is included because it provides a reference point that increases redundancy without using any prediction intelligence. This approach is basically adding Hyper-gossiping [54] to other NWB algorithms.

2. Counter-Based Solution: if the node does not hear $n$ other nodes rebroadcast the packet within a certain amount of time, it will rebroadcast it again. This solution
is attractive because it naturally adapts to the interference level and density of the network. In a dense/low interference area, a number of rebroadcasts is likely to be received after a node rebroadcasts a packet. But in sparse/high interference areas, this is not the case, and the algorithm rebroadcasts a packet to enhance reliability.

First, the behavior of a fixed value of $n$ across the network is studied, followed by the adaptation of the value to reflect the neighboring topology.

3. Adaptive SAR: Rather than having a fixed criteria that applies throughout the network, the appropriate threshold for rebroadcast can be adaptively set at the individual nodes. For example, a node can disable SAR if it determines that the SAR broadcasts have not helped the NWB recently. By doing this, the node can cut down on overhead when the broadcasts are not needed, and re-enable SAR later, in case new nodes have moved into the surrounding area. Alternatively, a node may assess its local neighborhood to compute the expected number of rebroadcasts and set its rebroadcast threshold to match those.

Furthermore, additional improvements to these metrics exist. Examples of these include:

1. Medium Access Control (MAC) Utilization: A node can take into account how busy the medium is, and use that to gauge how likely the loss of a NWB is. This is potentially unrepresentative, since the node is testing how busy the MAC layer is at the source, rather than at the destination.

2. Density: A node can use the number of neighbors it has to determine whether it is in a dense or sparse area of the network. Furthermore, it may be able to use this information to determine whether it is a leaf node, where a rebroadcast is wasteful, since no new nodes will be covered. Depending on the NWB algorithm being used, the density can be further defined as two different values: (1) The physical density: this
consists of the number of neighboring nodes; (2) The NWB density: this is the number of neighboring nodes that perform a NWB transmission. If not all neighboring nodes transmit, it is not useful to track all physical neighbors.

In the next section, the results of using a pure probabilistic solution, a counter-based solution, and adaptive solutions are presented. The adaptive solutions include the following modifications to the NWB protocols:

1. Flooding: This combines the counter-based approach, MAC utilization, density, and observed SAR effect. When a node receives a flooded packet, a timer is set to later rebroadcast the packet an additional time. The node increments a counter every time the packet is heard after the original reception. When the SAR timer expires, this counter is examined. If it is equal to zero, it is likely that an additional broadcast will be wasteful. After a few cases of this in a row, SAR can be disabled. The node keeps track of the counter information for the past few broadcasts, and uses this as the observed number of neighbors. A metric is made based on the ratio of the counter value to the observed average number of neighbors. This metric is combined with the MAC utilization, and the second broadcast is made only if the metric is above a threshold.

2. Ad Hoc Broadcast Protocol (AHBP): This combines the MAC utilization metric along with a variation of the density criteria. Since AHBP is a static CDS algorithm, the nodes that are needed to broadcast are known at the time of scheduling the SAR timer. When broadcasted packets are received, the SAR timer is updated with the node information that sent the packet. When the timer expires, a metric based upon the ratio of nodes that were heard from compared to the missing nodes, along with the MAC utilization, to rebroadcast the packet. This approach allows the static algorithm to only broadcast if the missing CDS nodes haven’t been heard from. An
additional broadcast if the nodes have been covered will gain no new coverage, and is purely wasteful.

3. Scalable Broadcast Algorithm (SBA): This approach is similar to the approach found in the AHBP modification. The nodes that were not covered in the original broadcast are tracked, and each duplicate NWB packet is tracked for information pertaining to these nodes. When the timer expires, a metric based on MAC utilization and the ratio of the heard from compared to missing nodes is used to determine whether the second broadcast will occur.

7.2 Experimental Evaluation

7.2.1 Preliminaries

The overhead required for the various ‘HELLO’ messages is not tracked. The reason this is omitted overhead is that it is not assessed per NWB but happens periodically. Thus, one round of neighbor discovery may benefit multiple NWBs.

The scenarios used were similar to those used in the NWB studies thus far; the scenario characteristics are summarized briefly here for readers’ convenience. In each topology, nodes were randomly deployed 30 nodes in a 1000 meter by 1000 meter area. 20 such topologies were used to obtain the results. In these scenarios, each packet has a fixed probability of being dropped during a transmission. This is representative of the effects of collisions as well as shadowing within the network. The effect of mobility were not considered in these experiments.

In each experiment, one NWB is generated per node. The broadcasts are timed to ensure that successive NWBs do not interfere with each other. Each data point represents an average of 20 different simulation runs with 20 different scenarios (resulting in different
topologies and source/destination selection for interfering connections). While confidence intervals are not depicted, the number of scenarios was sufficient to have 95% confidence intervals be within 1% of the mean value across all measured values.

### 7.2.2 Evaluation of SAR Approaches

![Figure 7.1: SAR Approaches Comparison, Coverage](image1)

![Figure 7.2: SAR Approaches Comparison, Overhead](image2)

Using a purely probabilistic metric to use SAR, coverage is slightly increased, while overhead is increased by the percentage used as the probability value $P$. This approach is a *blind* method of controlling robustness. A node rebroadcasts solely based on a probability, and takes no external observations into account. As a result, nodes perform the SAR broadcast when not necessary, and a critical rebroadcast may not occur.

Using the counter-based metric for SAR, coverage values are increased more than the probabilistic-based approaches, and the overhead fluctuates, based on network conditions. This approach does make use of observed network behavior, and the results are better, with higher coverages and lower overhead. A counter-based approach is *not blind*, but it also *not adaptive*. For example, nodes near the edge of the network (leaf nodes) may not have their counter value met, resulting in them performing the additional SAR broadcast. This broadcast is wasteful, since no new nodes will be covered.

The effect of the problem of leaf nodes broadcasting unnecessarily can be seen at a
0 loss rate in the counter-based solution. In this case, an oracle implementation of SAR would not increase the redundancy because no losses occur. However, in the simple counter implementation, there is an increase in overhead with SAR even at 0 loss rate.

To address this problem in an algorithm such as AHBP, a node can use its neighbor knowledge to see how strongly connected it is. A node that is a leaf node will not have a high neighbor count. This knowledge can be used to not cause additional SAR broadcasts if the node has heard a number of broadcasts equal to its CDS neighbor count. Furthermore, for static algorithms, such as AHBP, the neighbors which are to rebroadcast are known at the upstream sending node. The sending node can ensure it has heard a transmission from each rebroadcasting CDS node, and cancel the additional SAR broadcast if the broadcast was propagated successfully.

An additional metric to be used is that of the MAC utilization. A node in a section of the network with more traffic will have a higher MAC utilization value, and the chances of a successful broadcast are smaller.

Figures 7.3 and 7.4 compare the base AHBP protocol, the counter-based AHBP-SAR protocol, AHBP-SAR with leaf node pruning, and AHBP-SAR with MAC utilization. It can be seen that the leaf node pruning results in coverage at the same level as the counter-based solution, with a lower overhead. This is due to the suppression of broadcasts from leaf nodes that do not cover additional areas of the network. The MAC utilization version
adapts to the increasing loss level in the network. Applied properly, this metric can also be valuable. Since each metric is valuable on its own, they are included in the criteria used for the adaptive SAR protocols.

The adaptive metrics cover cases where a counter-based metric does not perform well. They adjust according to more external network indicators, such as the observed network traffic load. Figures 7.1 and 7.2 show the coverage and overhead for the three approaches in a sparse 30 node environment, with modifications to the AHBP protocol. In these graphs, it can be seen that the probabilistic approach has the poorest coverage, along with an overhead that does not adapt to the network conditions. The counter-based approach has coverage higher than the probabilistic approach, along with an overhead that tends to increase as the loss rate increases in the network. Lastly, the adaptive approach has the best overall coverage, and an overhead that is increased as the loss rate increases in the network. This overhead starts out around the level of the base AHBP protocol, and stays below the other approaches until the loss rate is sufficiently high. Even at very high loss rates, the overhead is below the level of flooding, which is constant at a value of 1.

The results for the other protocols and densities were similar, and are not presented here to conserve space. Furthermore, since the adaptive approach had the best results, the studies in the rest of this chapter will deal solely with the adaptive protocols.

### 7.2.3 Adaptive SAR Evaluation

SAR was implemented according to the criteria presented in the previous section. For the NWB algorithms other than flooding, the additional rebroadcast is only scheduled if an initial rebroadcast is decided upon by the algorithm. For example, in AHBP where a subset of the nodes is selected to relay the packet further, only those nodes that have an original forwarding responsibility are tasked with an additional rebroadcast according to the probabilistic or counter-based criteria.
Figure 7.5 shows the coverage obtained with the protocols modified with SAR, along with Flooding and DCB for comparison. Referring to Figure 5.4, the coverage for the SAR protocols is higher than their respective base protocols. Furthermore, the coverage of the SAR protocols is significantly higher than that of DCB.

The overhead for the protocols in a 30 nodes environment is shown in Figure 7.6. With the SAR protocols, the overhead increases as the drop probability increases. This shows that as the loss rate goes up, additional nodes compensate for the loss dynamically and schedule a rebroadcast. This dynamic adaptation does not exist in DCB because its degree of redundancy is statically fixed (at 2), regardless of the loss rate experienced in the network.

To demonstrate that these solutions are viable for dense networks as well as sparse networks, the same protocols were evaluated in a 60 node environment. Figure 7.7 plots
the coverage obtained by the protocols, while Figure 7.8 plots the corresponding overhead. Again, the coverage obtained by the SAR protocols is better than the corresponding base protocols and DCB. The overhead remains below flooding, except at very high loss rates in the network. This overhead adapts and increases as the loss rate is raised throughout the network.

Examining all of this data, it can be seen that the coverage of AHBP with SAR is raised to a level near flooding, but still remains significantly below the overhead present in flooding. The CDS algorithms modified here tended to have a lower overhead than flooding, but a much higher coverage. This achieved the first goal of making use of the CDS trees present in many algorithms which cuts down on redundancy. The second goal of increasing the robustness of the algorithms in face of losses was also met.

### 7.3 Summary

Flooding provides a fixed degree of redundancy: in low density scenarios and at high loss rates, this redundancy is not sufficient. The SAR approaches presented here outperform flooding by dynamically adding additional redundancy where it is needed. In contrast, in high density scenarios, the available redundancy is sufficient to keep coverage acceptable at a high loss rate, but is overkill at low loss rates. In this case, SAR outperforms flooding under low losses by keeping the overhead much lower than that of flooding and dynamically growing it as the loss rate increases. Finally, for many applications, such as route discovery, the increased reliability is worth a small increase in overhead.

Different criteria were examined as potential metrics for deciding when to perform an additional rebroadcast. By utilizing the different criteria, protocols were designed that adapted to the network conditions, resulting in high network coverage with a low overhead.

This solution is an example of a NWB robustness solution that uses implicit feedback.
Simple criteria were used to trigger an additional rebroadcast. This rebroadcast was performed only when necessary, and added a significant level of coverage as a result. Furthermore, since the feedback is implicit, no extra strain is placed on the network in order to achieve a more robust NWB.
Chapter 8

Directed Broadcast

This chapter presents and analyzes the Directed Broadcast (DB) Medium Access Control (MAC) level primitive for improving robustness. Directed Broadcast attacks the source of unreliable broadcasts – the fact that the underlying MAC level broadcast is unreliable. In the solution space discussion in Chapter 6, DB represents a MAC level solution that uses explicit feedback with each packet, from a selected member of the receiving nodes. Directed Broadcast is first presented, and then its use in improving Network Wide Broadcast (NWB) algorithms is shown. Finally, the performance of the DB enhanced algorithms is analyzed, in terms of coverage and normalized overhead.

8.1 Overview

Recall that the underlying reason for MAC broadcast unreliability is the fact that it is not possible to conduct the Request to Send/Clear to Send/Data/Acknowledgement (RTS/CTS/DATA/ACK) handshake for collision avoidance and link level reliability due to the fact that there are multiple receivers. Having the individual receivers acknowledge the broadcast leads to collisions on the acknowledgements. DB bypasses this problem by
selecting a single partner among the receiver set to conduct the handshake process with. All other neighbors still receive the data portion of the broadcast.

Effectively, the packet is unicast to the partner neighbor, but is marked as ‘public’ so that all neighbors receive and process it. At the neighboring node, the packet is handled like all other traditional unicast packets - since the packet is targeted to that node, it can accept it and pass it up the network stack appropriately. At other neighboring nodes, they inspect the packet to see if it is a directed broadcast by examining the bit that was previously set. If it is set, the packet is handled as a broadcast packet would be, otherwise it is discarded. The node that is the target of the directed broadcast is the only one that performs the RTS/CTS handshake with the sending node. If the RTS/CTS handshake does not succeed in the normal 7 tries it is given, the broadcast data goes out in a traditional broadcast packet form.

Directed broadcast increases reliability in two ways: (1) it ensure that at least one sender-selected neighbor receives the packet; retransmissions are used if necessary to accomplish this task; and (2) the RTS/CTS handshake reduces the potential for collisions. This effect should be especially valuable if losses are due to collisions. In addition, the ability of directed broadcast to control what neighbor receives a packet with full reliability can be utilized by the NWB algorithms that use them.

The choice of the neighbor can be simple (using known nodes from active connections, recent floods, or listening promiscuously), or sophisticated (proactively finding neighbors and choosing the node(s) most likely to benefit). Directed broadcast is ideal for protocols that require neighbor knowledge, such as the Ad Hoc Broadcast Protocol (AHBP) [40], Scalable Broadcast Algorithm (SBA) [38], and Double Covered Broadcast (DCB) [52].
8.2 Related Work

Tang and Gerla [42] propose a MAC level scheme where all the receivers ACK a broadcast. If the sender receives no acknowledgements, it retransmits the packet. If multiple receivers reply, the sender interprets noise on the medium (as multiple replies collide) as an acknowledgement. If no acknowledgements are received, the packet is rebroadcasted again (up to a 7 time retry limit, similar to unicast packets). Nodes are required to keep a window of sent packet numbers, and attempt to update all nodes in the network in a round-robin fashion, forwarding any broadcasted packets a node does not have in its buffer. This solution results in at least one node receiving the packet, with an attempt to synchronize other nodes in the network later. However, it has multiple shortcomings. All nodes acknowledge a broadcast packet, resulting in energy waste. Multiple acknowledgements also raises the amount of contention in the network. Since the protocol just requires a single ACK to be returned to the broadcasting node, a specific neighbor can not be guaranteed to have received the broadcast. This protocol also requires modifications to the radio such as detecting noise from multiple transmissions. Lastly, no RTS/CTS collision avoidance mechanism is used for sending out the broadcasts.

Directed broadcast offers several advantages over their solution: (1) the guaranteed receiver can be selected: this allows us to pick critical nodes for guaranteed reliability. For example, in algorithms relying on Connected Dominating Sets, or other virtual backbone NWB algorithms, the backbone/relay nodes can be selected as the directed broadcast partner; (2) it does not require modifications to the radio such as detecting noise from multiple transmissions; the directed broadcast mechanism is a simple mixture of existing radio capabilities; (3) it achieves additional reliability because of the RTS/CTS collision avoidance mechanism; and (4) it is energy efficient: only the broadcast partner participates in the handshake. In contrast, all receivers acknowledge a packet in the other scheme.
8.3 Improving NWB Reliability with DB

DB can be used to improve NWB algorithms by replacing MAC broadcasts with Directed Broadcasts. However, a critical component is how the DB partner is selected. This can most directly be done with topology-sensitive algorithms such as the CDS-based ones (AHBP, SBA, and DCB) because the set of neighbors is tracked proactively as part of the CDS construction. In addition, in these algorithms there are two classes of neighbors – those in the CDS and those who are not. Since it is more critical to reach backbone neighbors (if they are not reached, all the nodes that are reachable through them are not covered), they represent a natural choice for a DB partner.

Thus, the NWB algorithm are augmented with DB as follows. For each of the algorithms (AHBP, SBA and DCB), nodes with rebroadcast responsibilities (those belonging to the CDS), simply pick a partner among candidate neighbors. Candidate neighbors are defined as CDS neighbors that have not already heard the packet. If there are no candidates, then any CDS neighbor is picked. One issue with SBA is that the CDS is not constructed statically – so all uncovered neighbors are potential partners in the DB and there is no distinction between CDS and non-CDS neighbors.

In addition to the base algorithm above, another variation is explored: Since it is critical to reach other CDS nodes, multiple DBs can be used to try and reliably reach them. This space is explored using a parameter $x$ which represents the number of candidates that attempted to reach with DB. The base algorithm above has $x = 1$. For any $x$ value, DB exchanges are carried out with the first $x$ candidates picked randomly from the candidate list. The performance of the improvements is studied in the next section.
8.4 Experimental Evaluations

Directed broadcast was implemented as described in the previous section, and added to AHBP, SBA, and DCB. For AHBP and DCB, only the nodes selected for forwarding by the standard algorithm are involved in the directed broadcast. If a group of neighboring nodes are part of the CDS forwarding nodes, one was chosen randomly as the broadcast partner. For the SBA algorithm, $x$ of the surrounding neighbors are used.

8.4.1 Preliminaries

The overhead required for the various ‘HELLO’ messages is not tracked. The reason this is omitted overhead is that it is not assessed per NWB but happens periodically. Thus, one round of neighbor discovery may benefit multiple NWBs.

The scenarios used were similar to those used in the NWB studies thusfar; the scenario characteristics are summarized briefly here for readers’ convenience. In each topology, nodes were randomly deployed 30 nodes in a 1000 meter by 1000 meter area. 20 such topologies were used to obtain the results. In these scenarios, each packet has a fixed probability of being dropped during a transmission. This is representative of the effects of collisions as well as shadowing within the network. The effect of mobility were not considered in these experiments.

In each experiment, one NWB is generated per node. The broadcasts are timed to ensure that successive NWBs do not interfere with each other. Each data point represents an average of 20 different simulation runs with 20 different scenarios (resulting in different topologies and source/destination selection for interfering connections). While confidence intervals are not depicted, the number of scenarios was sufficient to have 95% confidence intervals be within 1% of the mean value across all measured values.
8.4.2 Base Case

The base performance of the protocols is presented first. Figure 8.1 shows the node coverage while Figure 8.2 shows the normalized overhead. These graphs were previously presented in Chapter 5 and are being repeated here for the readers' convenience. As previously observed in this dissertation, the static CDS approaches perform worse than the dynamic one (SBA) because of their inability to compensate for losses along the backbone. DCB outperforms AHBP because of its double coverage CDS algorithm compared to AHBP's single-coverage one. In terms of overhead, both SBA and AHBP provide lower overhead than DCB (because their forwarding set provides only single coverage). Flooding outperforms all in terms of coverage because of its high redundancy; however, it performs poorest in terms of overhead.

It is important to note that both the effect of density and loss rate vary within the network. Some areas of the topology may be more dense than others. Moreover, the effect of the surroundings, the distance between sender and receiver, and the presence of interference from competing connections make packet loss rates vary as well. For problem studies, a single density of 30 nodes was used to simulate a sparse network.
8.4.3 Directed Broadcast Evaluation

The effect of the RTS/CTS handshake can be seen in the graphs when comparing the base protocol to the protocol with $x=1$. The same number of protocol transmissions are done, except that the DB flavor provides certainty that the packet arrived intact. This leads to a substantially higher coverage value, with only a minor overhead increase. It should be noted that since more nodes are reached with the NWB in the DB protocol, that the overhead values will be altered as a result.

The effects of different values of $x$ can also be seen in the graphs. In Figure 8.3, the coverage of AHBP and flooding are compared with directed broadcast, with $x$ values of 1-3. The $x$ values of 2 and 3 yield higher results, as extra broadcasting has been done. In Figure 8.4, the overhead is plotted, with the higher $x$ values causing greater overhead as
expected. In practice, the RTS/CTS handshake would cause some nodes to cease transmissions temporarily, resulting in a lower drop probability. Preliminary experiments indicate this holds true.

Figure 8.5 and 8.6 plot the effect of directed broadcast on the DCB algorithm. Since the DCB algorithm ensures each node is covered twice, the overhead with higher $x$ values is more noticeable.

Figure 8.7 and 8.8 explore the effect of directed broadcast on the SBA algorithm. As the SBA algorithm is a dynamic algorithm, the forwarding node does not know which nodes further into the network will be chosen as forwarding nodes. Consequently, the SBA algorithm has a much higher overhead at higher $x$ values. A $x$ value of 1 provides enough gains that higher $x$ values are not needed. Furthermore, since the SBA algorithm knows each neighbor’s location, the choice of neighbor to perform the directed broadcast with can be done to achieve better results. For instance, a neighbor that is extremely close is more likely to be in range if mobility exists in the network. Carrying out the directed broadcast is more likely to succeed, and neighboring nodes will still hear the transmission.

### 8.4.4 Dense Network Evaluation

All of the previous experiments were done in sparse networks, where the loss of a broadcast could potentially cause the NWB to fail. In this section, the effects of using Directed
Broadcast in a higher density scenario (50 nodes in the same area) are explored. In this case, it is expected that flooding will have higher redundancy and therefore higher tolerance to losses (but also high overhead). However, since AHBP and DCB attempt to eliminate redundancy, they are still vulnerable to losses.

Figure 8.9 contrasts the node coverage for flooding, DCB, and AHBP, as well as Directed Broadcast with AHBP. Figure 8.10 compares the overhead for those protocols. In this case, the coverage obtained by flooding is quite high; however, the overhead is high. For example, base AHBP has an overhead of only 40-50% that of flooding. With DB, the coverage of AHBP catches up with that of flooding at $x = 2$ – The overhead remains between 60% and 80% that of flooding.

The performance of DCB under dense scenarios also improves with DB. Note that the
performance of base DCB is significantly better than base AHBP in this case, since the higher density provides nodes in position to carry out double coverage. DCB with $x = 2$ overtakes the performance of flooding. However, the overhead of DCB is quite a bit higher than that of AHBP, and in fact, higher than flooding at $x = 2$.

8.5 Summary

This chapter presented a new MAC level primitive, Directed Broadcast, for improving NWB robustness. By making the MAC level broadcast a reliable transmission, existing NWB algorithms are greatly enhanced with respect to coverage and reliability. Many NWB algorithms utilize a CDS to cover nodes in the network. This approach yields an overhead far lower than the traditional flooding approach. However, a failure along a link of the CDS results in the NWB becoming unsuccessful. By combining DB with the CDS algorithms, the coverage of the NWB becomes successful in the presence of losses- on par with, or better than, the coverage of flooding. Furthermore, the overhead of the revised NWB algorithms is comparable to or lower than the overhead of flooding. The DB algorithms were shown to be successful both in sparse and dense networks.

This solution is one that uses explicit feedback. One node of the neighboring node set is chosen to send an ACK packet back upon successful reception of the NWB data. With this approach, the NWB obtains the reliability of unicast transmission, and also does not incur a high level of overhead or latency for NWB transmissions.
Chapter 9

Link-Quality Sensitive Connected Dominating Set NWB

Wireless communication properties make wireless transmissions unreliable for two primary reasons: (1) Collisions: the wireless channel is non-uniformly shared, giving rise to the well known hidden terminal problems [22]; and (2) Fading and obstacles can cause deep fades in signal power (20dB, or 100x changes in signal power are common). This leads to a large number of transmission errors, especially when the two communicating nodes are far from each other.

The solution presented in this chapter is in the class of fixed redundancy: rather than attempting to detect/predict losses and compensate for them, a fixed degree of redundancy is built into the NWB algorithm. In contrast, this work proposes a Link Quality sensitive Connected Dominating Set (LQ-CDS). LQ-CDS tracks the state of the links and uses that to determine how much redundancy to build in to provide sufficient safety margin for covering nodes. This work is most similar to Double Covered Broadcast (DCB) [52]. In DCB, recall that a CDS is constructed that covers each node at least twice. In contrast, LQ-CDS tracks the link quality and builds in redundancy in coverage that takes into account
this information. Thus, DCB may provide double coverage even to nodes that get covered with high quality links; LQ-CDS may find that a single transmission suffices in this case. Conversely, double coverage may not be sufficient if the two covering transmissions occur over poor quality links; LQ-CDS recognizes this case and builds in alternative coverage (either providing more redundancy or selecting rebroadcast responsibilities that avoid the weak links).

9.1 Background

Recall from Chapter 2, that for MANET study, different propagation models are used. One commonly used is the Two Ray Ground model. While used quite often for research, this model is not realistic, as it does not take the effects of signal fading into account.

The signal fading propagation model is a model that is more advanced than simplified models that are often used in simulations. The signal fading model takes into account the distance between two nodes and represents the received power of a packet as a random variable based on the distance [87].

Another important difference between the Two Ray Ground model and the signal fading model is the variation of chance of packet reception. In the Two Ray Ground model, assuming no interference, a packet will be successfully received if the receiving node is within transmission range of the sending node. With the signal fading model, the chance of a successful reception varies, depending on distance. In reality, the strength of a received packet fluctuates significantly, even at a constant distance [93, 94]. As the distance between two nodes is increased, the chance of a successful packet transmission is decreased. This difference in behavior is exhibited in Figure 9.1.

To improve reliability in the face of losses, MAC protocols like IEEE 802.11 [21] use retransmission of packets that are not acknowledged. Such an approach cannot be used
with broadcast packets because there are a number of receivers. Accordingly, if a broadcast packet is lost due to a collision, **the loss is not detected by the sender and no retransmission is carried out.** This makes MAC level broadcast operations much more susceptible to losses. As a result, operations which rely on MAC level broadcast suffer from loss of coverage.

For propagating data through a network, many algorithms based on CDS trees are used. These approaches build a virtual backbone that covers all nodes in the network. This backbone is a connected subset the nodes of the network from which all nodes in the network are one-hop reachable. If the CDS nodes broadcast, all the nodes in the network are covered. While finding the optimal CDS is NP-complete, algorithms have been developed to construct them distributedly, and near-optimally in terms of the size of the CDS and the overhead to construct it (e.g., [34, 35]).

An example of a CDS can be seen in Figure 9.2. The solid lines represent the virtual backbone of the network. The dashed lines represent paths taken by packets received as broadcasts from the nodes in the CDS tree. In this hypothetical network, if nodes $A$ and $B$ broadcast, all nodes in the network can receive the message being propagated through the network.

One problem that may occur in an environment with signal fading (or an environment
with heavy traffic) is that the quality of the links may be poor. Existing CDS algorithms view the link as a boolean value— it either is present or it is not. In reality, the link quality can vary with distance or with the amount of traffic near the sending or receiving node. For example, a few possible link quality values are superimposed on the sample CDS previously described in Figure 9.3. In this picture, the link between the two CDS nodes is poor, having a quality of 0.1, due to the distance between nodes $A$ and $B$. In contrast, the link between node $C$ and both nodes $A$ and $B$ is better, each having a quality of 0.6.
9.2 Link Quality Sensitive CDS

The signal fading propagation model has the effect of losing packets, especially if the nodes communicating are far away from each other. In the context of a CDS algorithm, the loss of MAC broadcast packets result in a coverage drop, and a potentially failed communication. Using a signal fading model, the probability of packet loss drops with the quality of the link and the distance between the nodes in free space.

The NWB algorithms presented earlier in this work are not aware of the effects of fading. Some solutions have incorporated this information into the protocols. For example, the Roofnet project [14] incorporates a metric called the Expected Transmission Count (ETX) [95], which is based on link loss ratios, potential asymmetry, and interference. When paths are built in the network, the sum of the ETX values for each link of the path are used as a gauge of the quality.

Microsoft has compared the ETX metric with other link quality metrics [96], and found that it has the best performance. They have derived a routing protocol called Link Quality Source Routing (LQSR) [15] which is part of their Mesh Connectivity Layer (MCL) software [97].

The solution presented here changes the problem of constructing a CDS in a MANET to one that attempts to covers all nodes with at least $P\%$ probability. To obtain neighbor knowledge, periodic exchange of ‘HELLO’ messages can be done, with the messages containing a list of known neighbors and their link qualities. The research presented here does not explore the assignment of link qualities in detail. Assuming an open network environment (no obstructions), one way link quality assignment can be done is to keep node location in the ‘HELLO’ packets, obtained through Global Positioning System (GPS) [98] information available at each node. Another approach is to keep track of a packet delivery ratio per node, as nodes with a high delivery ratio are more likely to be closer and are of
generally higher link quality. A third approach is to use timestamps in the ‘HELLO’ packets in order to track propagation delay. For this study, node locations are tracked with GPS information.

In realistic environments, the quality may be influenced by other factors besides the distance between nodes. For example, obstructions between the nodes, such as concrete walls, will influence the link quality. In practice, techniques that measure the signal to noise ratio of packet receptions or the transmission delivery ratio should be considered in link quality. The ETX metric presented earlier is an example of a metric which takes these into account [14, 95].

To estimate link quality in an environment with fading, a similar approach as used by others [99] has been taken. As the signal fading propagation model uses variation of received packet power, which fluctuates due to distance and fading effects, the computation of the link quality can be difficult. The assumption is made that each node has location information, obtained through GPS, and that the environment is free of obstructions. Having the location data, the following formula can then be used to estimate the link quality, based on distance:

\[
\text{Quality}(d) = \begin{cases} 
1 - \left(\frac{d}{R}\right)^{2\beta} & \text{if } d \leq R \\
\frac{(R - d)^{2\beta}}{2} & \text{otherwise}
\end{cases}
\]

In the above formula, \( d \) represents the distance between the two nodes, \( R \) represents the transmission distance, which varies depending on physical hardware and power used for transmitting, and \( \beta \) represents the ideal path loss in the system, as known in the signal fading model.

The aim of this solution is to achieve coverage of all nodes with some probability \( P \). In order to do this, a basic CDS would be built. When a node wishes to perform a broadcast
the following steps are done:

1. Find all 2 hop neighbors that are only reachable by a single node.
2. Mark those single nodes as broadcasting nodes.
3. While not all 2 hop neighbors are covered, add 1 hop neighbors that cover the remaining two hop neighbors with the best qualities.
4. For each 2 hop neighbor, examine all paths to it in the cover set. If the 2 hop neighbors have link qualities that result in a path probability less than $P$, add the one hop neighbor that has the highest link quality to the node as part of the broadcaster set.

For example, if 2 hops have link qualities of $x$ and $y$, the path quality is $(x)(y)$. The chance of path failure is $1 - ((x)(y))$. If the chance of the packet reaching the node via any path is below $P$, more paths have to be added.

To calculate the chance of a packet reaching the node along any path, the following approach can be used [100]: The chance of a packet reaching the destination along path $A_i$ is the product of the link qualities in that path. The product of the probabilities of reaching the destination along multiple paths is needed, and this can be denoted as:

$$p_i = P\{A_i\}, \quad p_{i,j} = P\{A_i A_j\} \quad ...$$

Furthermore:

$$S_1 = \Sigma p_i, \quad S_2 = \Sigma p_{i,j} \quad ...$$

where $i < j < k < ... \leq N$.

The chance of the packet being sent successfully along one of the $N$ paths to the destination is:

$$P = S_1 - S_2 + S_3 - S_4 + ... \pm S_N$$
This formula can then be reduced to:

\[ P = \sum_{i=1}^{N} (-1)^{i+1} S_i \]

Examining the CDS example shown earlier, the link between nodes A and C and nodes B and C can be leveraged, as shown in Figure 9.4. The path A – C – B has a quality of .6 * .6, or .36. By using both paths, the overall chance of a packet flowing from A to B is increased from .1 to .1 + .36 – (.1 * .36) or .424.

With this solution, group communication operations are made more reliable in a realistic environment. Signal fading is more likely to cause loss of packets at greater distances. Since CDS algorithms attempt to cover a large area with a minimum number of nodes, it is likely that those nodes will be at larger distances from each other. This solution is a fixed redundancy solution, which provides a way to counteract the effect of signal fading. By adding coverage based on link quality, the redundancy is increased where needed, but is not increased unnecessarily.
9.3 Experimental Evaluation

To provide a study of the problems encountered in a network with signal fading, the following static NWB algorithms are studied (previously presented in Chapter 5):

- Ad Hoc Broadcast Protocol (AHBP) [38]: Nodes track two hop neighbor and use this information to explicitly select a set of 1-hop neighbors to rebroadcast the packet such that all the 2-hop neighbors are covered. AHBP is a static CDS based approach.

- Double Covered Broadcast (DCB) [52]: This is a static topology-sensitive CDS-based algorithm with fixed built in redundancy (CDS developed to provide double-coverage for every node)

9.3.1 Preliminaries

The overhead required for the various ‘HELLO’ messages is not tracked. The reason this is omitted overhead is that it is not assessed per NWB but happens periodically. Thus, one round of neighbor discovery may benefit multiple NWBs.

The scenarios used were similar to those used in the NWB studies thus far; the scenario characteristics are summarized briefly here for readers’ convenience. In each topology, nodes were randomly deployed 30 nodes in a 1000 meter by 1000 meter area. 20 such topologies were used to obtain the results. In these scenarios, each packet has a fixed probability of being dropped during a transmission. This is representative of the effects of collisions as well as signal fading within the network. The effect of mobility were not considered in these experiments.

As with other NWB experiments in earlier chapters, in each experiment, one NWB is generated per node. The broadcasts are timed to ensure that successive NWBs do not interfere with each other. Each data point represents an average of 20 different simulation runs with 20 different scenarios (resulting in different topologies and source/destination
selection for interfering connections). While confidence intervals are not depicted, the number of scenarios was sufficient to have 95% confidence intervals be within 1% of the mean value across all measured values.

To create losses in the network, the signal fading propagation model is used. The pathloss exponent was set to 2.65, which is representative of a lightly shadowed urban area. The shadowing deviation was set to 7.5, which is in the middle of the outdoor range for the signal fading model [88].

### 9.3.2 Base Case

![Figure 9.5: Coverage](image1)

![Figure 9.6: Overhead](image2)

Figure 9.5 shows the coverage obtained by the NWB protocols in environments of varying densities. As expected, DCB has a higher coverage than AHBP. This behavior is expected, since the protocol tries to cover all nodes in the network with two broadcasts. As the density of the network increases, the overall coverage increases as well. The overhead for these scenarios can be contrasted in Figure 9.6. The overhead values have been normalized; that is, overhead is plotted for only the nodes that successfully received a NWB, not all nodes in the network. Since DCB attempts to cover all nodes with more broadcasts, it naturally has a higher overhead than AHBP. As the density of the network is increased, the overall cost of a NWB is lowered, as more nodes are covered per broadcasted packet. This
behavior is consistent with the patterns found in Chapter 5.

### 9.4 LQ-CDS Evaluation

![Figure 9.7: Coverage (30 Nodes)](image1)

![Figure 9.8: Overhead (30 Nodes)](image2)

Figures 9.7 and 9.8 show the coverage and overhead obtained for the LQ-CDS algorithm in a 30 node environment. Different coverage probabilities $P$ are listed along the X-axis. The values for AHBP and DCB are plotted as a reference. As expected, as $P$ is increased, the coverage obtained increases, along with the overhead.

![Figure 9.9: Coverage (60 Nodes)](image3)

![Figure 9.10: Overhead (60 Nodes)](image4)

Figures 9.9 and 9.10 plot the coverage and normalized overhead for the algorithm in a 60 node environment. Again, AHBP and DCB are plotted as reference markers. LQ-CDS algorithm has greater gains in denser scenarios, compared to the sparser 30 node scenarios.
Examining the data in detail, for small coverage probabilities (.2 or less), there is only a moderate gain with this algorithm, compared to AHBP. This is because the base AHBP algorithm builds a CDS that does cover all nodes with this low of a probability. Intuitively, this makes sense, as the nodes in the CDS tree are likely to be far away from each other, resulting in link qualities that are very low. The coverage and overhead of this algorithm starts out higher than that of AHBP due to the fact that in step 3 of the algorithm, as described earlier, nodes are chosen that cover remaining nodes with the best quality, rather than with quantity, as AHBP does. As the coverage probability approaches .4, the coverage increases moderately. This is the suggested $P$ value for this particular algorithm.

This algorithm, like AHBP and DCB, is a static algorithm. Nodes that are downstream from the source node are predetermined to be broadcasting nodes or not. As a result, the algorithm does not adapt as well to losses as a dynamic algorithm, like the Scalable Broadcast Algorithm (SBA) [40]. Furthermore, since the nodes require neighbor knowledge information, the coverage of the protocol is directly tied to the number of ‘HELLO’ messages received. If the ‘HELLO’ packets are lost, the resulting CDS built from neighbor knowledge can be incomplete, resulting in poorer coverage of the network as a whole.

The networks studied in this evaluation are relatively sparse and an aggressive signal fading model being used. Typically weak links (e.g., sub 50% are marked as bad and not used). A different model should be evaluated, with link qualities in a higher range (50%-95%), instead of the current model’s qualities of (0%-100%), with most being in the low range (the area in the low range is much larger than the area in the strong range (close to the transmitter). This also is why the differing values of $P$ do not make a large impact. The sparse 30 node experiments demonstrate these characteristics- there is not enough available redundancy in the network in order to obtain higher coverage.
9.5 Summary

The results shown in this chapter indicate that this algorithm performs well in both sparse and dense networks. When building new NWB algorithms, any increase in coverage must be balanced by maintaining a reasonable amount of overhead. Even though this algorithm increases overhead, it does so only minimally, with a moderate increase in coverage. Furthermore, in some NWB contexts such as routing, an increase in overhead can be considered worthwhile, since the results are important for network function and the operation occurs infrequently.

This solution is an example of a NWB algorithm that achieves robustness by tracking neighborhood state information such as neighbor link quality and providing a fixed level of redundancy. This approach requires no implicit or explicit feedback (only in tracking the state). By using the link quality to achieve a fixed level of redundancy, more nodes can be added into the CDS tree as appropriate, providing more coverage for weaker areas of the network, and less coverage for high quality areas of the network.
Chapter 10

Micro-Analysis

This chapter identifies and presents preliminary analysis and characterization of the second problem considered in this dissertation. More specifically, it is conjectured that the interference relationship between nodes have a defining effect on their performance in terms of fairness and efficiency. As a result, such interactions that occur in practice can play a role in the unpredictable unfairness problems that were observed in general scenarios. It can be noted that these interactions are typically not considered in the MAC fairness studies (previously overviewed in Chapter 3), which consider only the potential number of interfering senders, not the detailed relationships between them.

10.1 Overview and Methodology

It is extremely difficult to carry out a comprehensive analysis of interference relations in general scenarios, with interactions between potentially a large number of concurrent transmitters with complex time-dependent transitive interactions. Instead, in order to provide initial understanding of the possible interactions with controllable complexity, the arising interactions in a basic scenario with two interfering single-hop connections are studied.
These configuration are used for analysis of fairness and throughput. Eventually, all general scenarios translate to multiple hop connections that interfere with each other. Thus, an understanding of how two hops interact is basic to understanding the behavior of general scenarios. Furthermore, by isolating the problem to its most basic form, the analysis is simplified and it is easier to isolate interactions that cause problematic behavior.

In a MANET, the simplest connection is between two nodes. The evaluated networks use four nodes, two for each connection. For evaluation, the abbreviations $S_x$ for source $x$ and $D_x$ for destination $x$, where $x$ is the connection number are used. All simulations were performed using NS-2 [74]. The default transmission parameters were used, resulting in a transmission range of 250m and a carrier sense range of 550m. A two-ray ground propagation model was used, so no effects from shadowing were introduced. Each scenario was run with 20 different random seeds, and the results for each connection were averaged. The simulations were run for 450 seconds each after establishing routing and Address Resolution Protocol (ARP) lookup information. Routing information was cached for the life of the simulation to remove routing effects and allow us to focus on MAC interactions.

To generate traffic, Constant Bit Rate (CBR) applications were used. Unless otherwise stated, the CBR applications sent 1000 byte packets at a rate of 100 per second, in order to achieve a channel near saturation. CBR was used so that no side effects of TCP, such as the rate sending window, were introduced. The queue lengths at each node were marked as infinite so that no packets were dropped due to queue restrictions.

### 10.2 Experimental Study

Table 10.1 lists the scenarios used for testing. In this table, $S_1$ and $D_1$ refer to the source and destination of the first connection; $S_2$ and $D_2$ are the source and destination for the second connection. The different scenarios occur based on the relationship of the nodes
Table 10.1: Scenario Criteria

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Reception Range</th>
<th>Interference Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S1-S2, D1-D2</td>
<td>S1-D2, S2-D1</td>
</tr>
<tr>
<td>2</td>
<td>S1-D2, D1-S2</td>
<td>S1-S2, D1-D2</td>
</tr>
<tr>
<td>3</td>
<td>S1-S2, S1-D2, S2-D1, D1-D2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>S1-S2, S1-D2, S2-D1</td>
<td>D1-D2</td>
</tr>
<tr>
<td>5</td>
<td>S1-D2, S1-S2, D1-D2</td>
<td>S2-D1</td>
</tr>
<tr>
<td>6</td>
<td>D1-D2, D1-S2, D2-S1</td>
<td>S1-S2</td>
</tr>
<tr>
<td>7</td>
<td>D1-S2</td>
<td>S1-S2, D1-D2</td>
</tr>
<tr>
<td>8</td>
<td>S1-S2</td>
<td>D1-S2, S1-D2</td>
</tr>
<tr>
<td>9</td>
<td>D1-D2</td>
<td>S1-D2, D1-S2</td>
</tr>
<tr>
<td>10</td>
<td>S1-D2</td>
<td>D1-D2, S1-S2</td>
</tr>
<tr>
<td>11</td>
<td>None</td>
<td>D1-S2</td>
</tr>
<tr>
<td>12</td>
<td>None</td>
<td>S1-S2</td>
</tr>
<tr>
<td>13</td>
<td>None</td>
<td>D1-D2</td>
</tr>
<tr>
<td>14</td>
<td>None</td>
<td>S1-D2</td>
</tr>
</tbody>
</table>

of the two connections: (S1, S2), (S1, D2), (D1, S2) and (D1, D2). In each scenario, the table lists which node pairs are in reception range (approx. 0-250m apart) and which are in interference range (approx. 251–550m apart). Node pairs that are not listed (e.g., S1, D2 in scenario 7) are outside interference range. Of course, in all scenarios S1 and D1, as well as S2 and D2 are in reception range. Scenarios with similar properties are grouped together. For instance, scenarios 11 through 14 are all scenarios with nodes only in interference range. While the format for presenting results is awkward, a table is the best format for presenting a completely heterogeneous set of data.

It should be noted that these scenarios are a sampling of the possible ones and a full characterization of the arising relationships and their relative importance is intended in the final version of this work. In Section 11 the plan for carrying out this analysis is outlined.

To simulate these different scenarios, one connection was kept in the same place (connection 1), and the other connection was moved around it, forming different layout permutations. Each scenario is tried using the standard 802.11 MAC layer protocol, with and without the RTS/CTS handshake. In addition, the MILD backoff algorithm, which was
Table 10.2: Standard 802.11, RTS/CTS enabled, % potential packets sent successfully

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Conn. 1</th>
<th>Conn. 2</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.505</td>
<td>.506</td>
<td>.505</td>
</tr>
<tr>
<td>2</td>
<td>.510</td>
<td>.511</td>
<td>.510</td>
</tr>
<tr>
<td>3</td>
<td>.509</td>
<td>.510</td>
<td>.512</td>
</tr>
<tr>
<td>4</td>
<td>.509</td>
<td>.510</td>
<td>.509</td>
</tr>
<tr>
<td>5</td>
<td>.883</td>
<td>.126</td>
<td>.504</td>
</tr>
<tr>
<td>6</td>
<td>.510</td>
<td>.510</td>
<td>.510</td>
</tr>
<tr>
<td>7</td>
<td>.510</td>
<td>.510</td>
<td>.510</td>
</tr>
<tr>
<td>8</td>
<td>.505</td>
<td>.506</td>
<td>.505</td>
</tr>
<tr>
<td>9</td>
<td>.921</td>
<td>.014</td>
<td>.467</td>
</tr>
<tr>
<td>10</td>
<td>.510</td>
<td>.510</td>
<td>.510</td>
</tr>
<tr>
<td>11</td>
<td>.070</td>
<td>1.000</td>
<td>.534</td>
</tr>
<tr>
<td>12</td>
<td>.510</td>
<td>.511</td>
<td>.510</td>
</tr>
<tr>
<td>13</td>
<td>.999</td>
<td>.999</td>
<td>.999</td>
</tr>
<tr>
<td>14</td>
<td>1.000</td>
<td>.071</td>
<td>.535</td>
</tr>
</tbody>
</table>

devloped to address fairness issues is studied [58]. In MILD, the CW is multiplied by 1.5 (rather than doubling it) when a loss occurs, and is decreased by 1, rather than reset when a transmission is successful. The MILD algorithm is also run with and without the RTS/CTS handshake. The overall percentage of packets sent per connection, as well as the total overall percentage of packets sent in the scenario are tracked.

Figure 10.1: Part of trace for Scenario 5

Figure 10.2: Part of trace for Scenario 9
### Table 10.3: Standard 802.11, RTS/CTS disabled, % potential packets sent successfully

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Conn. 1</th>
<th>Conn. 2</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.541</td>
<td>.543</td>
<td>.542</td>
</tr>
<tr>
<td>2</td>
<td>.548</td>
<td>.548</td>
<td>.548</td>
</tr>
<tr>
<td>3</td>
<td>.531</td>
<td>.532</td>
<td>.532</td>
</tr>
<tr>
<td>4</td>
<td>.532</td>
<td>.532</td>
<td>.532</td>
</tr>
<tr>
<td>5</td>
<td>.942</td>
<td>.140</td>
<td>.541</td>
</tr>
<tr>
<td>6</td>
<td>.548</td>
<td>.548</td>
<td>.548</td>
</tr>
<tr>
<td>7</td>
<td>.548</td>
<td>.549</td>
<td>.548</td>
</tr>
<tr>
<td>8</td>
<td>.541</td>
<td>.543</td>
<td>.542</td>
</tr>
<tr>
<td>9</td>
<td>1.000</td>
<td>.001</td>
<td>.500</td>
</tr>
<tr>
<td>10</td>
<td>.541</td>
<td>.543</td>
<td>.542</td>
</tr>
<tr>
<td>11</td>
<td>.999</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>12</td>
<td>.549</td>
<td>.548</td>
<td>.548</td>
</tr>
<tr>
<td>13</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>14</td>
<td>1.000</td>
<td>.999</td>
<td>1.000</td>
</tr>
</tbody>
</table>

### Table 10.4: MILD, RTS/CTS enabled, % potential packets sent successfully

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Conn. 1</th>
<th>Conn. 2</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.496</td>
<td>.501</td>
<td>.498</td>
</tr>
<tr>
<td>2</td>
<td>.514</td>
<td>.493</td>
<td>.504</td>
</tr>
<tr>
<td>3</td>
<td>.501</td>
<td>.502</td>
<td>.502</td>
</tr>
<tr>
<td>4</td>
<td>.503</td>
<td>.502</td>
<td>.502</td>
</tr>
<tr>
<td>5</td>
<td>.973</td>
<td>.021</td>
<td>.497</td>
</tr>
<tr>
<td>6</td>
<td>.503</td>
<td>.503</td>
<td>.503</td>
</tr>
<tr>
<td>7</td>
<td>.504</td>
<td>.504</td>
<td>.504</td>
</tr>
<tr>
<td>8</td>
<td>.496</td>
<td>.501</td>
<td>.498</td>
</tr>
<tr>
<td>9</td>
<td>.332</td>
<td>.110</td>
<td>.221</td>
</tr>
<tr>
<td>10</td>
<td>.504</td>
<td>.504</td>
<td>.504</td>
</tr>
<tr>
<td>11</td>
<td>.026</td>
<td>.993</td>
<td>.510</td>
</tr>
<tr>
<td>12</td>
<td>.504</td>
<td>.503</td>
<td>.504</td>
</tr>
<tr>
<td>13</td>
<td>.474</td>
<td>.474</td>
<td>.474</td>
</tr>
<tr>
<td>14</td>
<td>.993</td>
<td>.026</td>
<td>.510</td>
</tr>
</tbody>
</table>

Table 10.3: Standard 802.11, RTS/CTS disabled, % potential packets sent successfully

Table 10.4: MILD, RTS/CTS enabled, % potential packets sent successfully


<table>
<thead>
<tr>
<th>Scenario</th>
<th>Conn. 1</th>
<th>Conn. 2</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.537</td>
<td>.541</td>
<td>.539</td>
</tr>
<tr>
<td>2</td>
<td>.551</td>
<td>.540</td>
<td>.545</td>
</tr>
<tr>
<td>3</td>
<td>.551</td>
<td>.529</td>
<td>.540</td>
</tr>
<tr>
<td>4</td>
<td>.543</td>
<td>.516</td>
<td>.530</td>
</tr>
<tr>
<td>5</td>
<td>.955</td>
<td>.119</td>
<td>.537</td>
</tr>
<tr>
<td>6</td>
<td>.545</td>
<td>.545</td>
<td>.545</td>
</tr>
<tr>
<td>7</td>
<td>.545</td>
<td>.546</td>
<td>.545</td>
</tr>
<tr>
<td>8</td>
<td>.537</td>
<td>.541</td>
<td>.539</td>
</tr>
<tr>
<td>9</td>
<td>.397</td>
<td>.084</td>
<td>.241</td>
</tr>
<tr>
<td>10</td>
<td>.546</td>
<td>.545</td>
<td>.545</td>
</tr>
<tr>
<td>11</td>
<td>.309</td>
<td>.620</td>
<td>.464</td>
</tr>
<tr>
<td>12</td>
<td>.545</td>
<td>.545</td>
<td>.545</td>
</tr>
<tr>
<td>13</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>14</td>
<td>.601</td>
<td>.331</td>
<td>.466</td>
</tr>
</tbody>
</table>

Table 10.5: MILD, RTS/CTS disabled, % potential packets sent successfully

Figure 10.3: Part of trace for Scenario 11

Figure 10.4: Part of trace for Scenario 14

10.3 Fairness

Examining Table 10.2, it can be seen that the standard 802.11 implementation, using BEB and RTS/CTS, is generally fair, in that each node got an equal share of the wireless medium. There were 4 scenarios that yielded unfair results (all of which were not symmetrical):

- Scenario 5: Unfairness was due to CSMA, as node D2 is in range with node S1. Few collisions (less than 1%) were recorded and it is not believed that these play a role in the unfairness. A partial trace can be seen in Figure 10.1. In this trace, Node 0 is
S1, Node 1 is D1, Node 2 is S2, and Node 3 is D2. It can be seen in this trace that collisions are not a factor, because no drops are recorded in this segment of trace. Around time 70.09, Connection 2 manages to obtain the medium after being blocked out for much of the time before then.

- Scenario 9: Unfairness is due to the two source nodes being out of interference range from each other. As a result, packets are sent in towards the destination nodes, and each source interferes with the other destination node causing uncontrolled collisions. Since the scenario is not symmetrical, it is understandable that the throughputs are not equal. A partial trace can be seen in Figure 10.2. This result is similar to Xu and Saadawi’s conclusions that the BEB promotes unfairness with larger packet sizes and large number of packets to send [8].

- Scenario 11: Drops at D1 were due to interference on the received RTS packets. Most RTS packets were received while a CBR packet was being sent on Connection 2. As D1 is within range of interference from S2, the RTS packet is dropped at Node 1, and Connection 1 can not send successfully. A partial trace showing this interaction can be seen in Figure 10.3.

- Scenario 14: Drops at D2 were due to interference on the received RTS packets. This scenario is similar to Scenario 11. Most RTS packets for the second connection were received while a CBR packet was being sent on Connection 1. As D2 is within range of interference from S1, the RTS packet is dropped at Node 3. A partial trace showing this activity can be seen in Figure 10.4.

In Table 10.3, it can be noted that turning off the RTS/CTS handshake solves the fairness problems of scenarios 11 and 14 (which were RTS related). It also does not cause any other fairness problems. Using the backoffs presented in the MILD algorithm, Table 10.4 shows that the unfairness issues presented above are not solved – that is, MILD does not
provide fairness in all cases. Examining Table 10.5, indicates that turning off the RTS/CTS handshake with the MILD algorithm aids the fairness issues in Scenarios 5, 11, and 14.

10.4 Throughput

Comparing Tables 10.2 and 10.3, one can see the effect of the RTS/CTS mechanism on throughput. Only one connection of the 28 fares worse with RTS/CTS disabled (connection 2 of Scenario 9). The overall throughput of all scenarios goes up with RTS/CTS disabled. Furthermore, the throughput of Scenarios 11 and 14 go up substantially.

Comparing this with the MILD data, it can be seen from Tables 10.4 and 10.5 that only 2 of the 28 connections do worse with the RTS/CTS handshake disabled, and only two of the scenarios have worse overall throughput. MILD causes a drop in performance relative to BEB, that can be severe in some cases. Overall, the scenarios with disabled RTS/CTS have a throughput gain of about 17 percent. As these scenarios are not representative of an entire network, this number is slightly inflated. A general network environment is studied later on.

10.5 Effect of Packet Size

Simulations of previous tests were done using packet sizes of 100 and 500 bytes (increasing the sending rate of the CBR connections proportionally). For clarity, these results are not presented in a tabular format. Using the data from above, the 1000 byte packets had a throughput increase of approximately 15 percent by turning off RTS/CTS. The 500 byte packet scenarios had a throughput increase of approximately 24 percent, while the 100 byte packet test runs increased throughput by nearly 49 percent. The overall fairness charts presented above kept the same pattern with both the 500 byte packet runs and the 100 byte
10.6 Collision Analysis

Since the RTS/CTS handshake is intended to alleviate some collisions in the network, an analysis was performed of the collisions in the micro-level scenarios, with and without the RTS/CTS handshake. Collisions were not a factor in Scenarios 1-2, 6-8, 10, or 12. In Scenarios 3-5, the non-RTS/CTS results had a comparable number of collisions on the CBR data packets as there were with the RTS packets in the RTS/CTS results. In Scenario 9, the non-RTS/CTS results had one collision for approximately every two RTS packet collisions. In Scenarios 11 and 14, the non-RTS/CTS results had one collision for every 14 RTS packet collisions. In Scenario 13, the non-RTS/CTS results had no collisions, while the RTS/CTS results had a small amount. Collision ratios with smaller packet sizes were similar, but slightly lower.

10.7 General Scenario Applicability

Since turning off the RTS/CTS handshake provided large gains in micro-level scenarios, a study of this effect was warranted in larger and more general networks. 20 general topologies were created with 30 nodes placed randomly in a 1000m by 1000m area, with CBR connections of varying lengths. By using random scenarios, the micro-level scenarios that occur most often will be implicitly tested more often. Calculations indicate that the overall throughput gain from turning off the RTS/CTS handshake was around 7%. Further studies need to be done to fully evaluate how the RTS/CTS handshake impacts performance with general networks, as well as specialized networks such as grids and chains.

Examining the basic 802.11 behavior, one can see that it is fair in many scenarios (4
scenarios were the exception). Furthermore, more fairness is achieved simply by turning off the optional RTS/CTS handshake. Changing how the CW is adjusted does not solve the fairness problems observed. Changing the CW adjustment only lowers the average throughput. The throughput of the simulations is better with the RTS/CTS handshake turned off as well. This is for two reasons. First, there is less overhead, since the handshake packets do not need to be in the network. Second, nodes do not need to be silent during the CTS/DATA/ACK period, so their throughput can be higher. These observations held true for packet sizes of 100, 500, and 1000 bytes.

With micro-level scenarios, there were only 4 scenarios that could be considered problematic, in that the wireless medium was not being shared evenly or throughput was not as high as it could potentially be. It was noted that turning off the RTS/CTS handshake aided many of the fairness problems in these shapes, and also increased the throughput.

### 10.8 Enumerating Interaction Cases

As the information presented in earlier indicates, there is knowledge that can be gained by studying Mobile Ad hoc Networks (MANETs) at a very basic level. The data presented in this chapter dealt with 14 specific configurations. It ignored capture effects and considered only a subset of the possible scenarios. In reality, there are many more potential configurations that can occur with two single hop connections.

The types of node interactions of interest are:

1. Carrier sense range: Transmissions from a node in this range can be sensed by the node being studied.

2. Transmission range: Transmissions from a node in this range can be received successfully, assuming no collisions occur.
3. Capture: When two or more nodes are within transmission range and they transmit simultaneously, the node being studied may receive one of the packets, or no packets, depending on the power of the received packet (which varies by distance). This behavior results in a matrix of boolean values, with the diagonal being of non-interest.

Given a network with 4 nodes, the relationship between transmitter and receiver for each pair is defined: they are within transmission range of each other. The relationship of the each node to the other two nodes with respect to its primary link is what defines the interactions that occur. It is assumed that at least one node of each pair must be within carrier sense range of the other pair; otherwise the two connections do not interact. Interference occurs when the signal to noise and interference power (SINR) drops below the capture threshold. In a given configuration each node may have:

1. There are 1 to 3 nodes within carrier sense range.

2. There are 1 to \(x\) nodes within transmission range. This number has an upper bound related to the carrier sense range number. For example, if there are 2 nodes within carrier sense range, there can be at most 2 nodes within transmission range.

3. A capture matrix of varying size. The capture matrix is a representation of which packet will be received correctly if two nodes transmit at the same time. The capture matrix contains \(2^{x^2-x}\) different possibilities of capture, where \(x\) is the number of nodes within transmission range.

Examining these properties for a single node yields 75 possible combinations. Furthermore, since these properties are for a single node, and there are 4 nodes in the network, the number of configurations is much higher.

To analyze these configurations, a study was done with 4 nodes. Node S1 (Source 1) was kept in a fixed position, while node D1 (Destination 1) was placed at the same X
coordinate, and moved incrementally away along the Y axis. Nodes S2 and D2 were kept within transmission range of each other and moved around the X and Y axis in a semi-circle around nodes S1 and D1. By moving in a semi-circle, half of the configurations were studied, with the other half being a mirror image. The first connection was kept in the same X coordinate, as the configurations made by moving in the X coordinate can also be created by rotating one of the already studied networks.

![Image](image.png)

**Figure 10.5:** Counts of snapshot occurrences by increment

The snapshots of a network were created by using the algorithm described above with different values for movement of the nodes. These increments varied from 5 to 100 meters, by 5 meters each. A tally of the total number of different configurations found per increment can be seen in Figure 10.5. As expected, as the increment is decreased, the number of scenarios found increases.

Despite the high number of scenarios found, the majority of these scenarios only occur a small portion of the time. These scenarios tend to deal with the different permutations of the capture matrix, described earlier. Figure 10.6 depicts the different scenarios with the number of times they occur in a 100m increment. In this study, there were 238 different configurations. Of these, 220 occurred less than 10% of the time, and 136 of them had only one occurrence.

A similar trend can be seen in the study of the scenarios in a 5 meter increment. Fig-
Figure 10.6: Snapshot occurrences, 100m increment

Figure 10.7: Snapshot occurrences, 5m increment

Figure 10.7 charts the scenarios with their tally of occurrences. Again, a majority occur fairly infrequently. It should be noted that these counts do not consider mirror images of a snapshot to be the same configuration. For example, if one configuration has the first connection interfering with the second connection in the same way that the second configuration has the second connection interfering with the first, they are treated as distinct network configurations. Similarly, as the destination nodes occasionally must transmit data, such as sending an acknowledgement (ACK) packet, mirror images involving the sources and the destinations are treated distinctly.

10.9 Summary

This chapter presented a sampling of the potential inter-relations of two single hop connections in a MANET. The behavior of the 802.11 MAC was shown to be generally fair, except for a few specific situations. The MILD algorithm was run in these scenarios, and it was shown that this algorithm did not correct the fairness problems. Moreover, the MILD algorithm resulted in a lower throughput in the network. The effect of the RTS/CTS handshake was shown to exacerbate the unfairness in the network, as well.
Chapter 11

Future Work

This section outlines some future research related to the problem of unreliability in congested Mobile Ad hoc Networks (MANETs). It should be noted that the solutions presented in this work are merely a first step in increasing reliability and throughput in congested MANETs. Potential future research activities, which can build upon this work, are as follows:

1. Development of more sophisticated algorithms to counter signal fading: As found in Chapter 5, dynamic Connected Dominating Set (CDS) algorithms adapt to losses in a Network Wide Broadcast (NWB) better than static algorithms such as Link Quality sensitive CDS do. Work can be done to adapt the dynamic Scalable Broadcast Algorithm (SBA) [40] to make it link-quality aware. Further studies on link quality estimation can also be performed, allowing other relevant data, such as traffic patterns, to influence the quality of the link.

2. Ensuring that all the micro-level scenarios at the Medium Access Control (MAC) level are addressed and evaluate their relative importance: As Chapter 10 explained, there are numerous permutations of a network with two single-hop connections. The scenarios that occur most often should be analyzed, with particular emphasis on
problems due to collision, capture, or interference. Once these scenarios are characterized, more study can be done to determine whether or not unfairness issues are present.

3. Consideration of the problem of generalizing the microanalysis to more complex settings: As having two single hop connections in a MANET is an unlikely situation, the micro-analysis should start to become more generalized for complex configurations. The first logical study is that of a single two hop connection. In this configuration, the middle node serves as both a sending and receiving node, so a study of the interactions with different topologies can be beneficial. Other potential layouts include chains and grids, although it may be difficult to fully quantify the behavior in a general manner.

4. Consideration of the problem of formulating fair access algorithms that are sensitive to the underlying causes of the problematic scenarios: Once the problematic scenarios have been identified by the processes described above, potential solutions can be described. For instance, topographies may be identifiable by exchanging ‘HELLO’ packets with location information. Once a node identifies that it is in a problematic scenario, it can adjust its MAC protocol parameters to allow fairness in the network. Potential parameters that could be adjusted are its sending rate and whether or not Request to Send/Clear to Send (RTS/CTS) packets are used.

5. Other potential solutions for problematic scenarios: If a node detects that it is in a configuration that prohibits fair access to the wireless medium, the MAC layer may be adjusted to change the access algorithm used to obtain access to the channel. In addition, the information about the topology may be fed to the routing protocol, in order to avoid links that interact destructively.
Chapter 12

Conclusion

This work examined the underlying issues affecting Mobile Ad hoc Networks (MANETs) in scenarios with high loads and/or losses. Two key problems were identified in the study of why MANETs had poor performance in straining environments: (1) Network-Wide Broadcasts (NWBs) are unreliable; (2) Fairness issues arise depending on nodes geographic locations with respect to one another.

NWBs are important operations in MANETs and are used in several routing and group communication algorithms. Existing research has targeted efficient NWB to reduce the amount of redundancy inherent in flooding (the simplest NWB approach). As a result, the NWB becomes more susceptible to loss of coverage due to transmission losses that result from heavy interference or transmission errors. This problem arises because NWBs rely on an unreliable MAC level broadcast operation to reach multiple nodes with one transmission for a more efficient coverage of the nodes. In the presence of interference or transmission errors, this results in nodes not receiving the NWB.

The reliability of NWBs was studied in detail. The existing solution space was outlined, and the effectiveness and relative cost of existing NWB algorithms was examined. The potential solution space for NWB robustness was examined in detail, and three solutions
representing different approaches were presented.

In the first solution, Selective Additional Rebroadcast (SAR), NWB algorithms are modified by having nodes optionally rebroadcast a packet a second time. This additional rebroadcast can be based on a simple heuristic such as a random probability or a counter representing the number of times a NWB was heard. Adaptive solutions for existing NWB protocols were evaluated, yielding significant increases in coverage with large increases in overhead. This solution is one that uses implicit feedback, as no extra transmissions are required for the transmitting node to learn about the success of a NWB.

In the second solution, Directed Broadcast (DB), a new MAC level primitive is introduced to send NWBs. Nodes wishing to send a NWB use neighbor knowledge and perform a Request to Send/Clear to Send (RTS/CTS) handshake with a neighbor. When the data packet is sent, neighboring nodes not involved in the handshake treat the data packet as if it was a broadcast packet, rather than discarding it as they would for a standard unicast packet. Besides adding the handshake to gain access to the wireless medium, this approach also adds in a recovery algorithm found in unicast transmissions, where up to seven attempts are made in order to send the data packet. A MAC level broadcast packet uses only one attempt, and if the packet is lost, the MAC layer is not informed, and will not attempt to resend the packet. By leveraging the acknowledgement (ACK) packet that is present in unicast transmissions, DB is a solution that uses explicit feedback. Nodes involved in the DB CDS tree send ACK packets to indicate the NWB was received successfully.

In the third solution, Link-Quality sensitive Connected Dominating Set (LQ-CDS), a CDS is built to cover all of the nodes in the network using link qualities based on shadowing. This allows nodes to be covered with some probability $p$, which is obtained by adding links in the CDS to ensure nodes are covered strongly enough. Existing NWB algorithms do not take shadowing into account, and all links between nodes are treated equally. This solution is one that does not use either implicit or explicit feedback, but instead makes use
of other knowledge, such as the quality of links in the network.

Fairness due to links’ low level interactions with other links has not previously been studied. This dissertation introduced topographic analysis done at a micro-level between two single hop connections. This work was shown to be different from the existing fairness studies that are well known in the MANET community today. By not taking a “black box” approach, there is a greater chance to fully understand how ad hoc networks behave. This micro analysis presented initial work in quantifying how a MANET behaves by removing variables such as the routing layer, packet queues, and TCP. Two single hop connections were studied in various configurations to determine potential throughput and interference. Plans for future studies, such as a single two hop connection and chain configurations were mentioned.

Addressing these issues allows high load MANETs to become more robust. As there are many variables present in a MANET, this work is just a first step in making them tolerate high levels of traffic. However, since NWBs are a key component in both routing and group communication protocols such as multicast, increasing their reliability is critical in order to sustain high traffic loads. Similarly, fairness issues related to node location must be understood in order to develop protocols that perform well in all node topographies. The research presented in this work will aid in these efforts.
A. Topology Samples

Figure A.1: 30 nodes

Figure A.2: 40 nodes

Figure A.3: 50 nodes

Figure A.4: 60 nodes
Figure A.5: 5x5 grid

Figure A.6: 6x6 grid

Figure A.7: 7x7 grid

Figure A.8: 8x8 grid

Figure A.9: Cluster
B. Micro-Analysis Layouts

Figure B.1: Scenario 1
Collision Range: S1-S2, D1-D2
Interference Range: S1-D2, S2-D1

Figure B.2: Scenario 2
Collision Range: S1-D2, D1-S2
Interference Range: S1-S2, D1-D2

Figure B.3: Scenario 3
Collision Range: S1-S2, S1-D2, S2-D1, D1-D2

Figure B.4: Scenario 4
Collision Range: S1-S2, S1-D2, S2-D1
Interference Range: D1-D2
Figure B.5: Scenario 5
Collision Range: S1-D2, S1-S2, D1-D2
Interference Range: S2-D1

Figure B.6: Scenario 6
Collision Range: D1-D2, D1-S2, D2-S1
Interference Range: S1-S2

Figure B.7: Scenario 7
Collision Range: D1-S2
Interference Range: S1-S2, D1-D2

Figure B.8: Scenario 8
Collision Range: S1-S2
Interference Range: D1-S2, S1-D2

Figure B.9: Scenario 9
Collision Range: D1-D2
Interference Range: S1-D2, D1-S2

Figure B.10: Scenario 10
Collision Range: S1-D2
Interference Range: D1-D2, S1-S2

Figure B.11: Scenario 11
Interference Range: D1-S2

Figure B.12: Scenario 12
Interference Range: S1-S2
Figure B.13: Scenario 13
Interference Range: D1-D2

Figure B.14: Scenario 14
Interference Range: S1-D2
C. Curriculum Vitae

Conferences

- Robustness of Network-Wide Broadcast in MANETs. Paul Rogers and Nael Abu-Ghazaleh. Accepted to MASS 2005.
- Route Compaction for Directional Route Discovery in MANETs. Vinay Kolar, Paul Rogers, and Nael Abu-Ghazaleh. Accepted to WiMob 2005.

Technical Reports


Papers in Progress

- Enhanced CDS Coverage in MANETs. Paul Rogers and Nael Abu-Ghazaleh.
D. Bibliography


