ABSTRACT

Title of dissertation: EFFICIENT CROSS LAYER DESIGNS FOR IEEE 802.11 WIRELESS NETWORKS

Tamer Nadeem, Doctor of Philosophy, 2006

Dissertation directed by: Professor Ashok Agrawala
Department of Computer Science

Various properties of wireless networks, such as mobility, frequent disconnections and varying channel conditions, have made it a challenging task to design networking protocols for wireless communications. In this dissertation, we address several problems related to both the routing layer and medium access control (MAC) layer in wireless networks aiming to enhance the network performance. First, we study the effect of the channel noise on the network performance. We present mechanisms to compute energy-efficient paths in noisy environments for ad hoc networks by exploiting the IEEE 802.11 fragmentation mechanism. These mechanisms enhance the network performance up to orders of magnitude in terms of energy and throughput. We also enhance the IEEE 802.11 infrastructure networks with a capability to differentiate between different types of unsuccessful transmissions to enhance the network performance. Second, we study the effects of the physical layer capture phenomena on network performance. We modify the IEEE 802.11 protocol in a way to increase the concurrent transmissions by exploiting the capture phenomena. We analytically study the potential performance enhancement of our mechanism over the original IEEE 802.11. The analysis shows that up to 35%

of the IEEE 802.11 blocking decisions are unnecessary. The results are verified by simulation in which we show that our enhanced mechanism can achieve up to 22% more throughput. Finally, we exploit the spatial reuse of the directional antenna in the IEEE 802.11 standards by developing two novel opportunistic enhancement mechanisms. The first mechanism augments the IEEE 802.11 protocol with additional information that gives a node the flexibility to transmit data while other transmissions are in its vicinity. The second mechanism changes the access routines of the IEEE 802.11 data queue. We show analytically how the IEEE 802.11 protocol using directional antenna is conservative in terms of assessing channel availability, with as much as 60% of unnecessary blocking assessments and up to 90% when we alter the accessing mechanism of the data queue. By simulation, we show an improvement in network throughput of 40% in the case of applying the first mechanism, and up to 60% in the case of applying the second mechanism.

EFFICIENT CROSS LAYER DESIGNS FOR IEEE 802.11 WIRELESS NETWORKS

by

Tamer Nadeem

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2006

Advisory Committee:

Professor Ashok Agrawala, Chair/Advisor
Professor Eyad Abed, Dean's Representative
Professor Raymond Miller
Professor A. Udaya Shankar
Professor Aravind Srinivasan
Dr. Jonathan Agre

to my loving parents and my two brothers

ACKNOWLEDGMENTS

I owe my gratitude to Allah and then all the people who have made this dissertation possible and because of whom my graduate experience has been one that I will cherish forever.

First and foremost I would like to thank my adviser, Professor Ashok Agrawala for giving me an invaluable opportunity to work on challenging and extremely interesting projects over the past years. He patiently guided me throughout my research career at UMD and always found time whenever I needed an intelligent discussion. I am also too thankful for giving me a chance to be part of MINDLab where I participated in several projects. Being part of it enabled me to collaborate with fellow students and work as a team.

I owe my deepest thanks to my family - my parents who have always stood by me and guided me through my career, and have pulled me through against impossible odds at times. Words cannot express the gratitude I owe them. I would also like to thank my two brothers for always being there for me.

I thank each one of my committee members for their valuable comments and feedbacks. I am grateful to Professor Raymond Miller for his helpful academic advices since my first year. His knowledge and experience in the network protocol field is insurmountable. Professor Liviu Iftode shared his expertise in distributed computing and pervasive computing. I was fortunate to work with him closely in several interesting projects. I also thank Dr. Jonathan Agre for the chance he gave me to work closely with Fujitsu Labs during my last year at UMD. I would like to thank my former advisors in Alexandria University; Professor Mohamed Ismail, Professor Mohamed Nazeeh, and Professor Badr Abu-Elnasr for their continuous support. I was fortunate to work with unbelievably talented individuals. Collaborating and writing papers with Professor Liviu Iftode, Professor Raymon Miller, Dr. Jonathan Agre, Professor Suman Banerjee, Dr. Lusheng Ji, and Dr. Chenxi Zhu were precious experiences. I am also grateful to the department staff members.

My friends have been a crucial factor in my finishing smoothly. The friendship I have with them is what kept me going on during the tough times. I would like to express my gratitude especially to Tamer Elsharnouby and Khaled Arisha for their friendship and support. I would also like to thank my friends Hisham Abdallah, Mohamed Abdallah, Mohamed Abdelaal, Ahmed Abdel Hafez, Abdel Hameed Badawy, Hatim Diab, Mona Diab, Tamer Elbatt, Mahmoud Elfayoumy, Ahmed Elgammal, Ashraf Elmasry, Mohamed Elmohandes, Eiman Elnahrawy, Mohamed Tamer Elrefae, Gehad Galal, Tarek Ghanem, Walid Gomaa, Mohannad Hazem, Yaser Jaradat, Zaki Sharbash, Ahmed Tolba, Adel Yousef, Moustafa Yousef, and Norann Zaghloul.

Thanks Allah and thank you all!

TABLE OF CONTENTS

1 Introduction **1**

1.1 Characteristics of Wireless Network 2

1.2 Cross-Layer Design 4

1.3 Contributions of the Dissertation 5

1.3.1 Wireless Networks in Noisy Environments 5

1.3.2 Physical Layer Capture Effect 6

1.3.3 Directional Antennas 7

1.4 Structure of the Dissertation 8

2 Background **9**

2.1 IEEE 802.11 Standard 9

2.1.1 IEEE 802.11 Distributed Coordination Function (DCF) 10

2.1.2 IEEE 802.11 Fragmentation 13

2.2 Radio Propagation Model 14

2.2.1 Free Space/Two-ray Propagation Model 15

2.2.2 Capture Effect 15

2.3 Directional Antenna 17

3 Efficient Ad Hoc Routing Protocols in Noisy Environments **20**

3.1 Related Work 24

3.2 Wireless Link Error Rates 26

3.3 Optimal Fragment Size for Energy Efficient Paths 29

3.4 AODV and its Proposed Modifications 33

3.4.1 Link Error Rates Estimation 35

3.4.2 Messages and Structures of AODV 36

3.4.3 Route Discovery 38

3.5 Performance Evaluation 43

3.5.1 Network Topology and Link Error Modeling 46

3.5.2 Metrics 48

3.5.3 Static Grid Topologies 49

3.5.4 Static Random Topologies 57

3.5.5 Mobile Topologies 57

3.6 Conclusion 67

4 Analyzing and Enhancing the IEEE 802.11 DCF in Noisy Environments 69
4.1 Related Work 70
4.2 Markov Chain Model of the IEEE 802.11 DCF in Noisy Environment . . 71
4.3 Model Validation 75
4.4 $smart_{BEB}$: Enhanced IEEE 802.11 MAC 80
4.5 Implementation of $smart_{BEB}$ Mechanism 81
4.5.1 RTS/CTS Access Mode 81
4.5.2 Basic Access Mode 83
4.6 IEEE 802.11 fairness in Noisy environments 85
4.6.1 Conclusion 89

5 LED: Location Enhancement for the IEEE 802.11 Distributed Coordination Function 90
5.1 Related Works 92
5.2 Performance of Capture Effect in 802.11 Networks 95
5.2.1 Inefficiency of Carrier Sense Mechanism 97
5.2.2 Probability of Non-interfering Transmission 100
5.3 Location Enhanced DCF Protocol 105
5.3.1 Protocol Overview 106
5.3.2 Physical Layer Design 108
5.3.3 MAC Layer Design 114
5.4 Performance Evaluation 119
5.4.1 Simulation Environment 120
5.4.2 Impact of Node Density 125
5.4.3 Impact of Network Load 129
5.4.4 Impact of Network Degree 133
5.4.5 Capture Factor β 135
5.4.6 Impact of Errors in Node Locations 138
5.4.7 Impact of Transmission and Carrier Sense Ranges 139
5.4.8 Experimenting with Infrastructure Networks 142
5.5 Conclusion 144

6 Opportunistic Mechanisms for IEEE 802.11 Networks using Directional Antennas I: Opportunistic Carrier Sense Transmission 145
6.1 Related Works 147
6.2 Problem Formulation 149
6.3 Analysis of Blocking Probabilities with OPP_{CS} 152
6.3.1 Model Assumption 152
6.3.2 Analysis of OPP_{CS} Probability 153
6.3.3 Verification of OPP_{CS} Model 156
6.4 Implementation of OPP_{CS} 158
6.4.1 Physical Layer Design 159
6.4.2 MAC Layer Design 160
6.5 Performance Evaluation 165

6.5.1 Impact of Network Degree 170
6.5.2 Impact of network load 171
6.5.3 Impact of Beamwidth Size 174
6.5.4 Impact of Transmission and Carrier Sense Range 178
6.6 Conclusion 179

7 Opportunistic Mechanisms for IEEE 802.11 Networks using Directional Antennas II: Opportunistic Head-of-Line Transmission 180
7.1 Problem Formulation 181
7.2 Analysis of Blocking Probabilities with OPP_{HOL} 181
7.2.1 Analysis of OPP_{HOL} Probability 182
7.2.2 Verification of OPP_{HOL} Model 183
7.3 Implementation of OPP_{HOL} 186
7.3.1 Physical Layer Design 186
7.3.2 MAC Layer Design 186
7.4 Performance Evaluation 189
7.4.1 Impact of Network Degree 192
7.4.2 Impact of network load 197
7.4.3 Impact of Beamwidth Size 199
7.4.4 Impact of Transmission and Carrier Sense Range 201
7.5 Conclusion 201

8 Conclusion and Future Works 203

Bibliography 207

LIST OF TABLES

3.1 MAC and PHY system parameter. 27
3.2 The parameter values used in simulation in addition to the standards values defined in [9]. 45

4.1 MAC and PHY system parameter. 79

5.1 Different transmission powers and their corresponding ranges used by ns-2. 138

7.1 The average and maximum values of $CountNH$ and $StarvTime$ for number of connections. 193
7.2 The average and maximum values of $CountNH$ and $StarvTime$ for different beamwidth sizes. 198

LIST OF FIGURES

2.1 IEEE 802.11 DCF Mechanism 11
2.2 RTS/CTS with fragmented packet 13
2.3 Ideally-sectorized model of directional antenna 18

3.1 Bit Error Rates for different Noise and Distance values using Equations 3.1 and 2.1. The parameter values in those equations are defined in Table 3.2. 27
3.2 Normalized energy consumption for each transmitted bit using different fragment sizes over wireless link using Equation 3.4 where $o_1 = 250bits$, $o_2 = 300bits$, and $v = 1unit$ 31
3.3 The 49-node grid topology. The shaded region marks the maximum transmission range for the node, A. $A \rightarrow B$ is one of the example flows used on this topology. 46
3.4 Effective reliable throughput for UDP flows, Grid Topology in Fixed Noise Environments 49
3.5 Average energy cost for UDP flows, Grid Topology in Fixed Noise Environments 50
3.6 Effective reliable throughput for UDP flows, Grid Topology in Random Noise Environments 52
3.7 Average energy cost for UDP flows, Grid Topology in Random Noise Environments 52
3.8 Effective reliable throughput for TCP flows, Grid Topology in Fixed Noise Environments 53
3.9 Average energy cost for TCP flows, Grid Topology in Fixed Noise Environments 54
3.10 Average number of hops/flow, Grid Topology in Fixed Noise Environments 55
3.11 Average number of hops/flow, Grid Topology in Random Noise Environments 55
3.12 Average path lifetime, Grid Topology in Fixed Noise Environments . . . 56
3.13 Average path lifetime, Grid Topology in Random Noise Environments . . 57
3.14 Effective reliable throughput for UDP flows, Random Topology in Fixed Noise Environments 58
3.15 Average energy cost for UDP flows, Random Topology in Fixed Noise Environments 58
3.16 Effective reliable throughput for UDP flows, Random Topology in Random Noise Environments 59

3.17 Average energy cost for UDP flows, Random Topology in Random Noise Environments . . . 59
3.18 Average number of hops per flow, Random Topology in Fixed Noise Environments . . . 60
3.19 Average number of hops per flow, Random Topology in Random Noise Environments . . . 60
3.20 Effective reliable throughput for UDP flows, Mobile Topology in Fixed Noise Environments . . . 61
3.21 Average energy cost for UDP flows, Mobile Topology in Fixed Noise Environments . . . 61
3.22 Effective reliable throughput for UDP flows, Mobile Topology in Random Noise Environments . . . 62
3.23 Average energy cost for UDP flows, Mobile Topology in Random Noise Environments . . . 62
3.24 Effective reliable throughput for TCP flows, Mobile Topology in Random Noise Environments . . . 64
3.25 Average energy cost for TCP flows, Mobile Topology in Random Noise Environments . . . 64
3.26 Average number of hops/flow, Mobile Topology in Fixed Noise Environments . . . 65
3.27 Average number of hops/flow, Mobile Topology in Random Noise Environments . . . 66
3.28 Average path lifetime, Mobile Topology in Fixed Noise Environments . . . 66
3.29 Average path lifetime, Mobile Topology in Random Noise Environments . . . 67

4.1 Markov Chain model for the backoff window in noisy environments . . . 72
4.2 Analytical goodput enhancement of $smart_{BEB}$ mechanism. . . . 75
4.3 Goodput enhancement for $smart_{BEB}$ implementation in RTS/CTS mode. 76
4.4 The τ values in noisy environments. . . . 76
4.5 The p_c and p_d values in noisy environments. . . . 77
4.6 Saturation goodput in noisy environments. . . . 77
4.7 The additional nodes to original 20 nodes. . . . 78
4.8 Measured τ_{actual} for different T time slots when $p_e = 0.4$. . . . 81
4.9 Goodput enhancement for $smart_{BEB}$ implementation in basic mode. . . . 82
4.10 The estimated p_e for variable error rates over time. . . . 82
4.11 The τ values of the two classes. . . . 86
4.12 Goodput of the two classes. . . . 86
4.13 G1/G2 ratio of the two classes. . . . 87

5.1 Example of network with 4 nodes, where R is transmission range and C is the carrier sense range . . . 96
5.2 Blocking effectiveness of carrier sense range for different scenarios. The ineffectiveness is measured by the percentage of the shaded area to the carrier sense area (πC^2). . . . 97

5.3 Inefficiency of carrier sense mechanism versus distance without exploiting the capture phenomena 99
5.4 Capture analysis where $x' = \frac{x}{\sqrt{\alpha}}$ and $m' = \sqrt{\alpha}m$ 100
5.5 The analytical and simulation values of the probabilities P_1, P_2, and P_b . . 103
5.6 The probability P_b with different load values t' where $t' = \tau/T$ 104
5.7 Packet Capture of IEEE 802.11 109
5.8 Message-In-A-Message 111
5.9 PHY-MAC layer structure 112
5.10 Frame structure 112
5.11 PHY-MAC interactions 112
5.12 Medium under utilization scenario of LED mechanism 123
5.13 Effective throughput versus node density using RTS/CTS access mode . . 125
5.14 Throughput enhancement over Original mechanism versus node density using RTS/CTS access mode 126
5.15 Packet collisions versus node density using RTS/CTS access mode 126
5.16 Fairness index versus node density using RTS/CTS access mode 127
5.17 Effective throughput versus network load using RTS/CTS access mode . . 127
5.18 Throughput enhancement over Original mechanism versus network load using RTS/CTS access mode 129
5.19 Collision packets versus network load using RTS/CTS access mode . . . 130
5.20 Fairness index versus network load using RTS/CTS access mode 130
5.21 Effective throughput versus network load using basic access mode 131
5.22 Throughput enhancement over Original protocol versus network load using basic access mode 131
5.23 Fairness index versus network load using basic access mode 132
5.24 Effective throughput versus network degree using RTS/CTS access mode 133
5.25 Throughput enhancement over Original protocol versus network degree using RTS/CTS access mode 134
5.26 Fairness index versus network degree using RTS/CTS access mode 134
5.27 Effective throughput versus capture factor (β) using RTS/CTS access mode 136
5.28 Effective throughput versus error range using RTS/CTS access mode . . . 136
5.29 Effective throughput versus transmission range using RTS/CTS access mode 137
5.30 Fairness index versus transmission range using RTS/CTS access mode . . 140
5.31 Effective throughput versus transmission range using basic access mode . 141
5.32 Fairness index versus transmission range using basic access mode 141
5.33 Effective throughput of infrastructure configuration versus packet rate using RTS/CTS access mode 142
5.34 Throughput enhancement over Original protocol of infrastructure configuration versus packet rate using RTS/CTS access mode 143
5.35 Fairness index of infrastructure configuration versus packet rate using RTS/CTS access mode 143

6.1 Opportunistic MAC example 149
6.2 Blocking analysis where R is the transmission range and C is the carrier sense range 151

6.3 The analytical and simulation values of the probabilities P_S=$P(Std_{Idle})$, P_O=$P(CS_{Idle})$, and P_G=$P(OPP_{CS})$ 157
6.4 The probability $P(OPP_{CS})$ with different load values t' where $t' = \tau/T$ and different number of sectors n 158
6.5 Frame structure 159
6.6 PHY-MAC interactions 159
6.7 Network throughput versus number of connections 166
6.8 Throughput enhancement over D-MAC mechanism versus number of connections 167
6.9 Fairness index for the network versus number of connections 167
6.10 Fairness index for a node versus number of connections 168
6.11 Average $ServTime$ versus number of connections 168
6.12 Maximum $ServTime$ versus number of connections 169
6.13 Network throughput versus network load 171
6.14 Throughput enhancement over D-MAC mechanism versus network load . 172
6.15 Fairness index for the network versus network load 172
6.16 Fairness index for a node versus network load 173
6.17 Average $ServTime$ versus network load 173
6.18 Maximum $ServTime$ versus network load 174
6.19 Network throughput versus beamwidth size 175
6.20 Throughput enhancement over D-MAC mechanism versus beamwidth size 175
6.21 Fairness index for a node versus beamwidth size 176
6.22 Average $ServTime$ versus number of connections 176
6.23 Network throughput versus transmission/carrier ranges 177
6.24 Throughput enhancement over D-MAC mechanism versus transmission/carrier sense ranges 177
6.25 Average $ServTime$ versus transmission/carrier sense ranges 178

7.1 The analytical and simulation values of the probabilities P_S=$P(CS_{Idle})$, P_O=$P(HOL_{Idle})$, and P_G=$P(OPP_{HOL})$ 184
7.2 The probability $P(OPP_{HOL})$ with different load values t' where $t' = \tau/T$ and different number of sectors n, where $m = 4$ 185
7.3 The total enhancement of OPP_{HOL} with respect to the original IEEE for different load values t' where $t' = \tau/T$ and different number of sectors n, where $m = 4$ 185
7.4 Network throughput versus number of connections 189
7.5 Throughput enhancement over D-MAC mechanism versus number of connections 190
7.6 Fairness index for the network versus number of connections 190
7.7 Fairness index for a node versus number of connections 191
7.8 Average $ServTime$ versus number of connections 191
7.9 Maximum $ServTime$ versus number of connections 192
7.10 Network throughput versus network load 194
7.11 Throughput enhancement over D-MAC mechanism versus network load . 194
7.12 Fairness index for the network versus network load 195

7.13 Fairness index for a node versus network load 195
7.14 Average $ServTime$ versus network load 196
7.15 Maximum $ServTime$ versus network load 196
7.16 Network throughput versus beamwidth size 197
7.17 Throughput enhancement over D-MAC mechanism versus beamwidth size 198
7.18 Fairness index for a node versus beamwidth size 198
7.19 Average $ServTime$ versus number of connections 199
7.20 Network throughput versus transmission/carrier ranges 200
7.21 Throughput enhancement over D-MAC mechanism versus transmission/carrier sense ranges 200
7.22 Average $ServTime$ versus transmission/carrier sense ranges 201

Chapter 1

Introduction

With recent advances in computer and wireless communications technologies, wireless networks are significantly increasing in use and application. In wireless networks, nodes are equipped with wireless transmitters and receivers using antennas which may be omni-directional (broadcast), highly-directional (point-to-point), or some combination. Nodes are free to move randomly and organize themselves arbitrarily; thus, the wireless network's topology may change rapidly and unpredictably.

Wireless nodes are organized into two main network formations: infrastructure networks and ad hoc networks. In infrastructure networks, one or more static base station (access point) must be set up ahead of time to provide connectivity to other nodes where all the communications must go through it. There are many situations in which such a static infrastructure is either inconvenient or impractical, but nonetheless communication is desired. For example, users with mobile computers might want to collaborate on a group project in an outdoor area where there are no wireless access points. In such cases, wireless nodes may arrange themselves into mobile ad hoc networks (MANET) [1] in which they rely on their cooperation in order to accomplish their tasks.

Broad range of communications standards, some of which are well established and interoperable, while others are still emerging, have been proposed for wireless networks. Some examples of such standards are: IEEE 802.11 [9, 4], HiperLAN [38], Bluetooth [96, 18], ZigBee [129, 102], and WiMax [34]. The IEEE 802.11 standard, the most widely used in wireless networks, defines the physical layer and the medium access control (MAC) for wireless communication. In this dissertation, we focus on the IEEE 802.11 standards. However, *all the mechanisms and schemes in this dissertation could be easily adjusted and adapted for other standards*.

Various properties of wireless networks, such as: limited resources (e.g., energy, bandwidth, and storage), limited radio range, no pre-existing infrastructure, mobility, vulnerable medium, and noisy channels, have made it a challenging task to design efficient networking protocols for these technologies. In this dissertation, we show how by optimizing the interaction and tuning the parameters of the network protocols between two or more layers for a given network characteristic, we can achieve significant enhancement in network performance.

1.1 Characteristics of Wireless Network

Wireless networks have characteristics that differ from wired networks such as: mobility, limited resources (energy, bandwidth, storage), limited radio range, different antenna models, no pre-existing infrastructure, and varying channel conditions. Among these characteristics, we focus on the following important characteristics:

1. Wireless communication suffers from channel noise and corresponding transmis-

sion errors. The impact of channel noise on the wireless network performance is significant. For example, constructing multi-hop routes with minimum number of links but of high error rates would increase the energy cost of transmissions due to the retransmissions overhead. Moreover, The inability of differentiating between packet drops due to error rates and those due to collisions, under noisy environments, degrades the performance of the network.

2. Contention based MAC protocols proposed in the literature and used in IEEE 802.11 standards follow the operational model of CSMA. The well known ”physical layer capture” phenomena in radio channels [8, 78, 82, 69, 128, 116] refers to the successful reception of the stronger frame in a collision. In particular, the physical layer capture allows the receiver to capture a frame if the frame's detected power sufficiently exceeds the joint interfering power of interfering contenders by a minimum threshold factor. A significant enhancement in the network capacity could be achieved by exploiting the capture phenomena in the protocol design.

3. In contrast to omni-direction transmissions in which the transmitted signal propagates in all direction, a node equipped with directional antenna is capable of transmitting a signal that propagates either with a beam of certain width in a certain direction or in all directions, which corresponds to unicast and broadcast, respectively. The use of directional antennas aims at increasing the network capacity by reducing the transmission interference and thus allowing multiple ongoing transmissions simultaneously, as opposed to the common omni-directional antenna that allows only one ongoing transmission at a time. New protocols have to be

devised to exploit the directional antenna features in order to increase the network performance.

1.2 Cross-Layer Design

The layered architecture of network protocols is widely accepted as being a good abstraction for network device functionality. The motivation of the layered architecture is to provide modularity and transparency between the layers to simplify the design of network protocols. Significant work has been done to develop efficient techniques for wireless networks, but most of the work has concentrated on optimizing layer(s) independently in the protocol stack.

However, it is becoming increasingly clear that local optimization of layers may not lead to global optimization. It is imperative that network protocols and designs should be engineered by optimizing across the layers. This design methodology is referred to as cross-layer design. Cross-layer design allows us to make better use of network resources by optimizing across the boundaries of traditional network layers. It is based on information exchange and joint optimization over two or more layers. Cross-layer designs yield significantly improved performance by exploiting the tight coupling between the layers in wireless systems.

In this dissertation, we address the issue of cross-layer networking, where the physical layer knowledge of the wireless medium is shared with higher layers, in order to improve performance.

1.3 Contributions of the Dissertation

The contributions of this dissertation fall into three areas related to the routing and MAC layers in wireless networks. These contributions are summarized in the following subsections.

1.3.1 Wireless Networks in Noisy Environments

One of the major goals in ad hoc networks is to minimize energy consumption in multi-hop communication. Constructing reliable and energy efficient multi-hop routes in ad hoc networks should take into account the channel noise in the vicinity of the nodes and evaluate the candidate routes based on the potential retransmissions over links. IEEE 802.11 adopts a fragmentation mechanism in which large packets are partitioned into smaller fragment to increase their transmission reliability over single hop. This fragmentation mechanism should be considered too by the routing protocols in evaluating the reliable and energy efficient routes.

We present mechanisms to compute energy-efficient paths, using the IEEE 802.11 fragmentation mechanism, within the framework of on-demand routing protocols in ad hoc networks. We show how our scheme accounts for channel characteristics in computing such paths and how it exploits the IEEE 802.11 fragmentation mechanism to generate optimum energy-efficient paths. Our results show that our proposed variants of on-demand routing protocols can achieve orders of magnitude improvement in energy-efficiency of reliable data paths [87, 85].

Also, we extend the study of noisy environments to the performance of the IEEE

802.11 infrastructure networks. We show that using the standard binary exponential back-off (BEB) mechanism in noisy environments results in a poor throughput performance due to its inability to differentiate between the causes of unsuccessful packet transmissions. We develop an ”enhanced BEB” mechanism that improves the IEEE 802.11 with a capability of differentiating between different types of unsuccessful transmissions and showed that the new mechanism enhances the network performance significantly with respect to the network error rates (noise level) [84, 86].

1.3.2 Physical Layer Capture Effect

Current physical layer implementations of IEEE 802.11 allow the receiver to capture a frame correctly provided its signal strength is sufficiently stronger and it arrives before the reception of the PLCP header[1] [123] of a frame with weaker signal strength that the receiver is currently engaged in receiving. However, we show how the network capacity increases significantly if the physical layer (PHY) is capable of capturing the strongest frame regardless if it comes before or after the weaker frame(s).

We modify PHY/MAC layers in a way that allow this capture mechanism. With this capture mechanism, we develop a location aware MAC protocol, in which the location of the nodes are embedded in the transmitted frames, to increase the concurrent transmission. Using the location information, each node is able to decide if it can start its own transmission concurrently with the ongoing transmission, or has to block its transmission until the end of current ongoing transmission. We analytically study the potential performance

[1] The PLCP header is part of the 802.11 frame that comes before MAC data subframe and contains logical information that will be used by the physical layer to decode the frame.

enhancement of our mechanism over the original IEEE 802.11. The analysis shows that up to 35% of 802.11 blocking decisions are unnecessary. The results are verified using the ns-2 simulator in which we show that our enhanced 802.11 can achieve up to 22% more throughput than the original 802.11 [90, 89].

1.3.3 Directional Antennas

Directional antennas have been introduced to improve the performance of 802.11 based wireless networks by increasing medium spatial reuse. However, The IEEE 802.11, and carrier sensing protocols in general, were developed with omni-directional antennas in mind. We exploit the spatial reuse of the directional antenna in the MAC layer of IEEE 802.11 standard by developing two novel opportunistic enhancement mechanisms.

The first mechanism augments the MAC protocol with additional information (location of the stations) that gives a node the flexibility to transmit data while there are ongoing transmissions in its vicinity. The second mechanism, using the augmented MAC protocol, changes the access routines of the MAC data queue. We show analytically that a station with directional antenna and using 802.11 protocol is conservative in terms of assessing channel availability, with as much as 60% of unnecessary blocking assessments. By altering the way the 802.11 accesses its MAC data queue, we show that the unnecessary blocking assessments of a node could reach 90%. Using the ns-2 simulator, we show improvements in network throughput of up to 40% in case of applying the first enhancement, and up to 60% in case of applying the second enhancement [88].

1.4 Structure of the Dissertation

Chapter 2 presents background. Chapter 3 describes the construction of efficient ad hoc routing protocols in noisy environments. Chapter 4 describes mechanism for enhancing 802.11 DCF in noisy environments. Chapter 5 presents how the capture phenomena can be exploited in 802.11 to enhance network performance. Chapter 6 describes how to augment the 802.11 MAC protocol with additional information to increase the number of simultaneous data transmissions. On top of that modification, Chapter 7 describes a new handling mechanism for the access routines of the MAC queue in 802.11 protocols. Some concluding remarks are presented in Chapter 8.

Chapter 2

Background

In this chapter, we present some background information necessary for the subsequent chapters. This presentation is in three parts. First, we present an overview of the IEEE 802.11 medium access control and its fragmentation mechanisms. Next, we describe the propagation model assumed in the dissertation and the capture phenomena. Finally, we give a brief overview of the implications of the use of directional antenna.

2.1 IEEE 802.11 Standard

The IEEE 802.11 standard [9, 4] for wireless networks has been widely used in most commercial wireless products. The standards specify the parameters of both the physical (PHY) and medium access control (MAC) layers of the network. The 802.11 networks could be organized in two different network architectures: infrastructure network and ad hoc network. In infrastructure networks, nodes communicate with each other by first going through a central node called Access Point (AP). On the other hand, in ad hoc mode nodes communicate directly with each other, without the use of an access point (AP).

In ad hoc architecture, nodes form the network routing infrastructure in an ad hoc fashion and rely on their cooperation in order to accomplish their tasks, for example, forwarding packets. A number of ad hoc routing protocols have been proposed and evaluated in other work. We classify the ad hoc routing protocols to: 1) classic pro-active protocols in which the routing tables are updated periodically throughout the lifetime of the network [81, 99, 113, 58, 43, 13], 2) re-active protocols, the very popular protocols in ad hoc networks, in which they discover the route to destination only when that route is needed [121, 100, 50, 63, 56, 28, 33, 97], 3) hierarchical protocols which usually combine two or more strategies to create several routing-layers [61, 95, 47, 94, 46, 52, 51], and 4) geographical routing protocols which are based on getting the geographical location of the nodes from additional hardware/software [12, 73, 65, 93].

In this section, we describe the preliminaries of the MAC layer.

2.1.1 IEEE 802.11 Distributed Coordination Function (DCF)

The IEEE 802.11 MAC specifies two access mechanisms: the contention-based Distributed Coordination Function (DCF) and the polling-based Point Coordination Function (PCF). At present, only the DCF is mandatory in the IEEE 802.11-compliant products which is the focus of this dissertation.

The IEEE 802.11 DCF access method is based on the Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) technique. The CSMA/CA mechanism requires a minimum specified gap/space between contiguous frame transmissions. Before a node starts transmission, it senses the wireless medium to ensure that the medium is idle for a period of time (DIFS Distributed Inter Frame Space), else the node waits until the

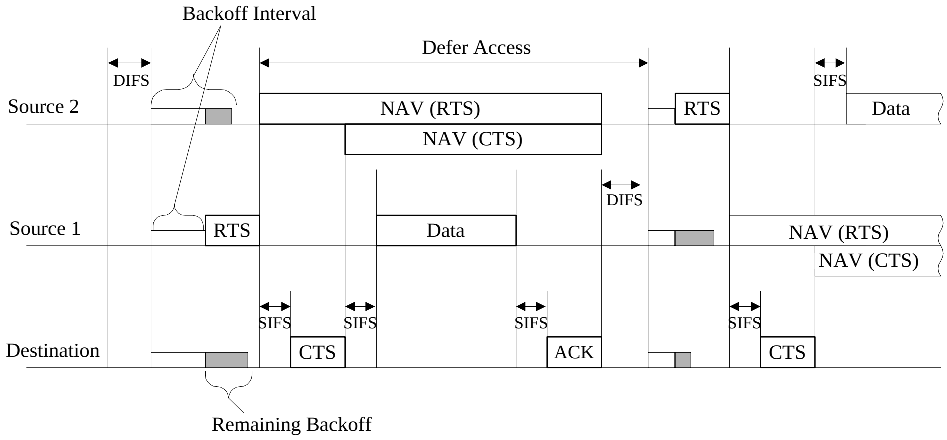

Figure 2.1: IEEE 802.11 DCF Mechanism

end of the in-progress transmission before again waiting for DIFS. In order to reduce the collision probability among multiple nodes accessing the medium, the node waits for a random backoff interval after the DIFS deferral and then transmits if the medium is still free (Source 1 in Figure 2.1).

If the packet is correctly received, the receiving host sends an ACK frame after another fixed period of time (SIFS Short Inter Frame Space) which is smaller than DIFS. After receiving an ACK frame correctly, the transmitter assumes successful delivery of the corresponding data frame. Otherwise, the packet is assumed to be dropped because of a collision corruption. In addition to this *basic* transmission mechanism, the DCF defines an optional *RTS/CTS* mechanism, which requires that the transmitter and receiver exchange short Request-To-Send (RTS) and Clear-To-Send (CTS) control frames prior to the actual data frame transmission. Figure 2.1 illustrates this mechanism for case of two sources and a destination competing for the medium access. The DCF adopts a slotted binary exponential backoff mechanism [9] to select the random backoff interval. This backoff interval is calculated by multiplying a selected random number by predefined time interval named tSlotTime [9]. The random number is drawn from a uniform distribution over the interval [0, CW-1], where CW is the contention window size and its initial value is aCWmin. In the case of an unsuccessful transmission, indicated by missing ACK frame or CTS frame, CW is doubled. Once CW reaches aCWmax, it remains at this value. After a successful transmission, the CW value is reset to aCWmin before the random backoff interval is selected. Each node decrements its backoff counter every tSlotTime interval after the wireless medium is sensed to be idle for DIFS time as long as medium is idle. If the counter has not reached zero and the medium becomes busy again, the node freezes its counter until the medium becomes free again for a DIFS period (the shaded parts in the backoff intervals of Source 2 and Destination in Figure 2.1). When the counter finally reaches zero, the node starts its transmission (the RTS frame in case of RTS/CTS mechanism or the data frame in case of basic mechanism).

Each node maintains a timer called the Network Allocation Vector (NAV) which tracks the remaining time of any ongoing data transmission. After a node receives a RTS, CTS, DATA, or ACK frame not destined for itself, it sets its NAV according to the "Duration" field of the frame. The Duration field contains the frame sender's estimation for how long the whole data delivery frame exchange sequence will take, or in other words, the reservation duration of this whole frame exchange sequence. Checking its NAV before a node attempts to transmit, is also known as "virtual carrier sensing". If the NAV is not zero, the node needs to block its own transmissions to yield to the ongoing data delivery. In summary, a node blocks its own transmissions if either physical carrier

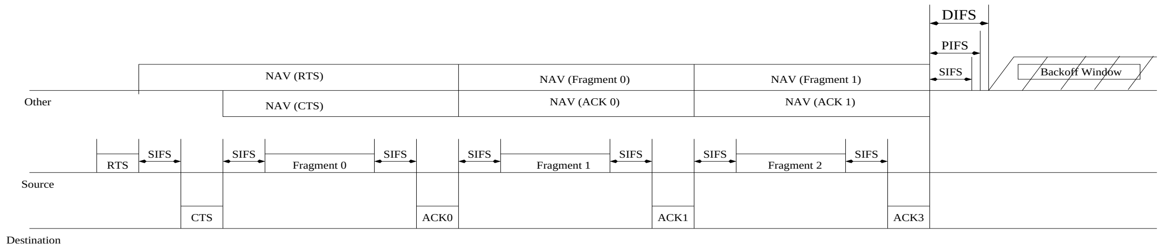

Figure 2.2: RTS/CTS with fragmented packet

sensing or virtual carrier sensing returns channel busy.

2.1.2 IEEE 802.11 Fragmentation

The process of partitioning a packet frame into smaller frames is called fragmentation. The IEEE 802.11 fragmentation mechanism creates smaller MAC frames than the original MAC ones to increase reliability by increasing the probability of successful transmission of the original frames in cases where channel characteristics limit reception reliability for longer frames [9, 4]. Only MAC frames with a unicast receiver address are fragmented. The IEEE 802.11 standards define *aFragmentationThreshold* as the fragmentation threshold. If a MAC frame length exceeds this threshold, it is fragmented to frames with length no longer than the threshold. The frames resulting from the fragmentation are sent as independent transmissions, each of which is separately acknowledged. This permits transmission retries to occur per fragment, rather than per original frame. Unless interrupted due to medium occupancy limitations, the fragments of a single frame are sent as a burst in the DCF mode of IEEE 802.11.

Figure 2.2 illustrates how IEEE 802.11 transmits the fragments using RTS/CTS mechanism. Each frame contains information that defines the duration of the next transmission. The duration information from RTS frames is used to update the network allocation vector (NAV) to indicate busy until the end of $ACK0$. The duration information from the CTS frame is also used to update the NAV to indicate busy until the end of $ACK0$. Both $Fragment0$ and $ACK0$ contain duration information to update the NAV to indicate busy until the end of $ACK1$. This is done by using the Duration/ID field in the Data and ACK frames. This continues until the last fragment, which has a duration of one ACK time plus one SIFS time, and its ACK, which has its Duration/ID field set to zero. Each fragment and ACK acts as a virtual RTS and CTS and no further RTS/CTS frames need to be generated after the RTS/CTS that began the frame exchange sequence as long as no fragment or ACK is lost. When a fragment or ACK is lost and a fragment retransmission is needed, the node has to wait for DIFS period augmented with random CW period of a idle channel and start the frame exchange sequence for the rest of the fragments with RTS/CTS frames as in Figure 2.2.

2.2 Radio Propagation Model

Several radio propagation models have been proposed in the literature [40, 41, 72, 32, 110, 105], to predict the received signal power of each packet at the receiver side. Different propagation models have proposed to capture the path loss model for indoor and outdoor scenarios. Some examples of those models are: free space model [40, 41, 105], two-ray ground reflection model [72, 105, 32, 110], and shadowing model [105, 110]. In this section, we describe the free space/two-ray propagation model in which many channels, especially outdoor channels, have been found to fit this model in practice. This propagation model is used in this dissertation where we focus on outdoor scenarios. However, as will be pointed out, the mechanisms described in this dissertation could be used with any other propagation model.

2.2.1 Free Space/Two-ray Propagation Model

In this propagation model, the following equation is used to calculate the received signal power in free space at distance D from the transmitter [40, 41, 105, 110]:

$$P_r = \begin{cases} \frac{Pt*G_t*G_r*\lambda^2}{(4*\pi)^2*D^2*L} & D \leq D_{cross} \\ \frac{Pt*G_t*G_r*h_t^2*h_r^2}{D^4*L} & D > D_{cross} \end{cases} \tag{2.1}$$

where P_r is the received signal power, P_t is the transmission power, G_t is the transmitter antenna gain, G_r is the receiver antenna gain, D is the separation between the transmitter and the receiver, h_t is the transmitter elevation, h_r is the receiver elevation, L is the system loss factor not related to propagation (≥ 1), λ is the wavelength in meters, and D_{cross} is calculated as $D_{cross} = (4 * \pi * h_r * h_t)/\lambda$. The first sub-model of Equation 2.1 is called the Friis free-space propagation model [40, 41] and only used when the distance between the transmitter and the receiver is small. The second sub-model is called the two-ray ground reflection model [72, 105, 110] and used when the distance is large.

2.2.2 Capture Effect

When a frequency modulation scheme, such as the Direct Sequence Spread Spectrum (DSSS) used by most IEEE 802.11 physical layer (PHY) implementations, is used in wireless communication, an effect known as the “capture effect” [7, 79, 83, 70, 45] occurs.

When two transmissions sent by two different transmitters at the same frequency overlap in time and they are received by a receiver, the signals of the stronger transmission will capture the receiver modem, and signals of the weaker transmission will be rejected as noise.

Different researchers (e.g., [45, 23, 71, 127, 67]) have studied the analytical and simulation models for characterizing the capture effects. Among the results of these previous works, we adopt a simple yet widely accepted model to describe the capture effect. In our model, a receiver captures the signals of a particular transmission if the received power P_r of this transmission sufficiently exceeds all other received power P_i of *n* other concurrent interfering contenders combined by a minimum ratio. That is, the capture occurs when:

$$P_r > \alpha \sum_{i=1, i \neq r}^{n} P_i \tag{2.2}$$

where α is this minimum ratio and it's called the capture ratio.

Wireless communication technologies, such as IEEE 802.11, do not pay special attention to capture effects mainly to keep the design simple. Also the contention-based MAC protocol largely reduces the time and space overlapping of simultaneous transmissions. Nonetheless, the capture effect still exists in IEEE 802.11 DSSS networks and has been confirmed by several published studies. Authors in [53, 127, 67] have also studied the impact of capture effect on traffic fairness and throughput of UDP and TCP flows for both ad hoc and infrastructure modes of IEEE 802.11 systems.

2.3 Directional Antenna

IEEE 802.11 was developed primarily for omni-directional antennas. It assumes that all the packets (RTS/CTS/DATA/ACK packets) are transmitted as omni-directional signals that are received by all nearby nodes. Most recently, directional antennas have been used to improve the performance of IEEE 802.11 based wireless networks [66, 108, 137, 118, 27]. In chapters 6 and 7 we propose mechanisms to exploit characteristics of directional antennas. In this section we briefly describe the operation of directional antennas.

Directional antennas can transmit data in both *omni* and *directional* modes. In omni-directional transmission, the node can transmit with equal power to all directions. In directional transmission, the node directs its energy toward a particular direction, often called the main lobe. In addition to this main lobe, there exist side and back lobes as wasted energy, which is called *flat-topped* pattern [108, 112, 119]. Unlike flat-topped pattern, we assume *ideally-sectorized* pattern [66, 92], that is, there are no side and back lobes as shown in Figure 2.3.

A node uses both omni and directional modes in receiving ongoing transmission. When the node is idle (not transmitting or receiving), it hears signals from all directions. But when it hears a transmission from a certain direction, it switches to directional receiving mode, and receives the frame from this direction.

The two common trends in directional antennas are *switched-beam* systems, and *steering-beam* systems [108]. A switched-beam system consists of a number of predefined fixed beams. Depending on the signal strength and direction, the node chooses one of the predetermined beams to transmit or receive data. A steering-beam system can point

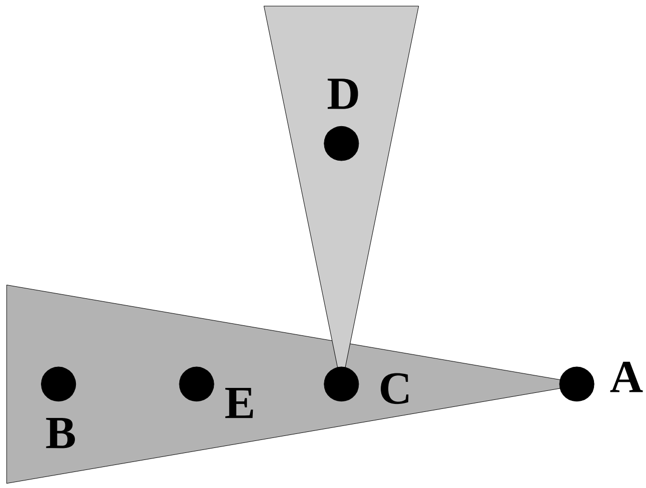

Figure 2.3: Ideally-sectorized model of directional antenna

its beam virtually in any direction depending on the transmitted or the received signals. Steering-beam systems provide more flexibility, but steering-beam systems have narrow main lobes, and smaller side and back lobes.

When a 802.11 node uses directional antenna, DATA and ACK frames are transmitted directionally. However, a variation from the omni RTS and CTS frames mentioned in the previous subsection is used. Different variations have been proposed in which each of RTS and CTS frames could be transmitted either omni, directional, or hybrid [66, 126]. We adopt best-fit RTS/CTS model. Here, when a node wants to transmit an RTS frame toward a certain destination, it checks if all directions are idle. If they are idle, the node transmits the RTS frame omni-directionally. Otherwise, the node transmits RTS frame in the direction of the required destination. Similar to [36], we include information about the required direction of transmission in the RTS frame. The rationale behind this approach is to notify the maximum number of neighbors of the ongoing reservation and, to assist them in taking the best decision of whether to proceed or refrain from transmission. The

CTS frame is treated similarly.

Note that the NAV mentioned in the previous subsection is not applicable within the directional transmission of frames. Thus, DNAV, proposed in [119, 27], is used with directional antenna. Unlike NAV, each DNAV is associated with a direction and a width, and multiple DNAV can be set for a node. A node maintains a unique timer for each DNAV, and also updates the direction, width and expiration time of each DNAV every time the physical layer gives newer information about the corresponding ongoing transmission.

Chapter 3

Efficient Ad Hoc Routing Protocols in Noisy Environments

Battery-power is typically a scarce and expensive resource in wireless devices. Minimizing energy consumption in wireless devices during communication is one of the interesting problems in the field of wireless communication for increasing the lifetime of the wireless devices. Different techniques and mechanisms have been proposed to reduce the communication cost and increase the power saving of the wireless devices. Large part of the work addresses energy-efficient link-layer forwarding techniques [136, 103, 44, 35, 114] and routing mechanisms [115, 21, 122, 22, 132] for multi-hop wireless networks.

These previously known energy-efficient routing techniques typically address two distinct and complementary objectives:

- *Finding energy-efficient end-to-end routes:* For wireless links, a signal transmitted with power Pt over a link with distance D gets attenuated and is received with power, $Pr \propto Pt/D^m$, where $m \geq 2$ is a constant that depends on the propagation medium and antenna characteristics. Value of m is typically around 2 for short distances and omni-directional antennae, and around 4 for longer distances as shown in Equation 2.1. The transmission powers for these links are, consequently, chosen proportional to D^m. Thus, protocols that compute energy-efficient end-to-end paths choose routes with a large number of small hops [115].

- *Maximizing the lifetime of a network:* Another metric of interest in wireless environments is the lifetime of the network. Techniques for increasing network lifetime include alternating awake and sleep cycles for nodes [132, 22] and heuristic choices for routing traffic flows that balance the residual battery power at different nodes [21, 122].

Wireless communication suffers from high transmission errors due to the channel noise. To increase transmission reliability, wireless MAC protocols adopt different error control and reliability mechanisms (e.g., FEC and ARQ). The IEEE 802.11 standard implements retransmission mechanism in which a packet is retransmitted over a link if no MAC layer acknowledgment is received. In addition, IEEE 802.11 adopts a fragmentation mechanism that partitions large packets into smaller fragments to increase transmission reliability.

Such reliability mechanisms are applied on all transmitted data packets regardless of the protocol service type (i.e. reliable service (e.g., TCP) or unreliable service (e.g., UDP)) the packets belong to. In consequence, these mechanisms affect significantly the communication cost and performance. Therefore, these reliability mechanisms should be considered in the choice of the data paths to cope with the energy efficiency objective. In particular, the choice of energy-efficient routes should take into account the channel noise in the vicinity of these nodes. Such noise would lead to transmission errors and consequent re-transmissions and thus increase the energy costs for reliable data delivery. Moreover, routing computations should take into account the different mechanisms provided by the wireless MAC layer to reduce the transmission errors, e.g. the IEEE 802.11 fragmentation mechanism.

Routing protocols in ad hoc networks can be categorized generally to: *pro-active* and *re-active protocols*. Pro-active protocols (e.g. link state and distance vector routing protocols) depend on maintaining routing information about the destinations at each node. A route is constructed in an incremental fashion in which each intermediate node, using some cost criteria; select the next link on the route toward the destination. As will be shown in Section 3.2, the wireless link (hop) error rate is estimated at the receiver end node of the link. In order to incorporate the link error costs in pro-active protocols where the sender node determines which link it transmits on, the receivers need to propagate all the link error information it gathered about the neighbor links to the sender side nodes to update their cost criteria. Obviously, using link error costs in pro-active routing protocols is not scalable due to the large transmission overhead in exchanging link error information between nodes.

On the other hand, re-active (on-demand) routing protocols compute routes only when needed in separate route-discovery phase. In this phase, intermediate nodes participate in selecting the links in which the nodes will receive the packets. This is contrary to the pro-active routing protocols where the intermediate nodes select links to forward the packets on. Hence, the link error computations fits perfectly with the re-active routing protocols in which the intermediate nodes (receiver end nodes) incorporate the estimated link error values in the choice of the route links with no need for data propagations.

Therefore, we focus on the re-active protocols for their inherent scalability and popularity in ad hoc networks.

In this chapter, we develop a minimum energy end-to-end reliable path computation mechanism for Ad-hoc On-demand Distance Vector routing protocol (AODV) [101]. The routing computation takes into account the channel noise, and the link error rates and its retransmission consequences. Our routing computation takes into account the *cross layer interaction* with the MAC layer in order to increase the reliability by exploiting the available fragmentation mechanism provided by the IEEE 802.11 layer. It should, however, become obvious from our description that our technique can be generalized to alternative on-demand routing protocols (e.g., DSR [62] and TORA [98]). Through our experimentation, we perform a detailed study of the AODV protocol and our energy-efficient variants, under various noise and node mobility conditions. As part of this study, we have identified some specific configurations where an on-demand protocol that does not consider noise characteristics can result in significantly lower throughput, even under conditions of low or moderate channel noise.

The roadmap of the chapter is as follow: The related work is presented next in Section 3.1. Section 3.2 presents background about the link error rate and the estimation mechanism. In Section 3.3, we present our formulation of the energy efficient path computation problem. Section 3.4 describes the AODV protocol, and then describes the necessary modifications to adapt it for our proposed path computations. The detailed simulation experiments to evaluate the performance of the protocols are showed in Section 3.5. Finally we conclude in Section 3.6

3.1 Related Work

A large number of researchers have addressed the energy-efficient data transfer problem in the context of multi-hop wireless networks. As described earlier, they can be classified into two distinct categories. One group focuses on protocols for minimizing the energy requirements over end-to-end paths. Typical solutions in this approach have ignored the retransmission costs of packets and have therefore chosen paths with a large number of small hops [114, 49]. For example, the proposed protocol in [114] is one such variable energy protocol using a modified form of the Bellman-Ford algorithm, where the nodes modify their transmission power based on the distance to the receiver, and where this variable transmission energy is used as the link cost to effectively compute minimum energy routes.

An alternative approach focuses on algorithms for increasing the lifetime of wireless nodes, by attempting to distribute the forwarding load over multiple paths. This distribution is performed by either intelligently reducing the set of nodes needed to perform forwarding duties, thereby allowing a subset of nodes to sleep over idle periods or different durations (e.g, PAMAS [115], SPAN [22], and GAF [132]), or by using heuristics that consider the residual battery power at different nodes [122, 21, 80] and route around nodes nearing battery exhaustion. However, none of these protocols has considered the link quality and the MAC layer retransmission effect in their computations.

Yarvis et al. [134] observe that hop-count performs poorly as a routing metric for a sensor network, and present the results of using a loss-aware metric. While this metric is likely to use low-loss paths with many hops and doesn't consider situations where a path with a smaller number of higher loss links would perform better, the cost function in our schemes handles such situation perfectly. A number of existing ad hoc wireless routing algorithms collect per-link signal strength information and apply a threshold to avoid links with high loss ratios ([25], [30], [33], [48], [55], [77]). While this approach may eliminate links that are necessary for connectivity, our method selects these links if there is no other possible paths. Papers [31] and [11] introduce a method for route selection using metrics accounts for link loss ratios. Authors in [11] assume that each node is aware about the error rates for its outgoing links with no mechanism description about how to acquire this information. They studied the minimum energy reliable communication problem for the standard pro-active routing protocols in static topologies only.

The metric in [31] combines the loss ratios in the two directions over a link. In consequence, the method selects a single path between two nodes regardless of the direction of the communication. This method doesn't work in situations when the optimum path for one direction is not the same for the other direction. Our cost function considers the cost only in the direction of the communications, which allows it to calculate the optimum path on each direction. Another difference, the [31] protocol appends the cost all the links along the route in the route construction packets while our method appends only fixed number of values (3 values) regardless of the number of links. Also, they experimented with static topologies only.

None of the above schemes consider the effect of the features provided by the MAC layer as our schemes make use of the fragmentation feature in the IEEE 802.11 MAC layer. Finally, this work does not assume using of sophisticated hardware to allow variable transmission power levels to be changed to make links better behaved to minimize energy consumption required to successfully deliver data as in [54] and [109].

3.2 Wireless Link Error Rates

It is important to explicitly consider the link's error rate as part of the route selection algorithm to reduce the retransmission cost. This is because the choice of links with relatively high error rates will lead to large number of packet re-transmissions and, hence, significantly increase the energy spent in reliable transmission.

Any signal transmitted over a wireless medium experiences two different effects: attenuation due to the medium, and interference with ambient noise at the receiver.

In the free space propagation channel model 2.1, described in Chapter 2, the ambient noise at the receiver is independent of the distance between the source and destination, and depends purely on the operating conditions at the receiver. The bit error rate, p, associated with a particular link is a function of the ratio of the received signal power (Pr) to the ambient noise.

The exact relationship between p and Pr depends on the choice of the signal modulation scheme. However, in general, several modulation schemes exhibit the following generic relationship between p and Pr is: $p \propto \textit{erfc}(\sqrt{\frac{constant \times Pr}{N}})$ where N is the noise signal power and $\textit{erfc}(x)$ is defined as the complementary function of $\textit{erf}(x)$ and is given by: $\textit{erfc}(x) = 1 - (2/\sqrt{\pi}) \int_0^x \exp^{-t^2} dt$. For the case of BPSK (Binary Phase-Shift Keying) and QPSK (Quadrature Phase-Shift Keying) the bit error is obtained by [104]

$$p = 0.5\ \textit{erfc}(\sqrt{\frac{Pr \times W}{N \times f}}) \tag{3.1}$$

where f is the transmission bit rate and W is the channel bandwidth (in Hz). Note

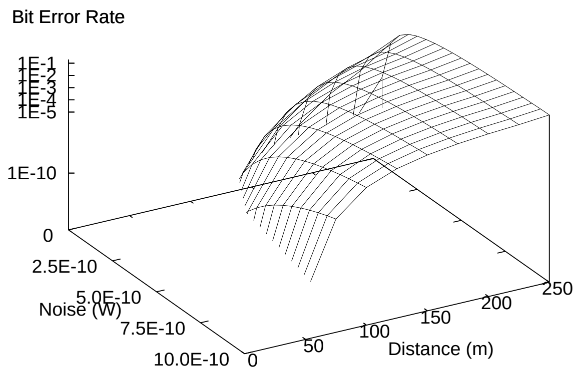

Figure 3.1: Bit Error Rates for different Noise and Distance values using Equations 3.1 and 2.1. The parameter values in those equations are defined in Table 3.2.

Parameter	*Value*	*Comments*
PHY header	24 octets	PHY layer overhead
MAC header	28 octets	MAC layer overhead
ACK	38 octets	ACK frame length + PHY header
RTS	44 octets	RTS frame length + PHY header
CTS	38 octets	CTS frame length + PHY header
Slot time	20 μs	idle slot time (δ)
SIFS	10 μs	SIFS time
DIFS	50 μs	SIFS + 2 * $delta$
aCWmin	31	minimum contention window
m	5	backoff levels

Table 3.1: MAC and PHY system parameter.

that the CCK (Complementary Code Keying) used by IEEE 802.11b to achieve the 11 Mbps, which we assume in this chapter where the bit rate f is 11 Mbps and the channel bandwidth W is 2 MHz, is modulated with the QPSK technology. Figure 3.1 plots the relation between the bit error rates, distance, and noise where the values of the propagation model parameters of Equation 2.1 are defined by Table 3.2.

We assume the transmission power of each node to be a fixed constant Pt[1]. For any

[1]Most current wireless cards do not provide any mechanism for adaptively choosing the transmission

particular link l, the energy required to transmit packets is independent of the distance D and depends only on the transmission power Pt and the packet size k bits. Although IEEE 802.11 uses a limited number of retransmission trials for a packet, we approximate the *mean* number of individual packet transmissions for a successful transfer of a single packet as $1/(1 - p_l)^k$. This approximation is justified by (1) using of large number of retransmission trials per successful transfer, and (2) the assumption of sources with infinite data packets. The mean energy cost, C_l, required for a successful transfer of this packet across the link is given by

$$C_l = \frac{E_l}{(1 - p_l)^{k_l}} \tag{3.2}$$

where E_l is the energy consumed by the sender node for each transmission attempt across the link and p_l is the bit error rate over that link. Any energy-efficient protocol should consider the cost C_l, that is equivalent to the mean energy required to successfully transmit a packet across the link l, in their decision of selecting link l or not. Note that we do not consider the cost of the control packets, e.g., RTS/CTS/ACK frames of IEEE 802.11, since the cost of the data packets dominates other costs.

In our proposed mechanism, it is sufficient for each node to estimate only the bit error rate, p, on its incoming wireless links from its neighboring nodes. Most wireless interface cards typically measure the signal-to-noise ratio (SNR) for each received packet. SNR is a measure of the received signal strength relative to the background noise and is often expressed in decibels as:

$$SNR = 10 \log \frac{Pr}{N} \tag{3.3}$$

---

power for each packet.

From the SNR value measured by the wireless interface card, we can calculate the ratio $\frac{Pr}{N}$. Substituting it in Equation 3.1, we estimate p experienced by each received packet. This SNR-based error rate estimation technique is useful especially in free space environments where such error models are applicable. For other environments, where signal path characteristics depend more on the location and properties of physical obstacles on the paths, we could use an alternative technique that is based on empirical observations of link error characteristics [87]. We focus on the SNR-based technique.

In practice, a passing mechanism should be used to hand the measured SNR and Pr values from the wireless interface card to the upper routing algorithm. This could be implemented either by allowing the upper layers to *pull* those information through calls to APIs provided by the wireless card, or by *pushing* those information up using call-back functions defined by upper layers (e.g., AODV).

From Equation 3.1, the average energy involved in transmitting packets decreases with reducing the packet size (k). On the other hand, using smaller packet sizes increases the transmission overhead which is translated to energy cost. In the following section, we show how to calculate the optimum fragment size over a link to reduce the energy cost.

3.3 Optimal Fragment Size for Energy Efficient Paths

To compute the minimum energy data paths, the evaluation of candidate paths is not merely based on the energy spent in a single transmission attempt across the wireless hops, but rather on the total energy required for packet delivery, *including potential retransmissions due to errors and losses* on the wireless link. Such a formulation is especially relevant in multi-hop wireless networks, where variable channel conditions often cause packet error rates as high as $15 - 25\%$.

Fragmentation decreases the average number of retransmission for a packet delivery by partitioning the original packet into smaller fragments. Clearly, from Equation 3.2, the energy consumed to deliver a single bit is lower in case of using fragments than the case of using original packet. In this section, we use the IEEE 802.11 fragmentation mechanism presented earlier in Chapter 2 to describe how to calculate the optimum fragment size for a link.

Fragmentation introduces an overhead associated with transmission of additional bits (additional energy cost) and additional delays (throughput reduction). Although we focus on minimizing the energy cost, the experiments show an increase in the throughput as a side effect of our proposed routing mechanism.

Two types of overhead bits are associated with the transmission of each fragment in IEEE 802.11. The bits (o_1), which are transmitted separately with each frame and are not considered as a part of the frame bits, represent one type of the overhead bits. As example: the PLCP preamble bits, the PLCP header [9], and the MAC ACK frames. The other type of the overhead bits (o_2) is transmitted within each frame such as the frame header and the frame CRC field. We assume that the energy necessary to transmit any bit of these types is equal to the energy needed to transmit any single fragment bit, v.

Given link l, it is required to find the optimal fragment size (${k_l}^*$) that is corresponding to the minimum transmission cost. Assume the original packet size to be transmitted over the link is L and it is fragmented to fragments each with size k_l, then the energy cost

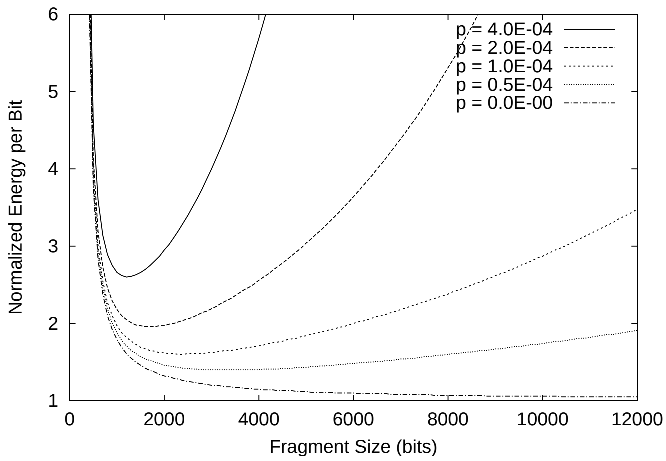

Figure 3.2: Normalized energy consumption for each transmitted bit using different fragment sizes over wireless link using Equation 3.4 where $o_1 = 250bits$, $o_2 = 300bits$, and $v = 1unit$

required for a successful transmission of single fragment, using Equation 3.2, is $\frac{(o_1+k_l)\times v}{(1-p_l)^{k_l}}$. Since the original packet will be partition into $\frac{L}{k_l-o_2}$ fragments, the total cost associated with a successful transmission of a packet is:

$$\begin{aligned} C_l &= \frac{L}{k_l - o_2}\times\frac{(o_1+k_l)\times v}{(1-p_l)^{k_l}} \\ &= L\times v\times\frac{o_1+k_l}{(k_l-o_2)(1-p_l)^{k_l}} \end{aligned} \tag{3.4}$$

Figure 3.2 plots Equation 3.4. It shows the mean cost of successful single bit delivery with different fragmentation sizes and different p_l values assuming the transmission bit energy, v, is one unit. Using small segment sizes, the link transmission cost is very high due to the high overhead included. With increasing the segment size, the cost is decreased until it reaches its minimum value using the optimal segment size (${k_l}^*$). Increasing the segment size beyond ${k_l}^*$ results in increasing the link cost again due to the increase in the retransmission trials. To find ${k_l}^*$, we differentiate Equation 3.4 with respect to k_l and equal it to zero to get:

$$k_l{}^* = \frac{(o_2 - o_1)\beta - \sqrt{(o_2 - o_1)^2\beta^2 - 4\beta(o_1 + o_2 - o_1 o_2 \beta)}}{2\beta} \tag{3.5}$$

where β is $\ln(1 - p_l)$.

Using optimum fragment size over links has two impacts.

1. It reduces the energy cost significantly over individual links. For example, in Figure 3.2 transmitting a 1500 bytes packet over link with $p = 1.0 \times 10^{-4}$ using fragments of size 300 bytes reduces the cost per bit by 54% from 3.48 energy unit to 1.6 energy unit.

2. It increases the possible alternative routes which gives the flexibility of selecting shorter paths with lower end-to-end energy cost. For example, consider two alternative paths: the first path consists of a single hop with $p = 4.0 \times 10^{-4}$ and costs of 2.6 units. The other path consists of two hops each with $p = 1.0 \times 10^{-4}$ and costs of 1.6 units. Although the individual link cost on the first path is higher than any of the links on the second path, selecting the first path will cost in total 2.6 units which is lower than the total cost of the second path (3.2 units).

We assume that given the p value of a link, the IEEE 802.11 MAC layer will calculate and use the optimum fragmentation size for packet transmissions in case the fragmentation mechanism is enabled. In practice, a passing mechanism between physical/data link layer and the network layer should be implemented as stated in Section 3.2 to help in passing information about what fragment size should be used and when the fragmentation is used between the layers as needed.

3.4 AODV and its Proposed Modifications

The Ad hoc On Demand Distance Vector (AODV) routing protocol is an on-demand routing protocol designed for ad hoc mobile networks. AODV not only builds routes only when necessary, but also maintains such routes only as long as data packets actively use the route. AODV uses sequence numbers to ensure the freshness of routes.

AODV builds routes using a route request-reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current source sequence number, and broadcast ID, the RREQ contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ sends a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it broadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If a node receives a RREQ which it has already processed, it discards the RREQ and do not forward it.

As the RREP propagates back to the source, nodes set up their forwarding pointers to the destination. Once the source node receives the RREP, it begins to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop-count, it updates its routing information for that destination and begins using the better route. As long as the route remains active, it continues to be maintained. A route is considered active as long as there are data packets periodically traveling from the source to the destination along that path. Once the source stops sending data packets, links time out and eventually are deleted from the intermediate node routing tables.

When a link break occurs while the route is active, the node upstream of the break propagates a route error message, RERR, to the source node to inform it of the now unreachable destination(s). On receiving such an RERR, the source node reinitiates route discovery, if it is still interested in a route to that destination node. A detailed description of the AODV protocol can be found in [101].

Our proposed modifications adhere to the on-demand philosophy, i.e. paths are still computed on-demand and as long as an existing path is valid, we do not actively change the path. Clearly other alternate designs are possible where even small changes in link error rates can be used to trigger exploration of better (i.e. more energy-efficient) paths. However, we view such a design as a deviation from the on-demand nature. Therefore, our proposed (energy-efficient) route computation instants are as original AODV either in response to a query for a new route, or to repair the failure of an existing route. To implement an energy-efficient AODV for reliable data transfer, we need to add two simple, but fundamental, capabilities at the wireless nodes:

1. Estimation of Bit Error Rates (BER) for different links.

2. On-demand computation of energy-efficient reliable routes.

3.4.1 Link Error Rates Estimation

As described in Section 3.2, bit error rates calculation depends on the power level of the received signal (Pr) and the ambient noise (N) surrounding a node. In order to estimate the error rates accurately, we need "good" measurements of Pr and N, and thus SNR. Generally, Pr and N vary with time: N varies due to the environment conditions, and Pr, which changes with distance, varies due to the nodes mobility. Consequently, we can not base our calculations on a single measurement. Rather we need to calculate those parameters as function of several measurements over a window of time, in order to capture the dynamics of the network.

We considered different approaches to calculate these measurements:

1. Instead of broadcasting single RREQ by each intermediate node during route discovery phase, each sender node broadcasts multiple RREQ packets in sequence separated by sampling period. To force the AODV layer of the receiver nodes to discard those entire RREQ packets except the last one, the TTL field of those RREQ packets is set to zero. The TTL field of the last RREQ packet is set to the regular TTL value. In this way, the receiver nodes calculate the parameter values using the measurements from those multiple RREQ packets. Although this approach follows the on demand theme however, it increases the duration of the route discovery phase, especially in large networks with expected long routes.

2. Each node periodically exchanges *Hello* packets with all its neighbors. In this method, nodes calculate and maintain the parameter values during their life time.

We choose to implement the second approach in which each node broadcasts *Hello* packet of small fixed size, at an average period t (one second in the implementation). To avoid accidental synchronization and consequently collisions, t is jittered by up to $\pm 0.25t$. The receiving nodes measure the SNR value for each received *Hello* packet, and uses this value to estimate the corresponding p of the incoming links as described in Section 3.2. Each node continuously updates its estimate of the SNR and the corresponding p using an exponentially weighted moving average of the sampled SNR values. As in all these averaging techniques, the estimation can be biased towards newer samples depending on the rate at which the noise conditions on the link changes. Similarly, the link error characteristics change with increasing node mobility and the estimation can be increasingly biased towards newer samples.

The *Hello* packets do not violate the AODV concept of maintaining routes on demand. The main reason is that each node maintains info about its links and it doesn't need to propagate this info to the neighborhood as in the case of the pro-active protocols. Broadcasting of *Hello* packets could change dynamically with the network traffics. One possibility, a node could stop broadcasting the *Hello* packets when it doesn't sense any traffic in the neighborhood and restart to broadcast them once it detects traffic.

3.4.2 Messages and Structures of AODV

To construct energy efficient route, nodes along the candidates paths need to exchange information about energy costs and loss probabilities within the route-discovery phase. Consequently, we added the following changes to the structures maintained by AODV (e.g., Broadcast ID and Routing tables) and to AODV messages (e.g., RREQ and RREP).

- **RREQ** Message: The information passed and accumulated through the RREQ messages is used by the destination node to judge which candidate paths has the minimum cost. One new field is needed:

- C_{req}: Stores the average energy cost to transmit a *single data bit* from the source to the current node along the path traversed by the RREQ message.

- **RREP** Message: The information passed through the RREP messages is used by each node along the reply path, to compute the cost of the partial route starting from the current node to the destination node. The new fields are:

- C_{rep}: Stores the average energy cost to transmit a *data bit* over the links traversed by RREP starting from the current node to the destination node.

- Fr_{rep}: The optimum fragment size, used by the receiving current node of the RREP message, to fragment the transmitted data packets on the next link towards the destination.

- $Bcast_{rep}$: This is the RREQ message ID that uniquely identifies the broadcast RREQ message which led to the generation of this RREP message.

- **Broadcast ID** Table: Each node maintains an entry in the Broadcast ID table for each route request query that is updated with each reception of RREQ. Based on those updates, the RREQ message either be dropped or forwarded as shown later.

- H_{bid}: The number of hops that has been traversed by the RREQ starting from the source node to the current node.

- C_{bid}: Stores the value of C_{req} field in the received RREQ.

- $Prev_{bid}$: Stores the ID of the node from which the current node received the RREQ. This entry is updated for each *received and forwarded* RREQ message by the current node.

- **Routing** Table: A node maintains an entry in the route table for each destination it has a route for. The new fields in this table are:

- C_{rt}: Stores the value of C_{req} field in the RREQ message or the C_{rep} field in the RREP message received by the current node. This field is used as an estimate of the cumulative upstream/downstream cost from this node to the source/destination node.

- Fr_{rt}: Stores the value of Fr_{rep} field in the RREP message. This value represents the optimum fragment size to transmit data packets on the next link toward the destination. It is passed to the IEEE 802.11 MAC layer with each transmitted packet either through API call or a special field within the packet. The MAC layer partitions the packet to fragments each with maximum size equal to Fr_{rt}.

In the rest of this section, we describe the operation of the route discovery (generation and processing of RREQ and RREP messages).

3.4.3 Route Discovery

AODV Routed discovery consists of two phases: route request phase and route reply phase. We now describe our modifications to these two phases.

Algorithm 1: ROUTE REQUEST HANDLER()

procedure RECVREQUEST(*RREQ* packet)

INPUT :

The received *RREQ* packet

VARIABLE :

BID : The broadcast ID table

n_{i-1} : Node transmitted this *RREQ*

n_i : Node receiving this *RREQ*

l : Link $\langle i-1, i\rangle$ *RREQ* traversed

${k_l}^*$: Optimum fragment size over link l (Equation 3.5)

H_{req} : Number of hops traversed by this *RREQ* message

ALGORITHM :

main

Calculate ${k_l}^*$

$\mathbf{C}_{req} \leftarrow C_{req} + \frac{v\times(o_1+{k_l}^*)}{({k_l}^*-o_2)(1-p_l)^{{k_l}^*}}$ (i)

$\mathbf{H}_{req} \leftarrow H_{req} + 1$

Search BID for Bid_{req}

if (Found an entry in BID**)**

then **if** **(**$(C_{req} \geq C_{bid})$ **or** $(C_{req} = C_{bid}$ **and** $H_{req} \geq H_{bid})$**)** (ii)
then $return$

else Add corresponding *RREQ* entry in BID

$\mathbf{H}_{bid} \leftarrow H_{req}, \mathbf{C}_{bid} \leftarrow C_{req}, \mathbf{F}r_{bid} \leftarrow {k_l}^*, \mathbf{P}rev_{bid} \leftarrow n_{i-1}$

Update the reverse route information (as in original AODV)

if n_i **(** the destination **or** have path to the destination**)**

then
Prepare the reply packet *RREP* and initialize its new fields as:
$\mathbf{C}_{rep} \leftarrow \frac{v\times(o_1+{k_l}^*)}{({k_l}^*-o_2)(1-p_l)^{{k_l}^*}} + C_{rt}$
comment: $C_{rt} = 0$ in case of n_i is the destination
$\mathbf{F}r_{rep} \leftarrow {k_l}^*, \mathbf{B}cast_{rep} \leftarrow Bid_{req}$
Send *RREP* to $Prev_{bid}$ node

else Forward the *RREQ* to n_i neighbors

Route Request Phase

Algorithm 1 describes the steps a node follows when it receives a RREQ message in modified AODV route request phase. The source node triggers the route discovery by broadcasting a RREQ message initialized with $C_{req} = 0$ (other fields are initialized as in the original AODV algorithm). When an intermediate node n_i receives RREQ message from a previous node n_{i-1}, it updates fields in the RREQ message (line (i) of Algorithm 1).

Node n_i examines the broadcast identification number [2] (Bid_{req}) stored in the RREQ message to check if it has seen any previous RREQ message belongs to the same route request phase or not. If this is the first instance for this RREQ or the cost associated with this RREQ is lower than the known one by the node n_i (line (ii) of Algorithm 1), the node adds a new entry in its *Broadcast ID* table and initializes its values as $H_{bid} = H_{req}$, $C_{bid} = C_{req}$, and $Prev_{bid} = n_{i-1}$ where H_{req} is the number of hops traversed by this RREQ messages that is stored within the RREQ message. Otherwise a previous RREQ message has been seen by the node n_i. In this case it compares the updated cost value in the RREQ message with that stored in the *Broadcast ID* table entry. If the boolean expression in line ii of Algorithm 1 evaluates to false, then this RREQ message is further forwarded. Otherwise the currently best known route has lower cost than the new route discovered by this RREQ message, and so is discarded.

As described in our modification, the intermediate nodes may broadcast multiple

[2] The broadcast identification uniquely identify all the RREQ messages belonging to the same route request phase.

RREQ messages for the same route request phase, as an opposite to a single RREQ message in original AODV. Although this broadcast costs more energy, experiments show that this overhead cost is marginal to the total energy saving.

Route Reply Phase

In AODV, the route reply (RREP) message can be generated by either the destination, or by an intermediate node that is aware of *any* path to the destination. Last part in Algorithm 1 shows how the destination node or an intermediate node that has a well-known route to the destination[3] generates and forwards RREP message.

In our modified version of AODV, the generation of RREP message is based on the cost of the candidate paths. If the destination node receives a set of RREQ messages from different paths, it chooses the path with the lowest cost among these alternatives and generates a RREP message along this path. Since the destination node receives multiple RREQ messages it has two choices: 1) Immediately reply with a RREP message for each better (i.e. more energy-efficient) route discovered by a new RREQ message, or 2) Wait for a small timeout to allow all RREQ messages to discover routes, and then send a single RREP response for the best discovered route. Clearly, the former approach will allow the destination node to select the optimum route at the expenses of transmitting multiple RREP messages. The later approach results in just a single transmission of RREP message at the expense of higher route setup latency. We choose to implement the first approach of sending multiple RREP messages.

Algorithm 2 describes how a node handles a RREP message in the modified route

[3] By ”well-known” we mean that the cost of the route from the current node to the destination is known.

Algorithm 2: ROUTE REPLY HANDLER()

procedure RECVREPLY(*RREP* packet)

INPUT :

The received *RREP* packet

VARIABLE :

RT : The routing table

BID : The broadcast table

n_i : Node receiving this *RREP*

$SeqNo$: Sequence number for the destination

H : Number of hops to the destination

ALGORITHM :

main

Search RT for an entry of the destination

if **(**Found an entry in RT**)**

then $\begin{cases} \textbf{if } ((SeqNo_{rep} < SeqNo_{rt} \textbf{ or } (C_{rep} \geq C_{rt}) \textbf{ or} \\ \quad (C_{rep} = C_{rt} \textbf{ and } H_{req} \geq H_{rt})) \\ \textbf{then } return \end{cases}$

else $\{$**A**dd entry in RT for the destination

comment: **U**pdate the fields of RT

$\mathbf{H}_{rt} \leftarrow H_{rep}, \mathbf{C}_{rt} \leftarrow C_{rep}, \mathbf{F}r_{rt} \leftarrow Fr_{rep}$

if **(**n_i is the source**)**

then $return$

else $\begin{cases} \textbf{G}\text{et the BID entry corresponding to } Bcast_{rep} \\ n_{i-1} \leftarrow Prev_{bid} \\ \textbf{C}\text{alculate the } {k_l}^* \text{ where } l \text{ is the link } \langle i-1, i \rangle \\ \mathbf{C}_{rep} \leftarrow \frac{v \times (o_1 + {k_l}^*)}{({k_l}^* - o_2)(1-p_l)^{{k_l}^*}} + C_{rep} \\ \mathbf{F}r_{rep} \leftarrow {k_l}^* \\ \textbf{S}\text{end } RREP \text{ to } n_{i-1} \text{ node} \end{cases}$

reply phase. Similar to RREQ message, when a node receives a RREP message for the first time or the received one has route with lower cost, it updates the entry in the *Routing* table corresponding to this RREP. Then, the RREP message are appropriately updated and forwarded to $Prev_{bid}$ node.

As described above, the node may forward multiple RREP messages in response to better routes found by successive RREQ messages that indicate progressively lower-cost routes.

3.5 Performance Evaluation

We perform detailed simulation-based studies on the performance of the AODV protocol, both with and without our modifications. The performance comparisons were done using the *ns-2* simulator, enhanced with the CMU-wireless extensions (the underlying link layer is IEEE 802.11 with 11 Mbps data rate). *We extend ns-2 version 2.1b8a with the full implementation of the IEEE 802.11 fragmentation mechanism*. We perform a detailed study of the AODV protocol and our energy-efficient variants, under various noise and node mobility conditions.

We model various scenarios of channel noise, interference between nodes due to channel contention, node mobility and their effects on performance. To study the performance of our suggested schemes, we implement and observe three separate routing schemes:

a) The Shortest-Delay (**SD**): The original AODV routing protocol that selects the route with the minimum latency.

b) The Energy-Aware (**EA**): Enhances the AODV protocol by considering the energy cost of a single bit transmission (without retransmission considerations) across that link. The cost calculation depends only on the route length and doesn't consider the link error rates in a similar manner to [114]. However, this algorithm selects, among the different candidate routes of the same cost, the one with the highest packet delivery probability.

c) Our Retransmission-Energy Aware (**RA**): Enhances the AODV protocol. The link cost considers the impact of retransmissions necessary for reliable packet transfer.

We run each one of the above schemes on IEEE 802.11 *fragmentation-disabled* version (SD_fix, EA_fix, and RA_fix), as well as *fragmentation-enabled* version (SD_var, EA_var, and RA_var). For fragmentation-disabled version, packets are transmitted at their original sizes. On the other hand, the MAC layer of the fragmentation-enabled version schemes exploits the fragmentation availability by partitioning the packets, over each link, to the optimum fragment size in order to increase the transmission reliability. *Only* RA_var scheme is aware of the fragmentation mechanism and *use* it in its route computations to obtain the best energy-efficient route.

We adopt RTS/CTS mechanism in the IEEE 802.11 MAC layer because of the following:

- RTS and CTS frames are small in size and consume a very little energy compared with the data packets. They do not get affected by the link error rates except in environments with very high error rates.

- Since RTS/CTS frames reduces the collision probability, using RTS/CTS mecha-

Parameter	*Value*	*Comments*
Packet Payload	1500 bytes	data frame payload length
MAC header	28 bytess	MAC layer overhead
PLCP Preamble	144 bits	PLCP Preamble overhead length
PLCP Header	48 bis	PLCP Header overhead length
ACK	14 bytes	ACK frame length
RTS	20 bytes	RTS frame length
CTS	14 bytes	CTS frame length
$Retran_{max}$	6	maximum retransmission trials
$Fragment_{min}$	150 bytes	minimum fragmentation size
f	11 Mbps	data transmission rate
W	22×10^6 Hz	channel bandwidth
Pt	0.281838 W	transmission power level
G_t	1.0	transmitter gain
G_r	1.0	receiver gain
h_t	1.5 m	transmitter height
h_r	1.5 m	receiver height
L	1.0	system loss factor
λ	0.125 m	signal wavelength

Table 3.2: The parameter values used in simulation in addition to the standards values defined in [9].

nism factors out the effect of collisions from our results.

- RTS/CTS frames are used in the AODV as a detection mechanism for link failure (absence) rather than using data packets. The link is triggered as broken if no CTS frame is received for a number of consecutive trials of a RTS frame (in our case we set that number to 4). In noisy environments, dropping consecutive data packets is most probably due to error rates and not to a links absence.

Table 3.2 summarizes the parameter used in our simulation[4].

[4]Note that the PLCP preamble, PLCP header, RTS frame, and CTS frame are sent at the basic access rate

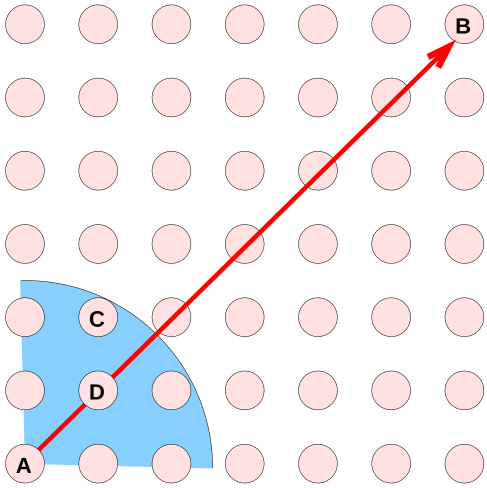

Figure 3.3: The 49-node grid topology. The shaded region marks the maximum transmission range for the node, A. $A \rightarrow B$ is one of the example flows used on this topology.

3.5.1 Network Topology and Link Error Modeling

For our experiments, we use different topologies each having 49 nodes distributed over on a 700×700 square region. The maximum transmission radius of a node is 250 units. We present results for three different topology scenarios:

- *Static Grid:* Nodes are immobile and equi-spaced along each axis as shown in Figure 3.3.
- *Static Random:* Nodes are immobile and uniformly distributed over the region.
- *Mobile Random:* Nodes are distributed uniformly at random over the region and allowed to move around using the random waypoint model [62] with zero pause time.

In all our simulations we use a set of 12 flows that were active over the duration of the experiment. We use both TCP and UDP flows for different experiments. For the

UDP flows, we choose the traffic sources to be constant bit rate (CBR) sources at rate of 5 packets per second. For the TCP flows, we use its NewReno variant. The UDP packets and TCP segments were 1500 bytes each. Each of the simulation runs for a fixed duration of 250 seconds including a warm up period of 50 seconds. Transmission flows start in serial with gap of 5 seconds between consecutive flows. Each point in the results is the average of 10 runs. For all the simulations, the energy cost to transmit single bit on a single attempt over a link was chosen to be 60μJ.

All the control packets, e.g., probe packets, RREQ, RREP messages, IEEE 802.11 RTC/CTS/ACK frames, as well as the data packet experience the same bit error rate (BER) of a wireless link which depends on the ambient noise level as shown in Equation 3.1. We partition the entire square region into small square grids (50×50 units each). We model the ambient noise of each of these small square regions as independent identically distributed white Gaussian noise of μ mean and standard deviation σ. The noise mean μ for the different small square grids was chosen to vary between two configurable parameters, N_{min} and N_{max} corresponding to minimum and maximum noise respectively, while the noise standard deviations σ was chosen to be equal to $(0.1 \times \mu)W$. We use different distributions for the μ over the entire region for different experiments as follow:

1. *Fixed Noise Environments:* N_{min} is equal to N_{max} and their values vary between $0.0W$ and $20.0 \times 10^{-11}W$.

2. *Random Noise Environments:* We fix N_{min} to $0.0W$ and vary N_{max} between $0.0W$ and $20.0 \times 10^{-11}W$.

Our results show that the other schemes are as good as the RA_var scheme only in zero noise environments. For all other cases, the RA_var scheme shows significant performance improvement, with the performance gain becoming larger with increasing levels of noise.

3.5.2 Metrics

To study the energy efficiency of the routing protocols, we observed the following metrics:

1. **Average Energy:** Computed per data bit delivered to the destination by dividing the total energy expenditure (over all the nodes in the network) by the total size in bits of the data units (sequence number for TCP and packets for UDP) received at any destination. It includes energy consumption due to control packets (e.g. RREQ, RREP messages, IEEE 802.11 RTS/CTS packets etc.) as well as the data packets. *The cost of periodic* Hello *packets is included only in our modified schemes (i.e. RA_fix and RA_var).* This metric is plotted in the logarithmic scale. Note that we plot the transmission energy cost only and not the reception energy cost since the reception cost is a scale of the transmission cost.

2. **Effective Reliable Throughput:** Counts the number of packets reliably delivered to the destinations. Note that different schemes are able to transfer a different number of packets over an identical time interval. Since all the experiments have been performed over identical durations, we do not actually divide this packet count by the simulation duration. Instead we simply compare the total number of packets successfully transferred over this duration.

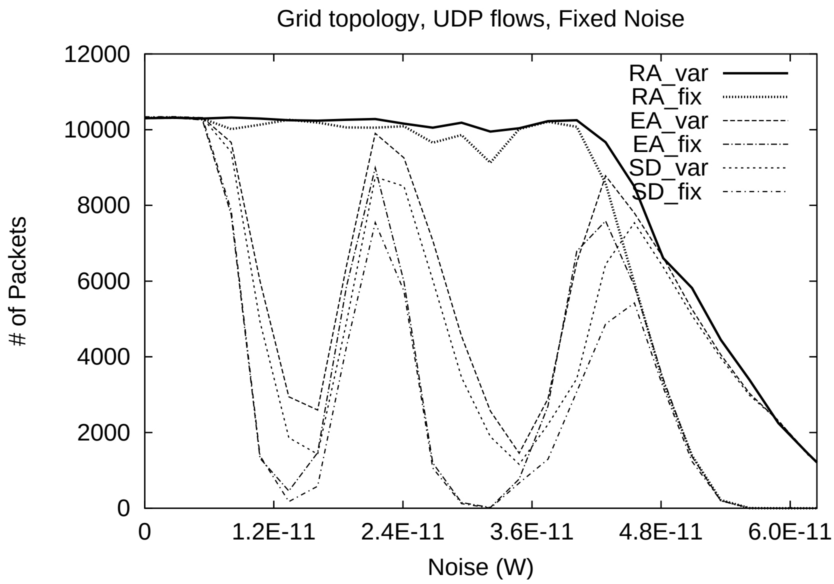

Figure 3.4: Effective reliable throughput for UDP flows, Grid Topology in Fixed Noise Environments

3. **Average Path Length:** Shows the average number of hops traversed by a data packet.

4. **Average Path Lifetime:** Counts the average time in which a path is active and carries data packets. Time needed for route discovery phase or route maintenance phase is not included in this metric.

3.5.3 Static Grid Topologies

Our static grid topology of 49 nodes is shown in Figure 3.3. Figures 3.4 and 3.5 show the effective reliable throughput and the average energy cost for experiments with fixed noise environments for UDP flows. Note that each data point on the plot corresponds to an experiment with a specified fixed noise value for the entire square region. Clearly for

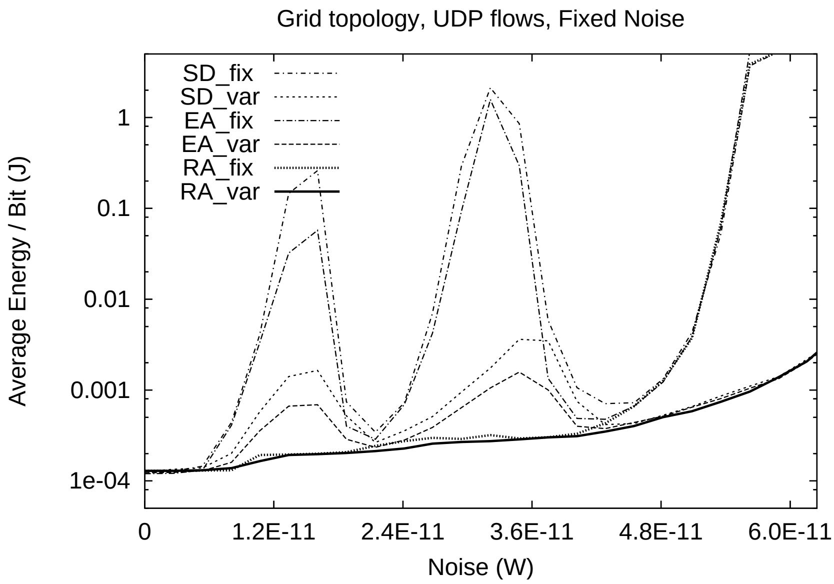

Figure 3.5: Average energy cost for UDP flows, Grid Topology in Fixed Noise Environments

very low noise environments, all schemes are equivalent. However, as the noise starts to increase, the RA schemes (RA_fix and RA_var) show significant benefits. It is interesting to note that for EA and SD schemes, the effective reliable throughput does not decrease monotonically. This is an interesting phenomenon that is related to the relative size of the RREQ and the data packets.

To explain this phenomenon, consider flow $A - B$ in Figure 3.3. Both SD and EA schemes try to choose a path with minimum number of hops. Therefore, the first hop for this flow will be the link $\langle A, C \rangle$. For a static link, the p is constant and depends on the noise value and the received power, but the packet error rate is not. Packet error rate depends on the size of the packets and is smaller for RREQ packets than the data packets. When the noise on the grid is $1.25 \times 10^{-11} W$, the p for the $\langle A, C \rangle$ link is 0.0008. The corresponding packet error rate for RREQ packets is about 0.5. Therefore RREQ packets sent by node A is correctly received at C in about 50% of the cases and the link $\langle A, C\rangle$ is chosen by both SD and EA schemes. However, the packet error rate experienced by the data packets on the same link is nearly 1. This causes significant losses for data packets and therefore the throughput achieved is lower. However, when the noise level increases (i.e. say $1.80 \times 10^{-11}W$), the p on the link goes up (i.e. to 0.00186). This causes the packet error rate for RREQ packets to increase to 0.8. Therefore most of these RREQ packets get lost across link $\langle A, C\rangle$. Consequently both SD and EA schemes shift to paths with shorter hops (which also have lower p) and their performance starts to increase again.

The RA schemes do not suffer from this anomalous behavior. This is because the RA schemes choose routes based on the p. Therefore, they automatically avoid links with high packet error rates for data packets. Both EA and SD schemes are oblivious of link errors and cannot make such intelligent choices. This behavior is clearly visible in the grid topology since the number of alternative paths are discrete and few. Since the number of path alternatives are discrete and few, RA_var has marginal benefit, both in energy and throughput, over RA_fix at low noise values. At noise values greater than $4.30 \times 10^{-11}W$, RA_fix performance degrades rapidly and faster than RA_var.

Figures 3.6 and 3.7 show the corresponding plots for the random noise environments. The EA and SD schemes consume about 140% more energy per successfully transferred data bit than the RA schemes, when the maximum noise is bigger than $2.50 \times 10^{-11}W$ and still achieves only half the throughput of the RA schemes. Clearly, due to high number of available alternative for route selection, RA_var performs much better than RA_fix scheme. In high noise environments, the RA_var scheme consumes about 77% less energy than RA_fix while maintaining about double the throughput.

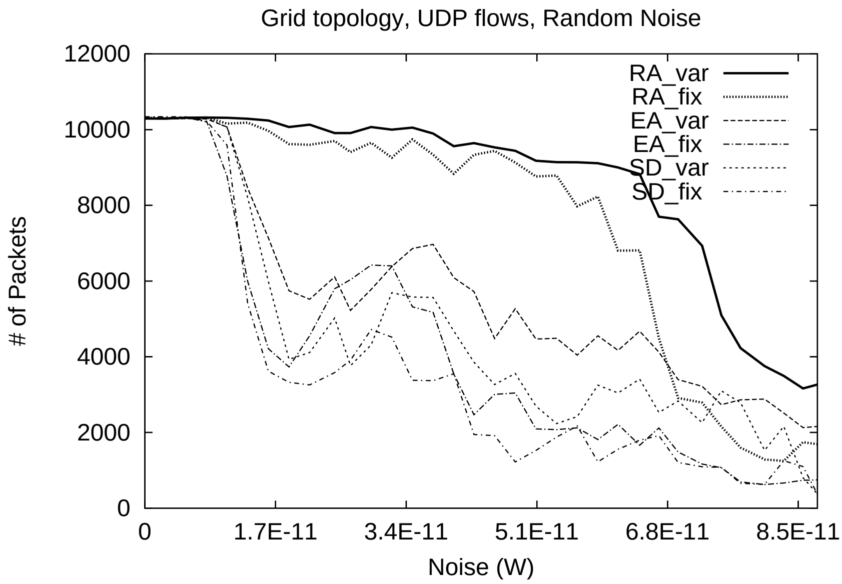

Figure 3.6: Effective reliable throughput for UDP flows, Grid Topology in Random Noise Environments

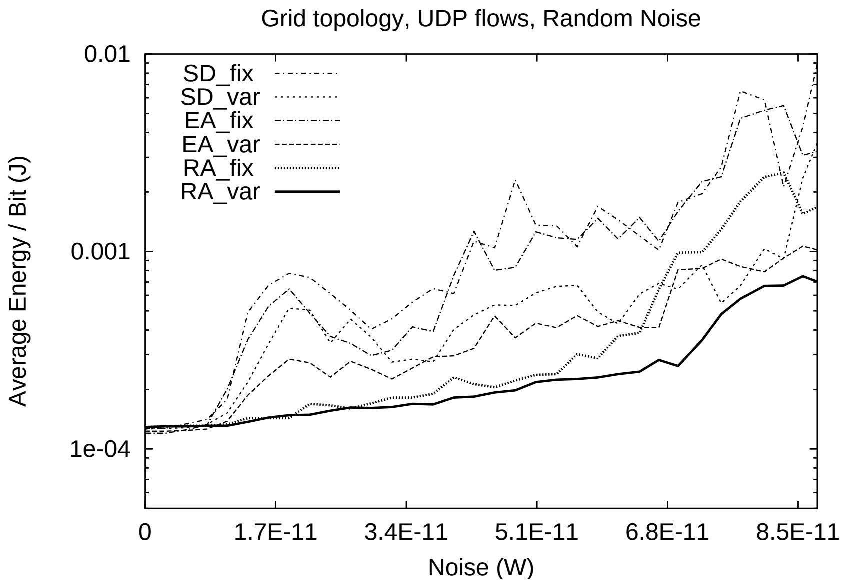

Figure 3.7: Average energy cost for UDP flows, Grid Topology in Random Noise Environments

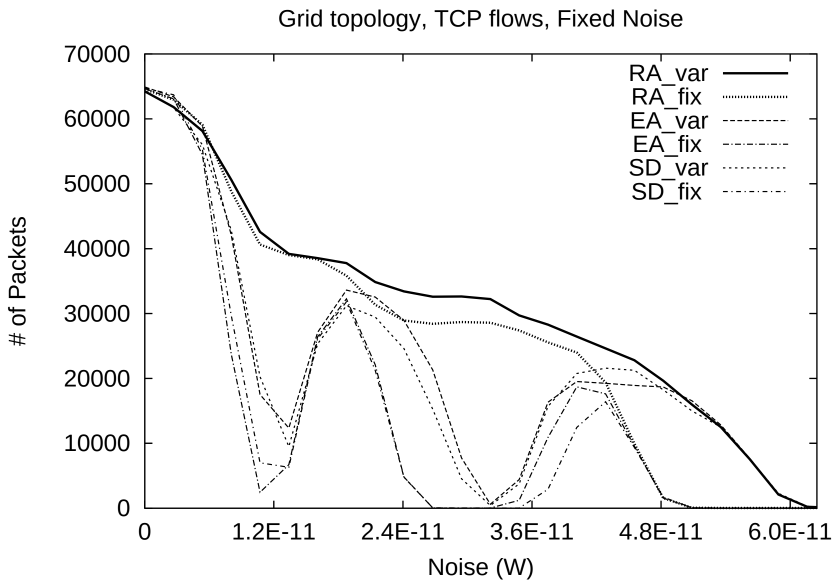

Figure 3.8: Effective reliable throughput for TCP flows, Grid Topology in Fixed Noise Environments

It is clear that the RA scheme has the highest effective reliable throughput among all the schemes especially with high links error rates. The RA scheme has the lowest energy requirements among all the schemes. From the figures, the throughput of RA scheme reaches about 50 times of the throughput or SD and EA schemes. Also the energy consumption of SD and EA schemes reaches about 50 times of the energy consumption of RA scheme.

Experiments with TCP flows show a similar performance. The case for fixed noise environments is shown in Figures 3.8 and 3.9. It is interesting to observe the different behavior of the effective reliable throughput metric for the different schemes (UDP and TCP). For TCP flows, the number of packets transmitted reliably for SD and EA schemes is dropped rapidly to zero for long ranges of noise. The decreasing trend in both these schemes is due to the increasing link error rates with the increase in noise. As the link

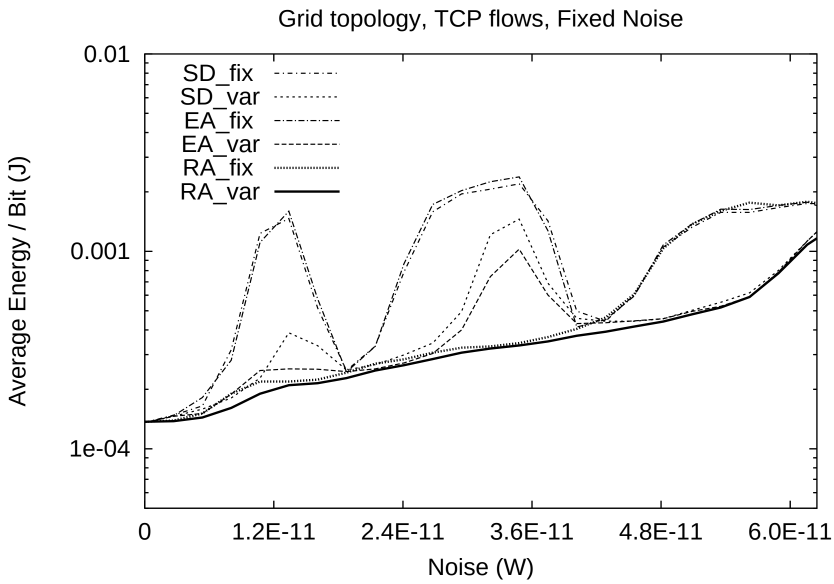

Figure 3.9: Average energy cost for TCP flows, Grid Topology in Fixed Noise Environments

error rates increase, packets see an increase in end-to-end delays due to the overhead delays spent in the increased number of retransmissions needed to ensure reliability. This indicates that the effect of our scheme has impressive effect on the TCP flows more than the UDP flows.

Figures 3.10 and 3.11 show the average number of hops per flow for fixed and random noise environments respectively. Both EA and SD schemes produce curves with average number of hops less than those of RA_fix and RA_var. This is because both techniques try to minimize number of hops. Figure 3.10 shows that RA_var performs better than RA_fix in specific regions of noise. But Figure 3.11 shows that RA_var outperforms RA_fix for almost all noise regions because of the large number of alternatives for route in random noise environments. In general, decreasing number of hops per flow reduces number of active links, which in turn reduces the number of active nodes. Therefore,

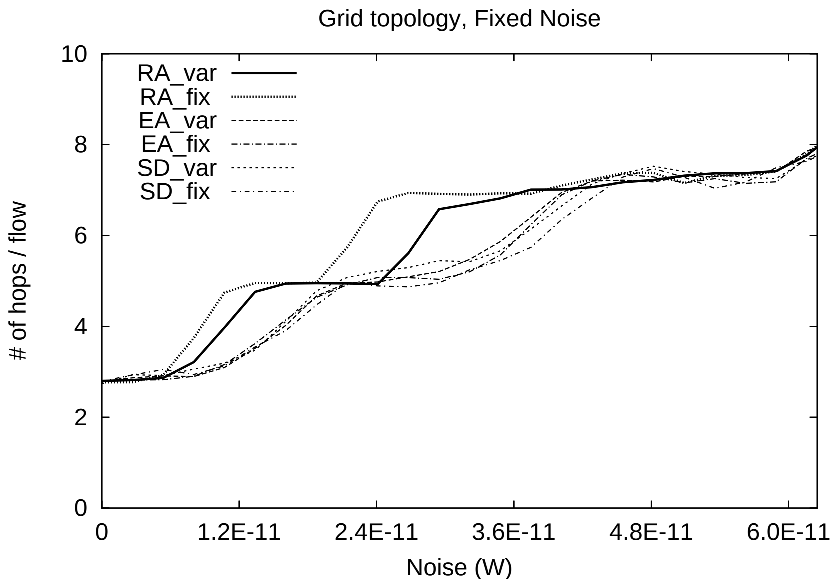

Figure 3.10: Average number of hops/flow, Grid Topology in Fixed Noise Environments

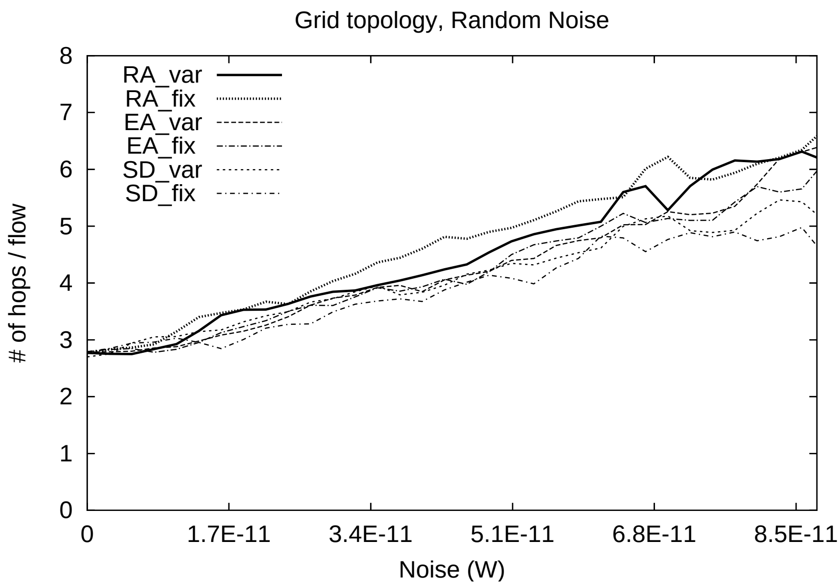

Figure 3.11: Average number of hops/flow, Grid Topology in Random Noise Environments

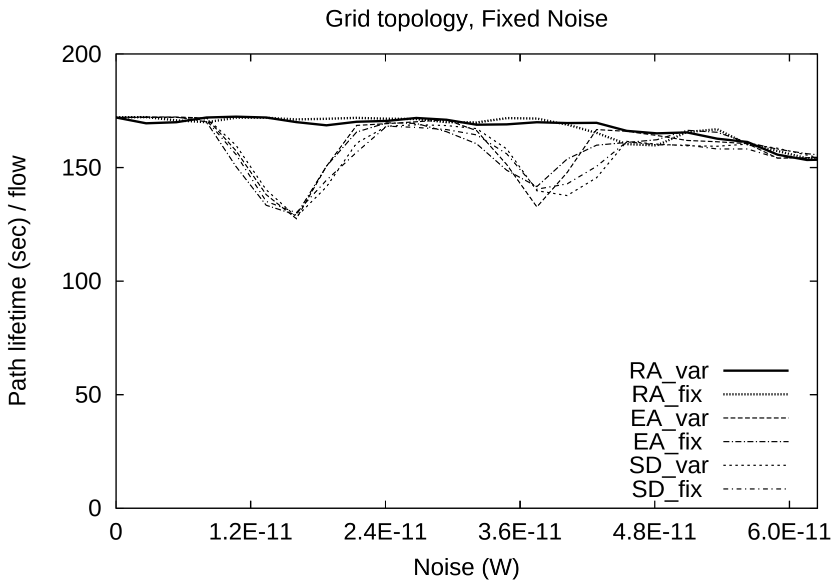

Figure 3.12: Average path lifetime, Grid Topology in Fixed Noise Environments

RA_var in comparison to RA_fix has the following impacts: (1) reduces the network load, (2) increases the network lifetime, and (3) scales better with number of flows.

Figures 3.12 and 3.13 show the average path lifetime per flow for fixed and random noise environments respectively. Note that this is a static topology in which links are not broken due to mobility but only due to dropping frames because of high error rates. Figure 3.12 shows that the path lifetimes of all schemes are similar to each other except at certain noise values for SD and EA schemes. As explained earlier, SD and EA schemes select short paths of links with high error rates. In this case, packets are dropped due to noise and consequently, AODV layer in the nodes at the receiver side of those links perceive those links as idle. Later, those links time out, and thus break the paths. This behavior occurs in small range values of noise as it appears in the curve notches in Figure 3.12. In case of random noise environments, SD and EA schemes have more

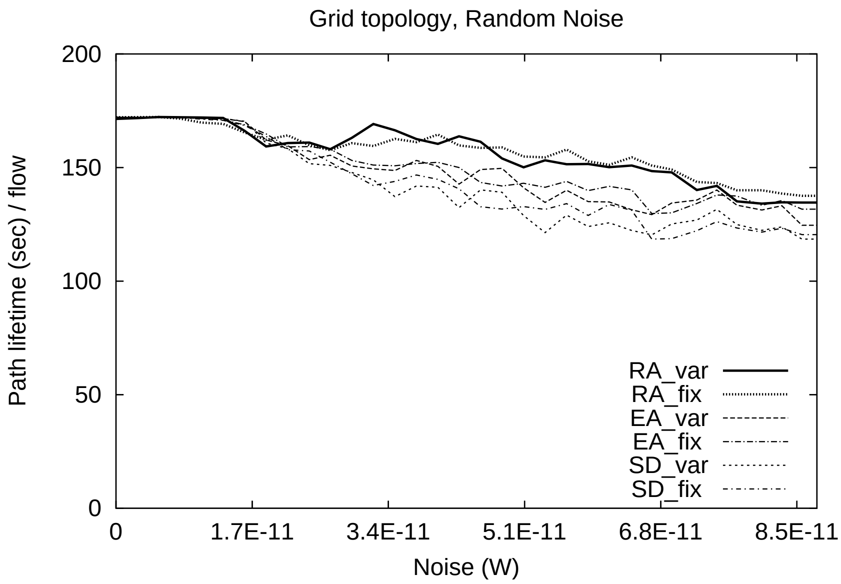

Figure 3.13: Average path lifetime, Grid Topology in Random Noise Environments

alternatives of short paths of links with high error rate. Therefore, the broken paths behavior occurs more frequently over a wide range of high noise values (contrary to the fixed noise case). This reduces their path lifetime as shown in Figure 3.13.

3.5.4 Static Random Topologies

Randomly generated static topologies show very similar behavior as the grid topology. As before, the RA schemes provide significant performance benefits over the SD and EA schemes. The results are shown in Figures 3.14, 3.15, 3.16, 3.17, 3.18, 3.19.

3.5.5 Mobile Topologies

Finally we present results of the experiments on randomly generated mobile topologies. Node mobility was based on the random waypoint model [62] where the maximum speed

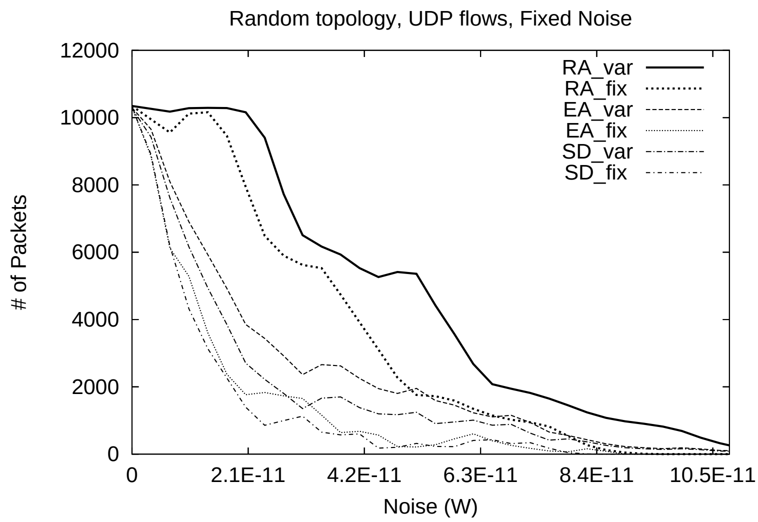

Figure 3.14: Effective reliable throughput for UDP flows, Random Topology in Fixed Noise Environments

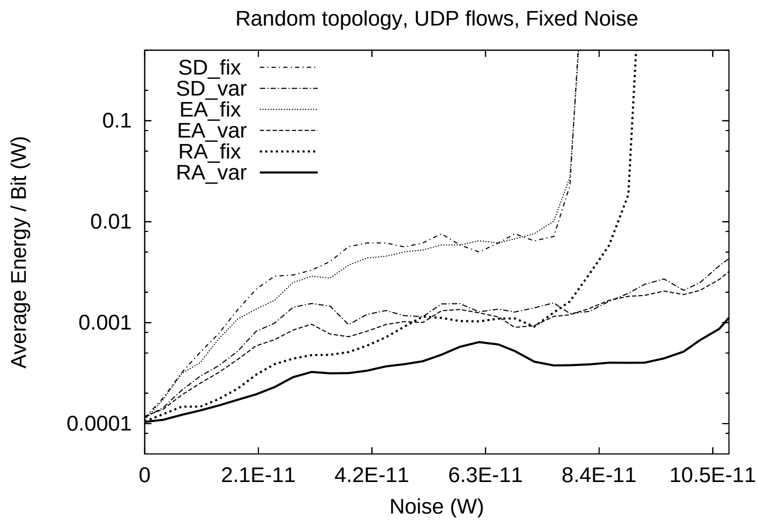

Figure 3.15: Average energy cost for UDP flows, Random Topology in Fixed Noise Environments

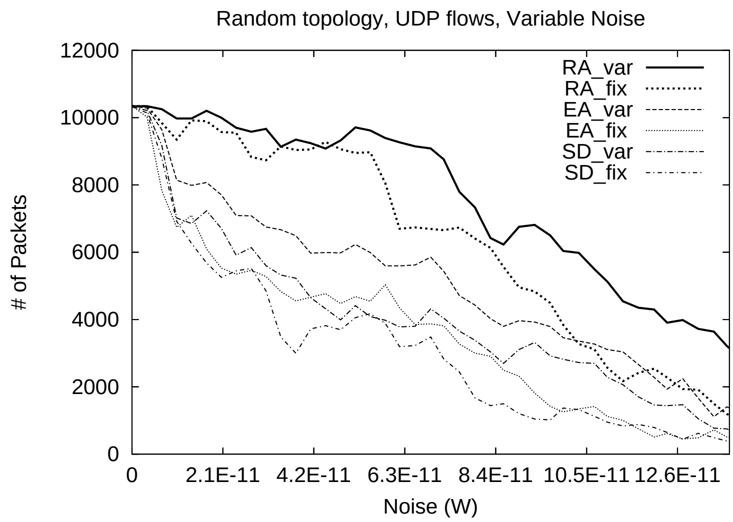

Figure 3.16: Effective reliable throughput for UDP flows, Random Topology in Random Noise Environments

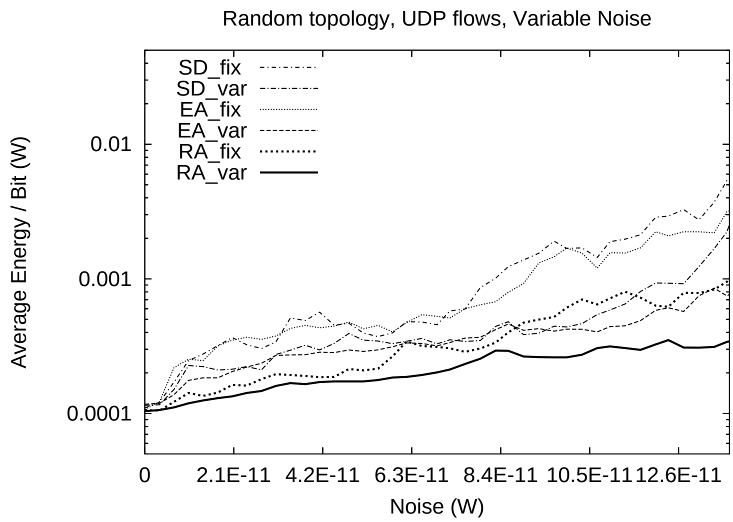

Figure 3.17: Average energy cost for UDP flows, Random Topology in Random Noise Environments

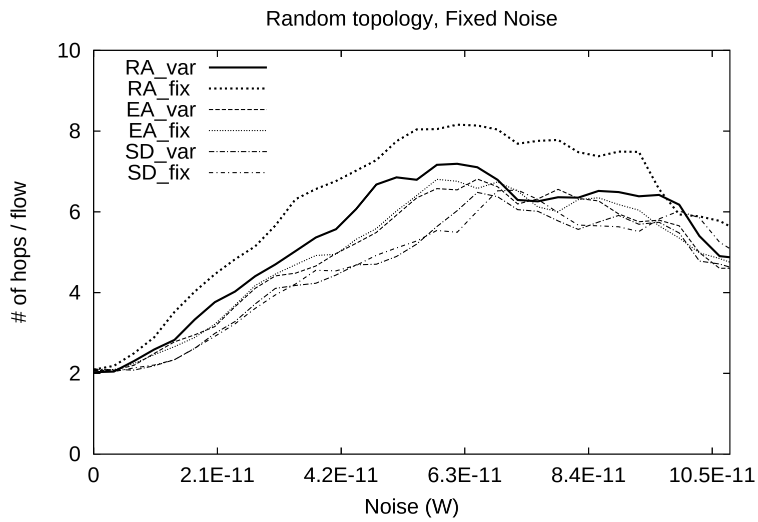

Figure 3.18: Average number of hops per flow, Random Topology in Fixed Noise Environments

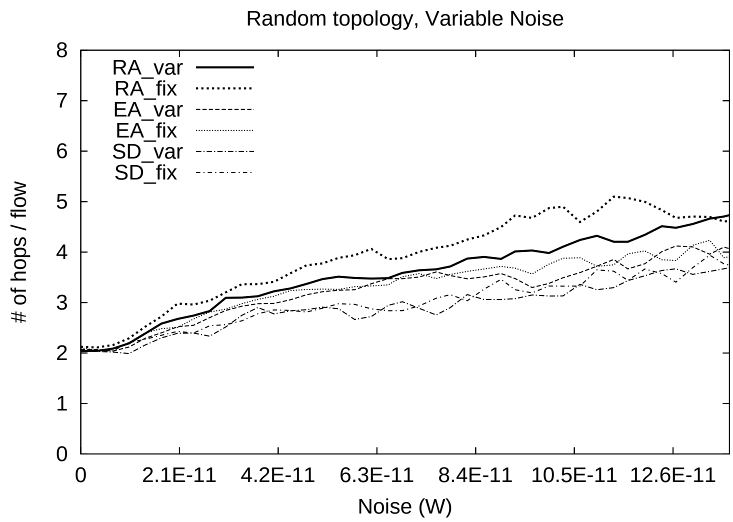

Figure 3.19: Average number of hops per flow, Random Topology in Random Noise Environments

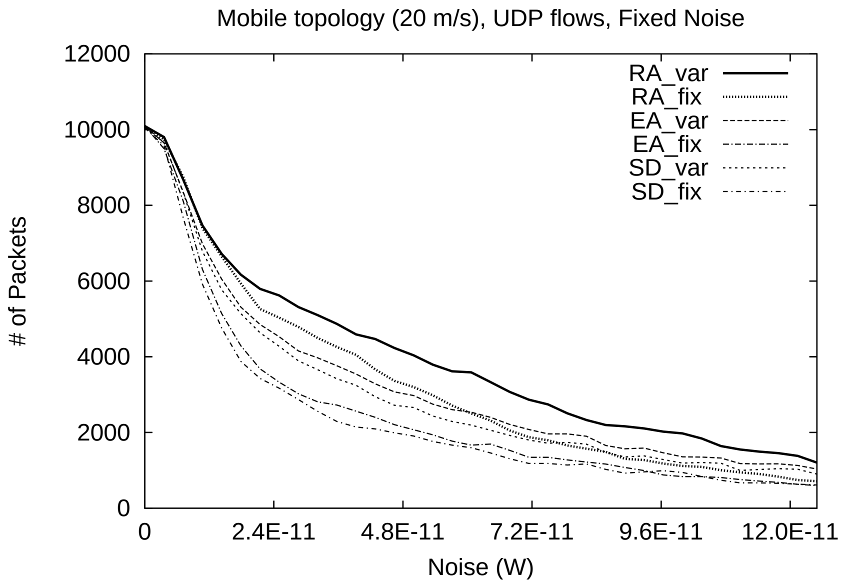

Figure 3.20: Effective reliable throughput for UDP flows, Mobile Topology in Fixed Noise Environments

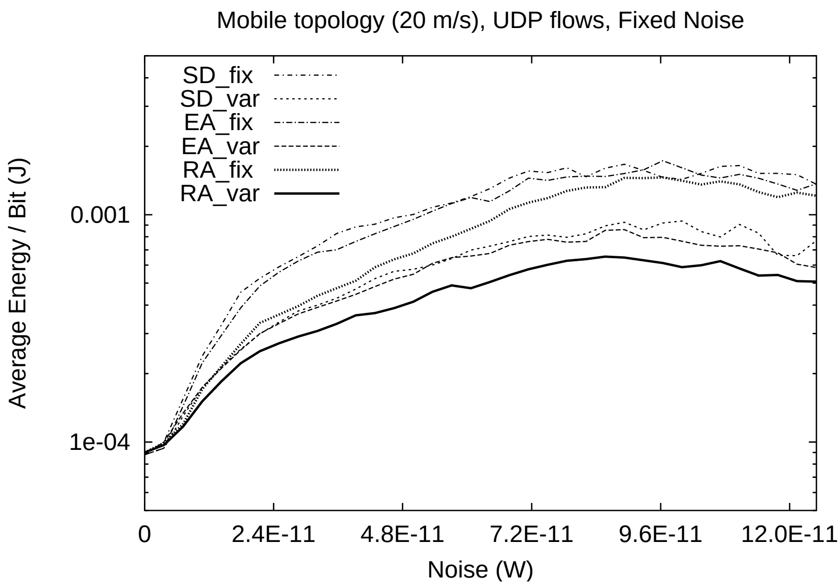

Figure 3.21: Average energy cost for UDP flows, Mobile Topology in Fixed Noise Environments

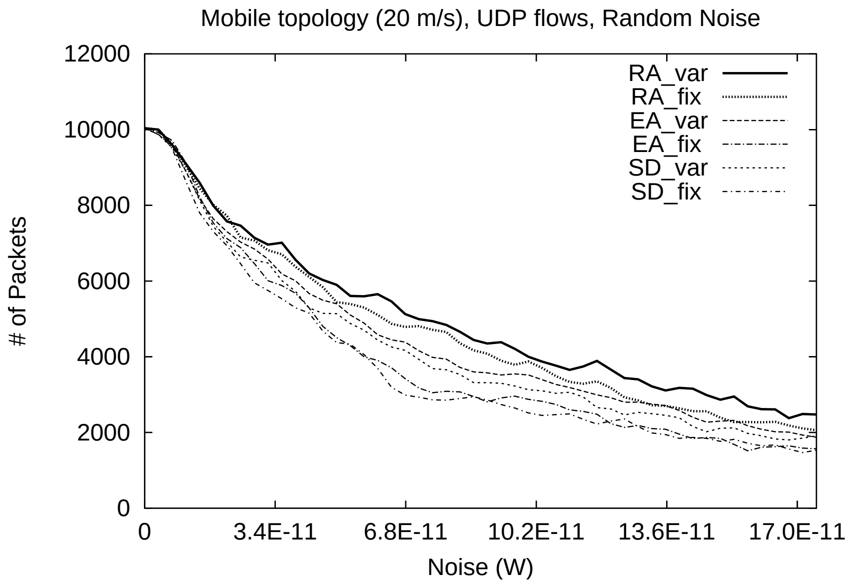

Figure 3.22: Effective reliable throughput for UDP flows, Mobile Topology in Random Noise Environments

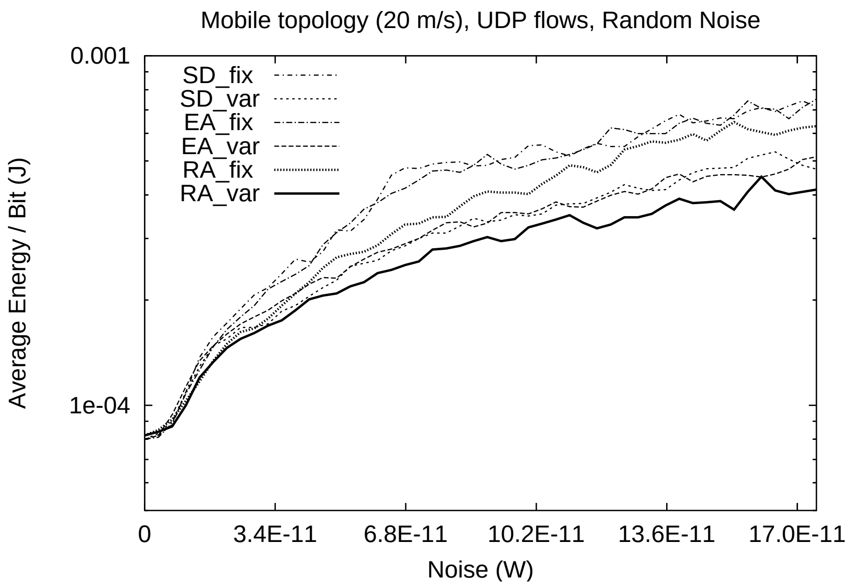

Figure 3.23: Average energy cost for UDP flows, Mobile Topology in Random Noise Environments

of a node was varied for different experiments[5]. In our simulation, we use a pause time of zero, which means that the nodes keep moving over the entire duration of the simulation. In this section we show the results for the case when the maximum speed of the wireless nodes is 20 m/s.

Figures 3.20 and 3.21 show the effective reliable throughput and the average energy per reliable delivered data bit respectively in the fixed noise environments. Figures 3.22 and 3.23 are the corresponding plots for the random noise environments.

A comparison with the static topologies indicates that mobility reduces reliable data throughput. In particular we also observe that the impact of mobility increases with increase in the channel noise. For example, in absence of channel noise, the reliable throughput achieved for the mobile topologies is about 5% lower than the corresponding static topologies. As the channel noise increases (e.g. maximum noise of 3.50 $\times 10^{-11}$ W) the data throughput achieved for the mobile topologies is significantly lower (e.g. about 40% less than the corresponding static topologies).

Figures 3.24 and 3.25 are the corresponding plots for the TCP flows in a random noise environments. Similar to UDP flows, the RA_var outperforms the other schemes both in energy cost and throughput. Comparing with the UDP flows, the end-to-end delays, due to the delays spent in increased number of retransmissions necessary to ensure reliability, has a significant effect on the TCP flows. This explains why the TCP throughput goes down faster than the UDP with the increase in the noise environments.

The results show that the other schemes are as good as the RA_var scheme only

[5]Since our simulations were performed over a relatively short duration of up to 5 minutes, and so we were not affected by the long term slowdown behavior of the random waypoint model [138].

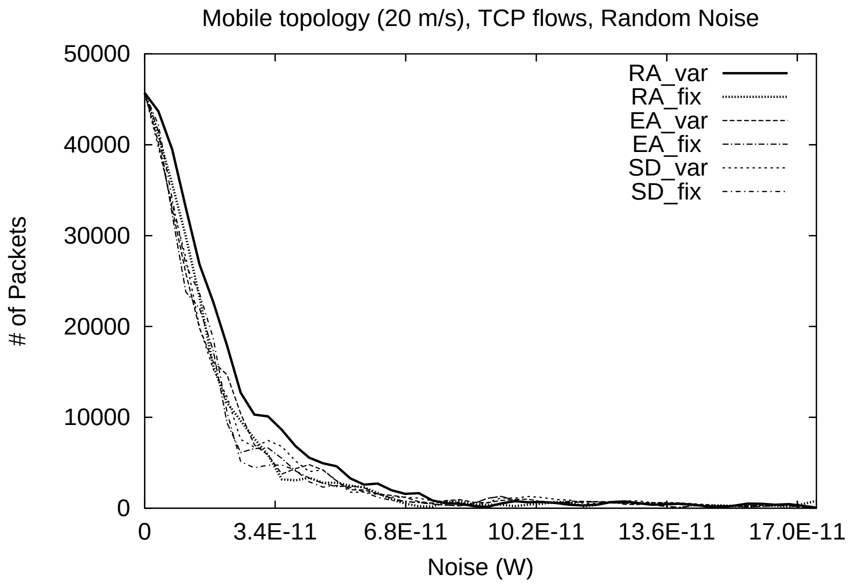

Figure 3.24: Effective reliable throughput for TCP flows, Mobile Topology in Random Noise Environments

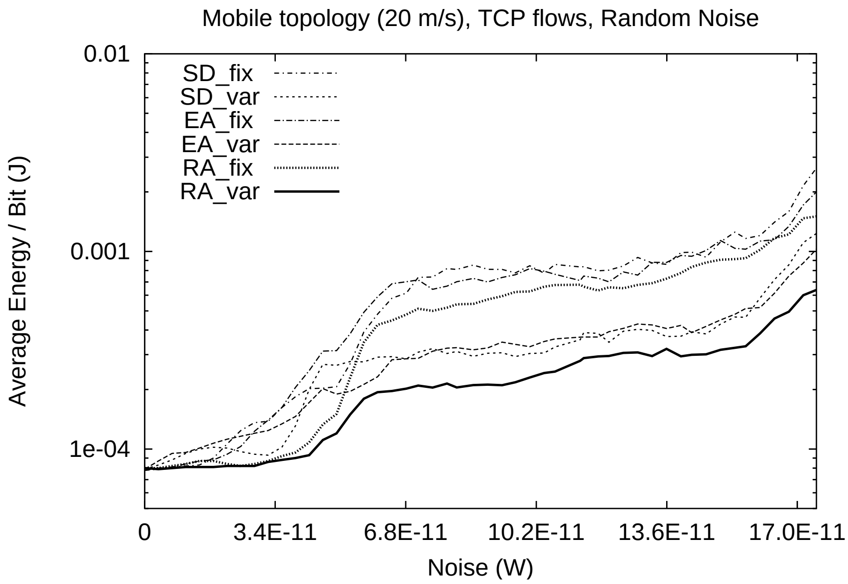

Figure 3.25: Average energy cost for TCP flows, Mobile Topology in Random Noise Environments

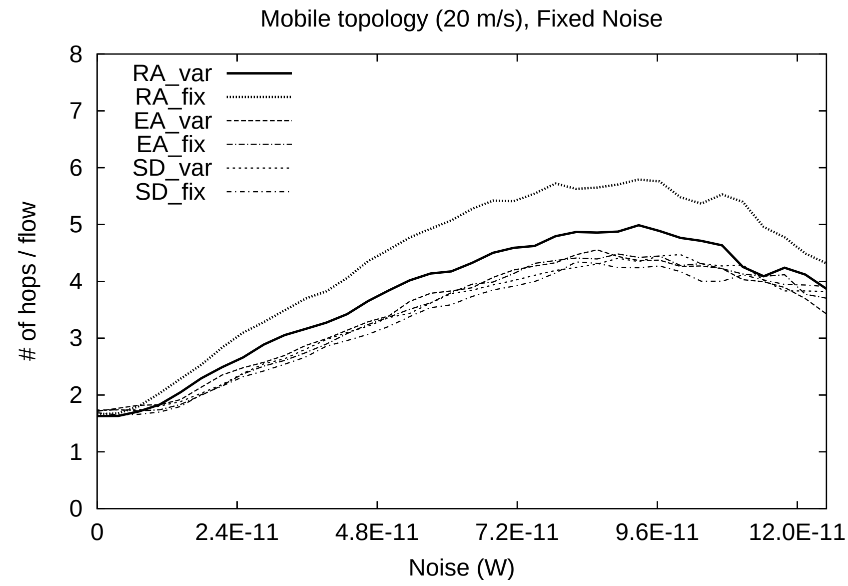

Figure 3.26: Average number of hops/flow, Mobile Topology in Fixed Noise Environments

in zero noise environments. For all other cases, the RA_var scheme shows significant performance improvement, with the performance gain becoming larger with increasing levels of noise.

As in the static topology, the average number of hops per flow for RA schemes is higher than the other schemes while RA_var maintains shorter paths than RA_fix. This is shown in Figures 3.26 and 3.27. Nodes mobility increases the chances of having minimum energy short paths, which explains the large difference between RA_var and RA_fix curves in comparison with the static topology.

The effects of mobility on the path lifetime are shown in Figure 3.28 and 3.29 for fixed and random noise environments respectively. The lifetime of the paths degrades gracefully with the increase in the noise level. However, the average path lifetime in both RA_fix and RA_var is larger than the other schemes with an explanation similar to the grid

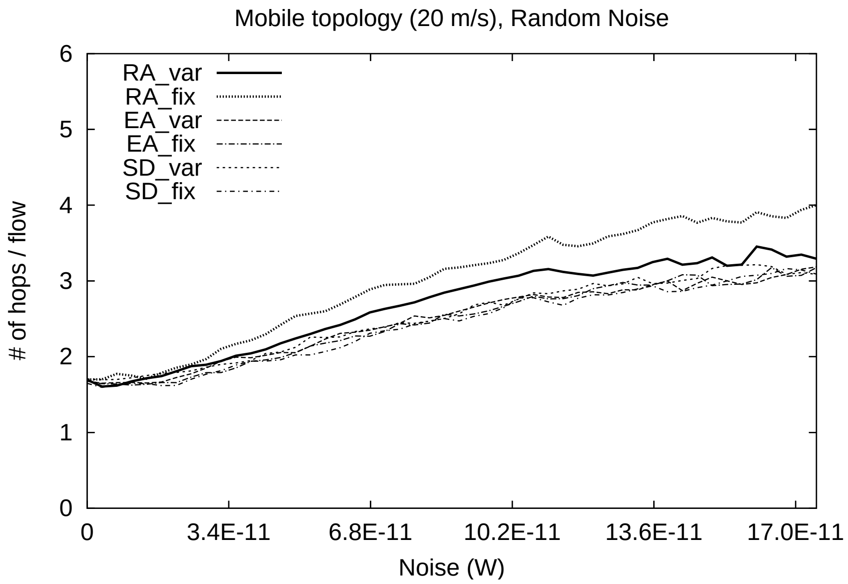

Figure 3.27: Average number of hops/flow, Mobile Topology in Random Noise Environments

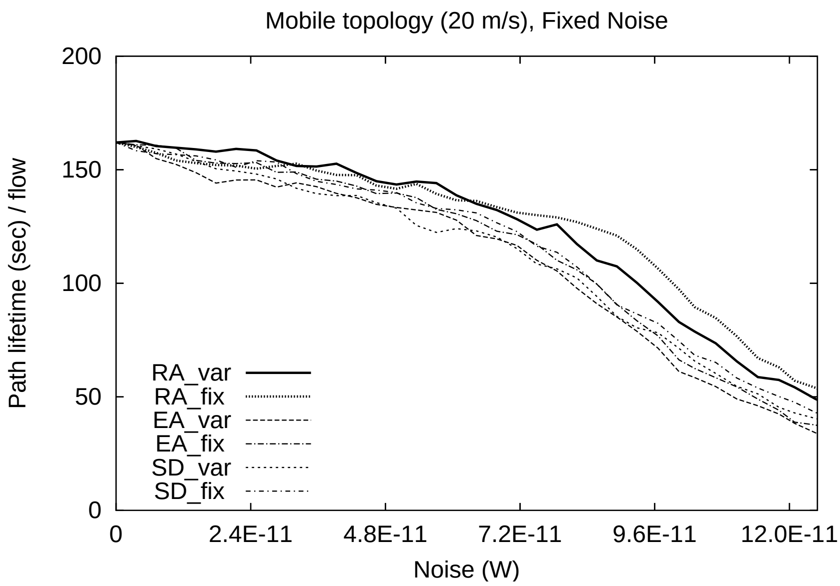

Figure 3.28: Average path lifetime, Mobile Topology in Fixed Noise Environments

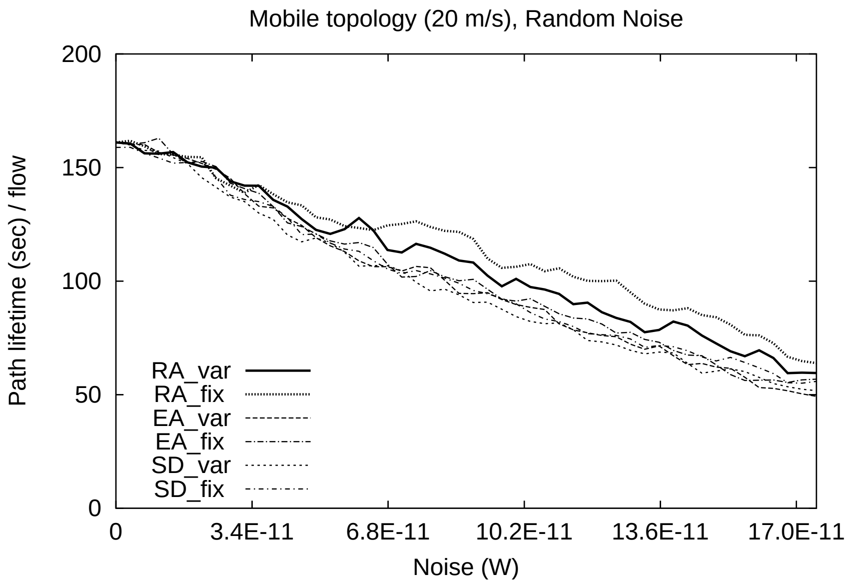

Figure 3.29: Average path lifetime, Mobile Topology in Random Noise Environments

topologies. An interesting observation from the curves is that the path lifetime in RA_var scheme is shorter than the corresponding time in RA_fix scheme which mean the rate of broken paths in RA_var is higher than the rate in RA_fix scheme. An explanation to that is RA_VAR tends to build shorter paths than RA_fix scheme as shown in Figures 3.26 and 3.27. Therefore, the average hop distance in RA_var paths is longer than the RA_fix paths and consequently, RA_var paths are more vulnerable to be broken because of node mobility than the RA_fix paths.

3.6 Conclusion

We have shown how AODV can be modified to compute minimum-energy routes, rather than ”shortest delay” routes. Our routing computations take into account the link error rates and its IEEE 802.11 retransmission consequences. Our modifications in routing layer take into account the cross layer interaction with the IEEE 802.11 layer by exploiting the available fragmentation mechanism in order to increase transmission reliability. From our description, however, it is obvious that our modifications and techniques can be ported and easily implemented in any alternative on-demand routing protocols (e.g., DSR and TORA).

Our simulations show that the retransmission-aware modification of AODV behavior can result in a significant (sometimes orders of magnitude) reduction in total energy consumption per packet, with the added benefit of higher throughput as well. In essence, the overhead of our energy-aware route establishment process (e.g., the periodic *Hello* packets, the forwarding of multiple RREQ and RREP) is more than compensated for by the lower energy consumed in data forwarding. The results, also, show that using packet fragmentation in routing in addition to retransmission cost (RA_var scheme) outperforms the routing with no fragmentation (RA_fix scheme) in terms of energy, throughput, and network load. Although we conducted our simulations using medium scale networks, the performance gains of our schemes will be magnified as the average path length becomes larger as in the case of using large-scale networks (hundreds or thousands of nodes).

Chapter 4

Analyzing and Enhancing the IEEE 802.11 DCF in Noisy Environments

As shown previously in the IEEE 802.11 DCF mechanism, the binary exponential backoff (BEB) mechanism is used for resolving packet collisions that occur as the uncoordinated nodes contend for the channel. To ensure packet transmission reliability, MAC acknowledgment (ACK) frames are used to indicate the correct reception of the data packets. A collision corruption for the transmitted packet is assumed in case of not receiving the CTS frame or not receiving the ACK frame. IEEE 802.11 doubles the CW in order to reduce the probability of collision. We refer to this mechanism as $naive_{BEB}$. Applying $naive_{BEB}$ mechanism in environments that suffers from errors due to the noise in the wireless channels, results in a poor throughput performance because it *always* assumes that the packet corruptions are due to collisions only.

In the rest of the chapter, we analytically study the performance of the IEEE 802.11 MAC for infrastructure networks using $naive_{BEB}$ mechanism in noisy environments. The model is verified using the *ns-2* simulator. We show how $naive_{BEB}$ affects the network performance due to its inability of differentiating between the causes of unsuccessful packet transmissions. An enhancement to the IEEE 802.11 MAC named as $smart_{BEB}$, that capable to differentiate between different types of corruptions that cause unsuccessful transmissions; collision corruptions and noise corruptions, is proposed. The performance of the proposed mechanism is studied analytically and then verified using *ns-2*. We show that $smart_{BEB}$ enhances the network performance up to order of magnitudes with respect to the network error rates (noise level). We also studied the noise effect on the fairness of IEEE 802.11 and show that $smart_{BEB}$ mechanism maintains the channel fairness between the competing nodes.

4.1 Related Work

One of the issues in the analysis of the IEEE 802.11 protocol is to devise an analytical model which can predict the collision probability and its effect on the performance metrics. Paper [24] analyzes the throughput and fairness issues of the DCF function and paper [19] gives the theoretical throughput limit of IEEE 802.11 based on a p-persistent variant. However, none of these captures the effect of the Contention Window(CW) and binary slotted exponential backoff procedure used by DCF in IEEE 802.11. Paper [16] uses Markov process to analyze the saturation throughput of IEEE 802.11 and show that the Markov analysis works well. The model is extended in [130] to consider the frame retransmission limits. While these studies use the stochastic analysis, TC model [120] uses the mathematical approximations with average values.

The models mentioned so far assume ideal channel conditions, where packet error does not occur. Qiao and Choi [106, 107] assume additive white Gaussian noise channel

(AWGN) and calculate packet error probability, then derive the goodput performance of PHY/MAC protocol analytically. However they assume that there are only two nodes (one sender and one receiver) therefore no collisions occur. In our model we consider both packet errors and the collisions among nodes. To our knowledge, neither of the previous works addressed the effect of environment noises of the network performance, nor the fairness between nodes suffering from different noise values.

4.2 Markov Chain Model of the IEEE 802.11 DCF in Noisy Environment

Our model is based on the one proposed by [16] and we use the same assumption for our analysis. The contending nodes are supposed to be a fixed number, n organized in a similar manner to the infrastructure mode. Let $b(t)$ be the stochastic process representing the backoff window size for a given node at slot time t[1]. Let m, maximum backoff stage, be the value such that $aCW_{max} = 2^m W_0$ where $W_0 = aCW_{min}$, and let us adopt the notation $W_i = 2^i W_0$, where $i \in (0, m)$ is called backoff stage. Let $s(t)$ be the stochastic process representing the backoff stage $(0, \ldots, m)$ of the node at time t. Similar to paper [16], the key approximation in this model is that the probability p_c that a transmitted packet collides is independent of the state s(t) of the node.

Unlike paper [16] which used p_c to calculate the transition probabilities, we use p_d

[1]The slot time refers to the time interval between two consecutive backoff time counter decrements. This value is fixed (δ) in case of idle medium, or variable that includes a packet transmission when medium is busy.

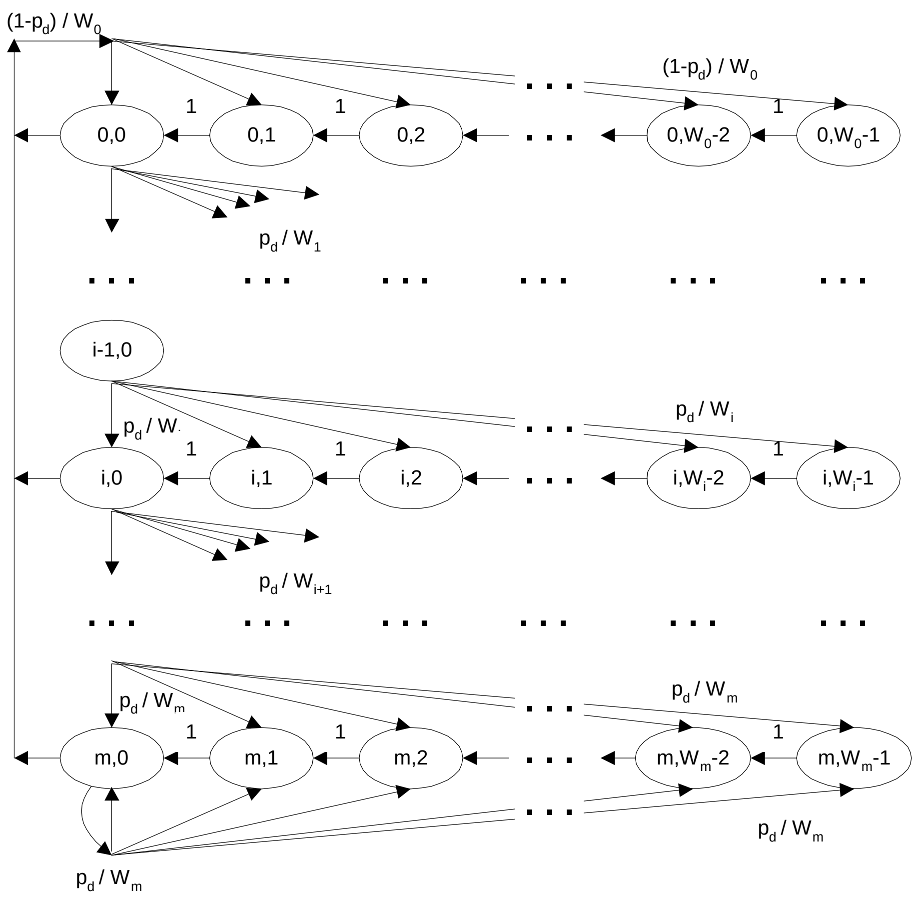

Figure 4.1: Markov Chain model for the backoff window in noisy environments

which captures the effect of the packet error rate, p_e, in the model in addition to the p_c. In the basic access mode, the transition probability because of packet corruption is:

$$p_d = p_c + (1 - p_c)\big(p_e + p_c^{ack} + (1 - p_c^{ack})p_e^{ack}\big) \tag{4.1}$$

and in case of using RTS/CTS access mode:

$$\begin{aligned} p_d \;&=\; p_c + (1 - p_c)\Big(p_e^{rts} + p_c^{cts} + (1 - p_c^{cts})\Big(p_e^{cts} + p_c^{data} \\ &\quad +(1 - p_c^{data})\big(p_e + p_c^{ack} + (1 - p_c^{ack})p_e^{ack}\big)\Big)\Big) \end{aligned} \tag{4.2}$$

where p_e^{rts}, p_e^{cts}, p_e^{ack} are the frame error probabilities (rates) of RTS, CTS, ACK respectively, while p_c^{cts}, p_c^{data}, p_c^{ack} are the colliding probabilities of CTS frame, data packet, ACK frame respectively. We can simplify these equations by neglecting the frames error probabilities because RTS, CTS, and ACK are short frames. Also, the colliding probabilities in the infrastructure mode are negligible after transmitting the first frame successfully using basic or RTS/CTS access modes. Therefore, Equations 4.1 and 4.2 are approximated by:

$$p_d = p_c + p_e - p_c p_e \tag{4.3}$$

We model the bi-dimensional process s(t), b(t) as discrete-time Markov chain and show it in Figure 4.1 using p_d. The probability τ that a node transmits in a randomly chosen slot time is:

$$\begin{aligned} \tau \;&=\; \textstyle\sum_{i=0}^{m} b_{i,0} \\ &=\; \frac{2(1 - 2p_d)}{(1 - 2p_d)(W_0 + 1) + p_d W_0 (1 - (2p_d)^m)} \end{aligned} \tag{4.4}$$

where $b_{i,k}$ is the nodeary probability for state s(t)=i, b(t)=k, $i \in (0, m)$ and $k \in (0, W_i - 1)$.

In steady state, p_d is expressed as:

$$p_d = 1 - (1 - p_e)(1 - \tau)^{n-1} \tag{4.5}$$

Equations 4.4 and 4.5 represent a nonlinear system in two unknowns τ and p_d (p_c) which can be solved using numerical techniques.

A time slot will be either idle (id) where no node is transmitting, has transmission of only one node (tr) with probability of p_e of corrupting the packet, or has a collision (cl) because two or more nodes are transmitting in the same time. The probabilities of these states are:

$$\begin{aligned} P_{id} &= (1 - \tau)^n \\ P_{tr} &= n\tau(1 - \tau)^{n-1} \\ P_{cl} &= 1 - (1 - \tau)^{n-1}(1 - \tau + n\tau) \end{aligned}$$

We define the saturation goodput of the network as:

$$\begin{aligned} G &= \frac{\text{E[successfully transmitted payload bytes in a slot time]}}{\text{E[length of a slot time]}} \\ &= \frac{(1 - p_e)P_{tr}E[S]}{P_{id}\delta + (1 - p_e)P_{tr}T_s + p_e P_{tr} T_f + P_{cl}T_c} \end{aligned} \tag{4.6}$$

where $E[S]$ is the average packet length and δ is the duration of an empty (idle) slot time. The T_s, T_f, and T_c are the average time the channel is sensed busy because of a successful transmission, failure (corrupted) transmission, or a collision respectively. In the case of using basic access mode we have:

$$\begin{aligned} T_s &= PHY_{hdr} + MAC_{hdr} + S + SIFS + ACK + DIFS \\ T_f &= PHY_{hdr} + MAC_{hdr} + S + DIFS \\ T_c &= PHY_{hdr} + MAC_{hdr} + S + DIFS \end{aligned}$$

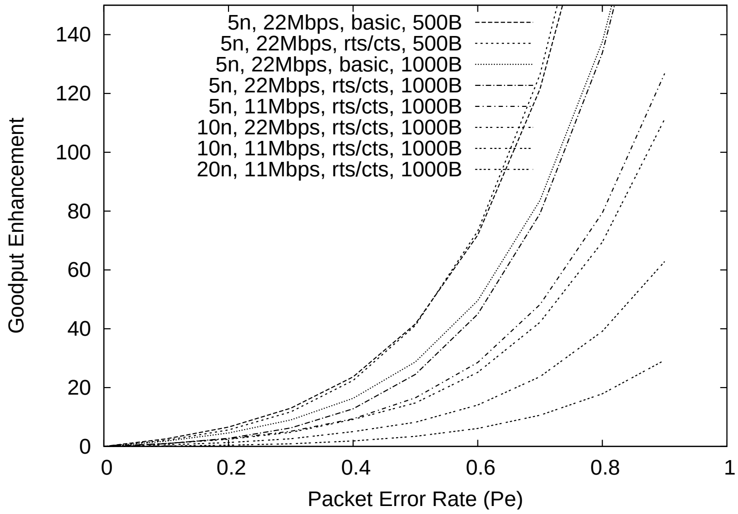

Figure 4.2: Analytical goodput enhancement of $smart_{BEB}$ mechanism.

and in the RTS/CTS access mode we have:

$$\begin{aligned}
T_s &= RTS + SIFS + CTS + SIFS + PHY_{hdr} + MAC_{hdr} \\
&\quad + S + SIFS + ACK + DIFS \\
T_f &= RTS + SIFS + CTS + SIFS + PHY_{hdr} + MAC_{hdr} \\
&\quad + S + DIFS \\
T_c &= RTS + DIFS
\end{aligned}$$

where MAC_{hdr}, PHY_{hdr}, and S are the MAC layer overhead, the PHY layer overhead, and data payload respectively. Note that all terms are expressed in time units (seconds).

4.3 Model Validation

We validate our model by comparing the analytical results with the results from *ns-2* simulator. Each node has enough data to transmit at any time during the simulation time to

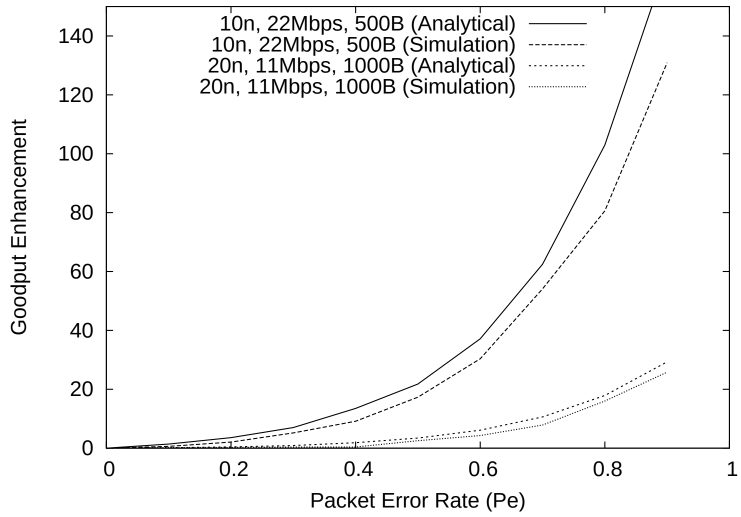

Figure 4.3: Goodput enhancement for $smart_{BEB}$ implementation in RTS/CTS mode.

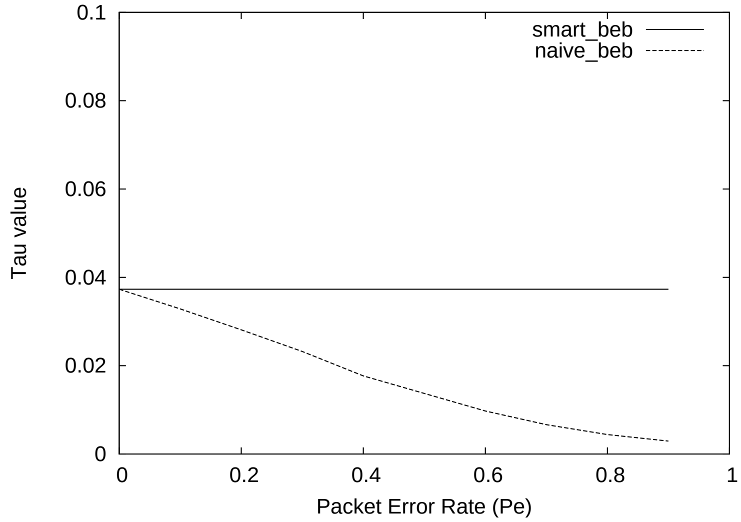

Figure 4.4: The τ values in noisy environments.

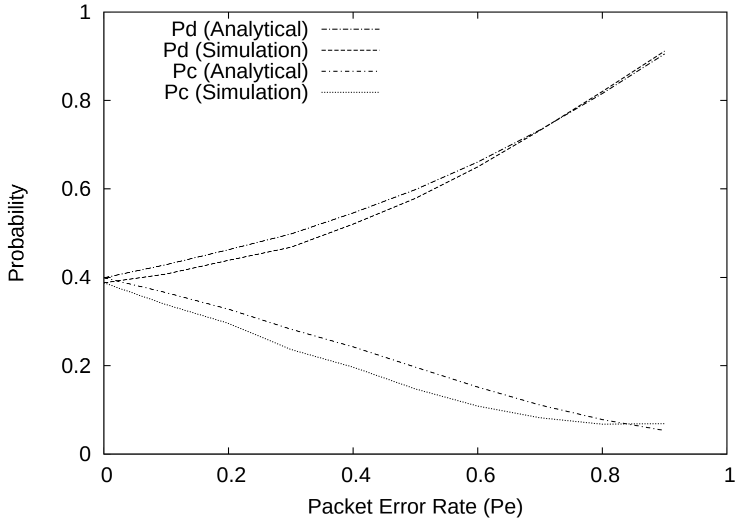

Figure 4.5: The p_c and p_d values in noisy environments.

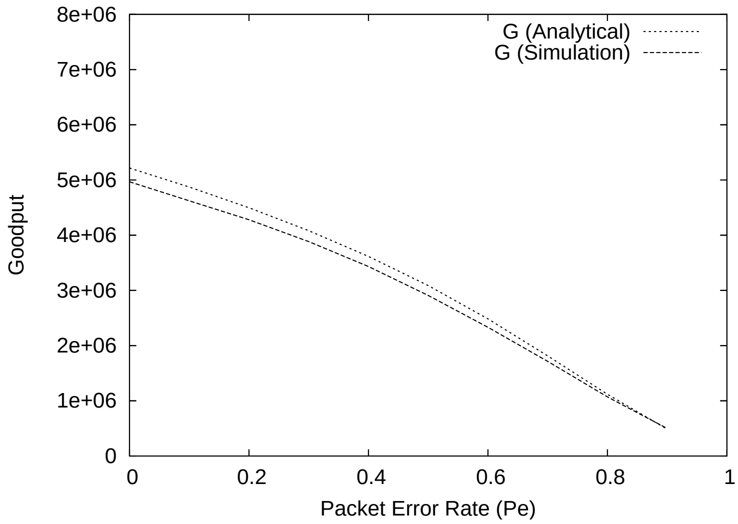

Figure 4.6: Saturation goodput in noisy environments.

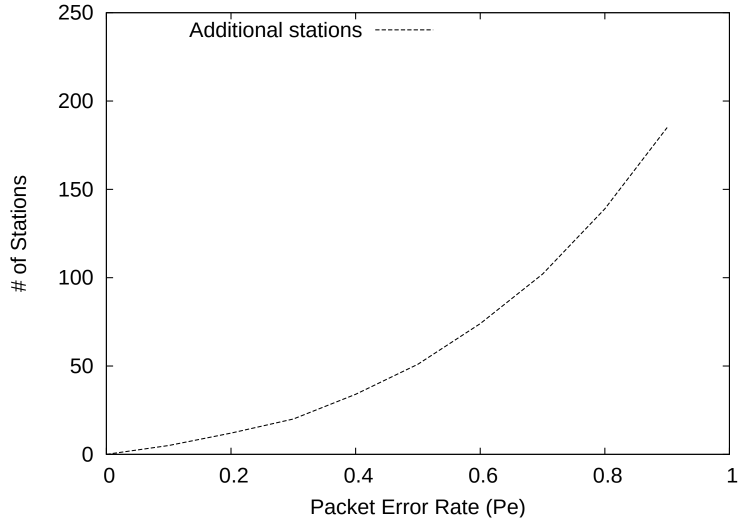

Figure 4.7: The additional nodes to original 20 nodes.

obtain the saturation goodput performance. We vary the channel noise to see the effect of system under different packet error rates p_e. To simplify the analytical model, we assume all nodes experience the same p_e. All the parameters used in analytical model and our simulations follow the parameters of DSSS [4], and are summarized in Table 4.1. Note that PHY header, RTS frame, and CTS frame are sent at the basic access rate. Different scenarios using different number of nodes, channel bit rates, payload sizes, and using both basic and RTS/CTS access modes were conducted to validate the model. Here, we show the results for the configuration of 20 nodes (nodes) in addition to the access point node to model the infrastructure mode using RTS/CTS access mode, 11 Mbps as the channel rate, and data payload is 1000 bytes in addition to IP header and UDP header of 20 and 8 bytes respectively.

Figure 4.5 plots the p_c and p_d values. The p_c is calculated as the number of missing CTS frames over the total number of transmitted RTS frames, and p_d as the summation of

Parameter	*Value*	*Comments*
PHY header	24 octets	PHY layer overhead
MAC header	28 octets	MAC layer overhead
ACK	38 octets	ACK frame length + PHY header
RTS	44 octets	RTS frame length + PHY header
CTS	38 octets	CTS frame length + PHY header
Slot time	20 μs	idle slot time (δ)
SIFS	10 μs	SIFS time
DIFS	50 μs	SIFS + 2 * $delta$
aCWmin	31	minimum contention window
m	5	backoff levels

Table 4.1: MAC and PHY system parameter.

the number of missing CTS and the number of missing ACK frames over the total number of transmitted RTS frames. The saturation goodput of the network using the basic access mode is showed in Figure 4.6. Comparing our approximated Markov model with the simulation results for runs of different configuration scenarios, we observe that analysis results match the simulation results closely which validates our model in Section 4.2.

From Figure 4.5 we observe an interesting behavior in which p_d increases with p_e while p_c decreases with the increase in p_e. This indicates that the increase in p_e has the same effect as that reducing the number of nodes. Specifically, with increasing p_e we can increase the number of active nodes to utilize the additional number of idle slots introduced by $naive_{BEB}$ mechanism while maintaining the original conditional collision probability (p_c) when $p_e = 0$. Consequently, values of the original P_{id} and P_{tr} are maintained that utilizes the network saturation goodput. The additional number of nodes could be calculated as follow:

$$n_{additional} = 1 + \frac{\ln(1 - p_d) - \ln(1 - p_e)}{\ln(1 - \tau)} - n_0 \tag{4.7}$$

where n_0 is the original number of nodes, τ is calculated using Equation 4.4, and p_d

is calculated using Equation 4.3. Note that p_c value is fixed with different values of p_e and is calculated by solving Equations 4.4 and 4.5 for the case when $n = n_0$ and $p_e = 0$. Figure 4.7 plots the number of additional nodes added to the original 20 nodes to maintain the same p_c value and consequently P_{id} and P_{tr}.

4.4 $smart_{BEB}$: Enhanced IEEE 802.11 MAC

The problem of the current IEEE 802.11 standard mechanism is that it does not differentiate between the corruption causes of packets. It assumes the *only* cause for dropping packets is collision.

In this section, we propose the $smart_{BEB}$ which is a mechanism to enhance the IEEE 802.11 with a capability to differentiate between different causes for packet corruptions. In case a packet is dropped because of collision corruption, the IEEE 802.11 standard BEB mechanism is followed and the contention window (CW) is doubled. If the cause of dropping a packet is noise (error) corruption, $smart_{BEB}$ handles the transmission as successful one and resets the CW to W_0. In addition, $smart_{BEB}$ handles the retransmission of the dropped packet as a new packet transmission.

To model $smart_{BEB}$, we need to replace p_d of Markov model in Section 4.2 by $\acute{p}_d = \acute{p}_c$ where $\acute{p}_c$ is the conditional collision probability. The probability $\acute{\tau}$ in the new model is estimated by solving Equations 4.4 and 4.5, substituting p_d with $\acute{p}_d$ and τ with $\acute{\tau}$. The $\acute{P}_{id}$, $\acute{P}_{tr}$, and $\acute{P}_{cl}$ are calculated similar to the Equations 4.6. The goodput, $\acute{G}$ for this model is calculated using similar equation to Equation 4.6. We define the percentage

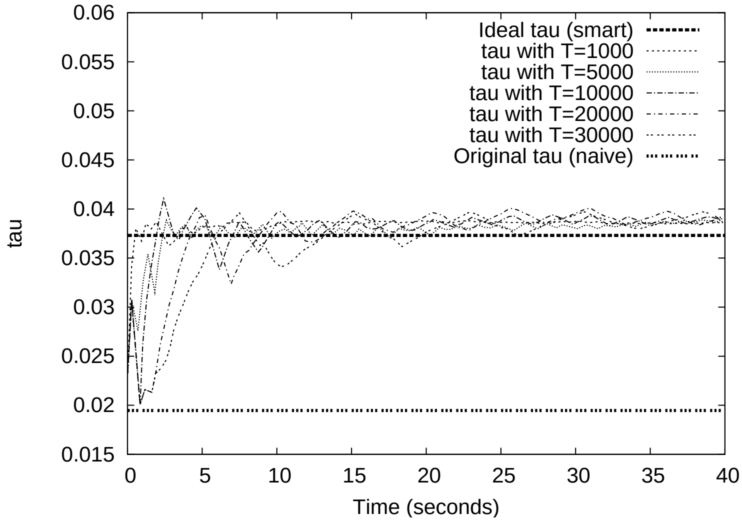

Figure 4.8: Measured τ_{actual} for different T time slots when $p_e = 0.4$.

of the goodput enhancement of $smart_{BEB}$ over $naive_{BEB}$ as:

$$\nabla G = \frac{\acute{G} - G}{G} \times 100 \tag{4.8}$$

Figure 4.2 shows analytical results of the ∇G for different configuration of data rates, number of nodes, and access modes in noisy environments. Using $smart_{BEB}$ mechanism enhances the system goodput significantly because it limits the contention window size that reduces the number of unnecessary idle time slots.

4.5 Implementation of $smart_{BEB}$ Mechanism

4.5.1 RTS/CTS Access Mode

In RTS/CTS mode, a node starts its transmission sequence by transmitting RTS frame. When it receives the CTS frame, it knows that the medium is reserved for its transmission. Then it transmits the data packet and waits for an ACK frame to verify a successful

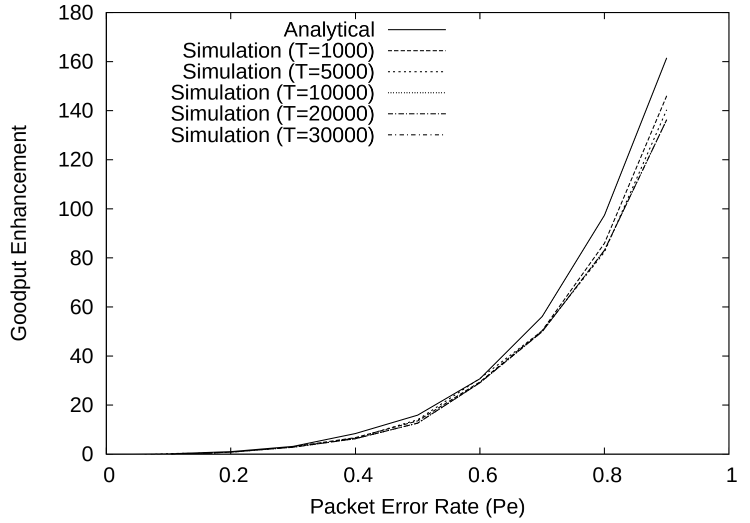

Figure 4.9: Goodput enhancement for $smart_{BEB}$ implementation in basic mode.

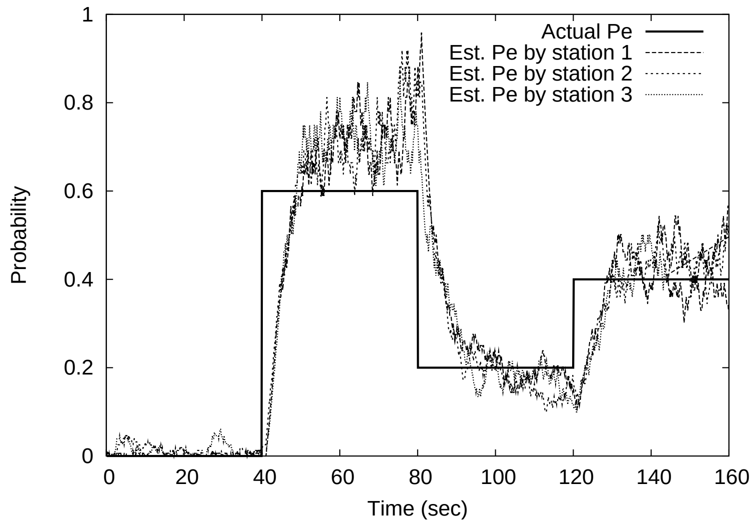

Figure 4.10: The estimated p_e for variable error rates over time.

transmission. Since RTS and CTS are short frames, the probability of corrupting those packets due to noise errors is small and the only reason for their corruptions is because of a collision. On the other hand, once a node receives CTS, the probability of a collision corruption to the data packet is negligible. Therefore, in $smart_{BEB}$ mechanism when a node does not receive a CTS, it assumes a collision and follows the IEEE 802.11 backoff mechanism in doubling the CW size. On the other hand, when a node does not receive a ACK, it assumes the loss of the data packet due to a noise corruption and reset CW to W_0. Figure 4.3 shows the goodput enhancement for different configuration using the $smart_{BEB}$ mechanism. The simulation parameters are as in Table 4.1. From Figure 4.3, the simulation results match the analytical results which verifies the correctness of this implementation mechanism.

4.5.2 Basic Access Mode

In basic mode, there are no hints similar to the RTS/CTS mode to help in guessing the cause of packet corruption. Therefore, a hypothesis is needed to help identify the cause of the packet corruption in the basic access mode. The key idea of the hypothesis is that when a node doesn't receive the ACK frame, it assumes the packet is dropped because of noise corruption with probability p, or because of collision corruption with probability $(1 - p)$. Estimation of p is based on the observation from Markov model, with the knowledge of the number of active nodes, that the τ value for each client is decreased with the increasing of p_e in $naive_{BEB}$ mechanism, while it is constant with different values of p_e in $smart_{BEB}$ mechanism. Figure 4.4 shows the τ values for scenario of 10 active nodes.

We propose two methods to estimate the number of active nodes: passive and active methods. In passive method, each node keeps sensing the channel and monitoring the activities on the wireless medium when it is not transmitting to count the number of different active nodes. In active mode, the access point of the infrastructure network co-operates by estimating the number of active nodes associated with it and broadcasting this information within the beacon frames or in a separate control messages. We summarize our mechanism mode as follows:

- Each node, initially, set its p to zero assuming all the packet losses are due to collision corruptions.
- With the knowledge of the number of active nodes, each node calculates the constant goal τ (τ_{ideal}) when p_e is zero using the Markov model in Section 4.2.
- Each node, during its life time, measures its actual τ value (τ_{actual}) each T time slots.
- If τ_{actual} is larger than τ_{ideal}, then the node is transmitting too frequently and needs to slow down by increasing its idle slots. Therefore, p is decreased by δ to increase the probability of collisions and subsequently increasing the CW more frequently.
- If τ_{actual} is lower than τ_{ideal}, then the node seldom tries to transmit and needs to increase the trials by reducing the number of idle slots. Hence, the node increases p by δ to assign more of the dropping packets to noise corruptions that results in decreasing (resetting) CW more frequently.
- The δ values are assigned with respect to the value of T. For example, for $T = 1000$, we let δ be 0.01, while in case of $T = 10000$, δ is equal to 0.05.

- When an ACK frame is missing, the node resets its CW to W_0 with probability p, and increase CW to $max(2 * CW, aCWmax)$ with probability $(1 - p)$.

To validate our implementation, we ran ns-2 for different scenario configuration. In this section, we show the results for scenario of 10 active nodes in addition to the access point transmitting data packets of size 500 bytes at data rate 22Mbps. We used the active method to estimate the number of active nodes. Figure 4.8 plots the average τ_{actual} for a single node over the simulation duration for different T time slots when $p_e = 0.4$, and the goodput enhancement is plotted in Figure 4.9. From the figures, the effect of T is not significant. Therefore, choosing small value for T would allow $smart_{BEB}$ to adapt to the environment noise level faster.

Since p is the percentage of the dropped packet assigned to the noise corruptions only, p is expressed as:

$$p = \frac{(1 - p_c)p_e}{p_c + p_e - p_c p_e} \tag{4.9}$$

Using this equation, a node could estimate the packet error rate p_e it experiences. Figure 4.10 plots the estimated p_e by the first three nodes for our scenario. In this simulation, p is incremented or decremented by $\delta = 0.01$ each 1000 time slots. As in the figure, the p_e estimations follow the actual p_e value as it changes over time.

4.6 IEEE 802.11 fairness in Noisy environments

In this section we briefly study the IEEE 802.11 fairness when different nodes experience different error rates in the noisy environments. We extended the Markov model in Section 4.2 to represent different classes of nodes. Although we describe the extension for

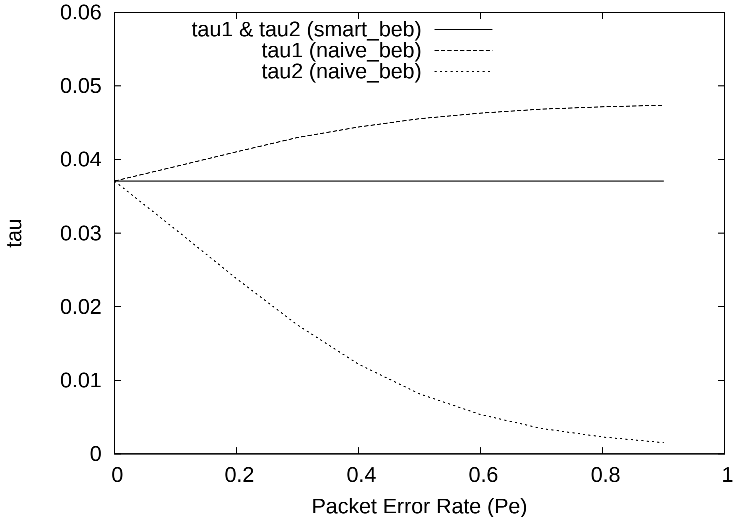

Figure 4.11: The τ values of the two classes.

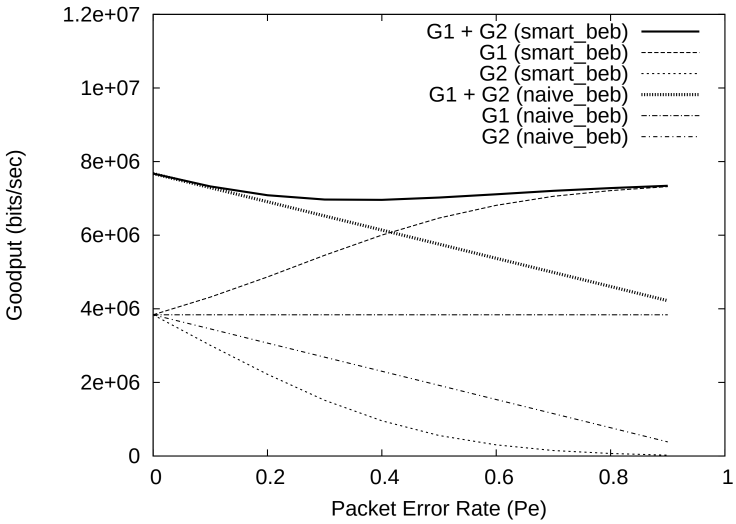

Figure 4.12: Goodput of the two classes.

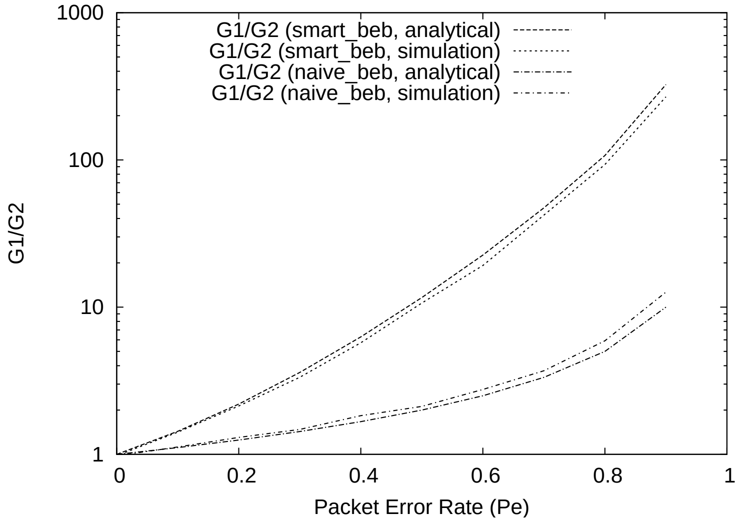

Figure 4.13: G1/G2 ratio of the two classes.

two classes only, the extension for more than two classes is straight forward.

Each node in the first class of n_1 nodes experiences packet drop rate p_{d1} which consists of error rate p_{e1} and the collision rate of p_{c1}. On the other hand, each node in the other class of n_2 nodes experiences drop rate p_{d2} that is a function of p_{e2} and p_{c2}. Similar to Equations 4.4 and 4.5, we get:

$$\tau_1 = \frac{2(1-2p_{d1})}{(1-2p_{d1})(W_0+1)+p_{d1}W_0(1-(2p_{d1})^m)}$$

$$\tau_2 = \frac{2(1-2p_{d2})}{(1-2p_{d2})(W_0+1)+p_{d2}W_0(1-(2p_{d2})^m)}$$

$$\begin{aligned} p_{d1} &= 1-(1-p_{e1})(1-\tau_1)^{n_1-1}(1-\tau_2)^{n_2} \\ p_{d2} &= 1-(1-p_{e2})(1-\tau_2)^{n_2-1}(1-\tau_1)^{n_1} \end{aligned} \tag{4.10}$$

where τ_1 and τ_2 are the probabilities of transmitting in a randomly chosen slot time for nodes in the first class and the second class respectively.

Similar, Equations in 4.6 are extended to:

$$
\begin{aligned}
P_{id} &= (1-\tau_1)^{n_1}(1-\tau_2)^{n_2} \\
P_{tr1} &= n_1\tau_1(1-\tau_2)^{n_1-1}(1-\tau_2)^{n2} \\
P_{tr2} &= n_2\tau_2(1-\tau_2)^{n_2-1}(1-\tau_1)^{n1} \\
P_{cl} &= 1-P_{id}-P_{tr_1}-P_{tr_2}
\end{aligned} \tag{4.11}
$$

where P_{tr1} is the probability that the time slot has a single transmission of a node belongs to first class, and P_{tr2} is the probability that the time slot has a single transmission form the second class. The goodput G_1 and G_2 of the first class and the second class are expressed as:

$$G_1 = \frac{(1-p_{e1})P_{tr1}S}{\varrho} \quad \text{and} \quad G_2 = \frac{(1-p_{e2})P_{tr2}S}{\varrho}$$

where $\varrho = P_{id}\delta + (1-p_{e1})P_{tr1}T_s + p_{e1}P_{tr1}T_f + (1-p_{e2})P_{tr2}T_s + p_{e2}P_{tr2}T_f + P_{fl}T_c$ and S, δ, T_s, T_f, T_c are the same as defined in Section 4.2.

As an example, we consider the configuration of a network consists of 10 active nodes, in addition to the access point, where $n_1 = 5$ nodes form the first class that do not experience any error rate ($p_e = 0$), and the rest of the nodes $n_2 = 5$ form the second class that experience same error rates where $0 \leq p_{e2} \leq 0.9$. Figure 4.11 shows the corresponding τ values. In case of using $naive_{BEB}$, the network is in favor of the nodes belonging to the first class and assign them more probability to access the network. While $smart_{BEB}$ guarantees that both classes will have equal probability (fair share) to access the network.

Figure 4.12 plots the analytical total goodput in addition to the goodputs of the individual classes assuming 11Mbps data rate and packet size of 1000 bytes and using RTS/CTS access mode. Total $naive_{BEB}$ total goodput is higher than the $smart_{BEB}$ total goodput because $naive_{BEB}$ favors the nodes with lower error rates which results in more *successful* transmissions. On the other hand, $smart_{BEB}$ maintains the fairness between nodes that decreases the number of successful transmission. Figure 4.13 shows the G_1/G_2 ratio. With $naive_{BEB}$, the goodput of the first class reaches hundreds times the goodput of the second class of nodes. Using $smart_{BEB}$, the goodput ratio is corresponding to the error rates.

4.6.1 Conclusion

We analyzed the network performance in noisy environments. We showed, analytically and by simulation, how the standard BEB of IEEE 802.11 degrades the network performance significantly in these environments. We proposed an enhanced BEB, $smart_{BEB}$, that enhances the network performance by order of magnitudes in noisy environments. $smart_{BEB}$, in contrast to the standard BEB mechanism, is capable to differentiate between different types of corruptions that cause unsuccessful transmissions; collision corruptions and noise corruptions. We showed how to implement the $smart_{BEB}$ in basic access mode and in the RTS/CTS access mode with minimal modification requirement to the IEEE 802.11 standard. Further, we studied the effect of the noises on the network fairness and showed how $smart_{BEB}$ guarantees the fairness by forfeiting the network goodput.

Chapter 5

LED: Location Enhancement for the IEEE 802.11 Distributed Coordination Function

Contention based MAC protocols are the mainstream for distributed and self-organized wireless networks since in these networks, the infrastructure is usually not present and there is no clear separation between the roles of access points and client nodes. The support of contention based DCF has also made IEEE 802.11 equipments popular choices for various wireless ad hoc networks.

Like many other contention based MAC protocols, the IEEE 802.11 DCF is based on Carrier Sense Multiple Access (CSMA) mechanism. In CSMA, a node may transmit if and only if the medium is sensed to be idle, hence prevented from interfering with any ongoing transmissions. If a node has data to transmit but a busy carrier is detected, its data transmission is postponed (blocked) till a later time.

The IEEE 802.11 DCF has been discovered not to be efficient in shared channel use due to its overcautious approach towards assessing the possibility of interference. In particular, a node simply blocks its own transmission when it senses the medium busy or it has received a channel reservation frame sent by any other node. However, in many cases this channel assessing node's own transmission would not actually disturb the ongoing transmission because the transmission would not introduce enough signal energy at the ongoing transmission's receiver to actually corrupt the reception.

Finer channel assessment schemes which do consider the above possibility are difficult to implement with information provided by the current IEEE 802.11 communication protocol. If more parameters regarding an ongoing transmission, such as the locations of the transmitter and receiver and transmission power level, can be provided to surrounding nodes, it is then possible for the surrounding nodes to make better estimations on if indeed their own transmissions may corrupt the reception of the ongoing transmission. Hence, more concurrent transmissions on a WLAN channel can be conducted and the communication channel can be used more efficiently.

In this chapter, we propose a novel contention-based distributed MAC scheme which assesses the channel condition more aggressively by exploiting radio signal capture phenomena [7, 79, 83, 70, 45] to increase simultaneity of data transmissions and enhance overall wireless network throughput. This scheme is designed as an enhancement to the DCF. In doing so, we develop a new MAC frame format in addition to the new MAC protocol to provide the additional information to help the nodes in deciding whether to block their transmissions or not, when there are ongoing communications occurring in their vicinities.

5.1 Related Works

Historically, the design of the IEEE 802.11 DCF was influenced by several other protocols. MACAW protocol [15], extending its predecessor Multiple Access Collision Avoidance (MACA) protocol [64], is based on the use of the Request-To-Send and Clear-To-Send (RTS/CTS) handshaking scheme. If a node has a packet to send, it firstly transmits a RTS packet to request the channel and the receiver replies with a CTS packet. After the sender receives the CTS packet successfully, it proceeds to transmit the actual data packet. Nodes that overhear the RTS packet will defer transmission for a sufficiently long period to allow the transmitter to receive the CTS packet. Nodes overhearing the CTS packet will back off for a period that is sufficiently long to allow the receiver to receive the entire data packet and acknowledge it. Sender nodes using RTS/CTS do not use the carrier sense mechanism to assess the channel availability. An extended protocol named Floor Acquisition Multiple Access (FAMA) is proposed in [42]. FAMA bears significant resemblance to IEEE 802.11, employing both local carrier sensing, as well as the RTS/CTS collision avoidance exchange for data transmission.

The IEEE 802.11 DCF uses a combination of physical/virtual carrier sensing and RTS/CTS channel reservation for channel protection. While these mechanisms are generally effective in reducing frame collisions, the protocol is rather pessimistic and not very efficient in channel use because it does not encourage enough concurrent transmissions. Our observation concurs with the views of other researchers, who have also proposed modifications to DCF for the purpose of increasing the number of concurrent transmissions in the network.

Authors in [135] suggest that by changing the timing of the steps within the RTS-CTS-DATA-ACK frame sequence and synchronizing the states among one hop neighbors, if the receivers of two frames transmitted by two neighbors are far apart enough, these two transmissions can be scheduled concurrently. [6] observes that in an "overactive RTS/CTS" situation, in which the RTS/CTS exchange affects more surrounding nodes than needed, just hearing RTS or CTS but not both does not justify for assessing the channel as busy. Thus a bystander to a pair of data transmitter and receiver should only block its own transmission if it receives both RTS and CTS.

The Interference Aware (IA) method proposed by [20] and [29] shares the same philosophy as our proposal in the way that nodes report channel condition by piggybacking channel condition information in the frame exchange sequence. In IA, the receiver of a RTS frame embeds the Signal to Interference Ratio (SIR) observed while receiving the RTS in its returning CTS frame. This way other nodes, also taking into account the SIR observed by themselves while receiving the same CTS frame, are able to calculate if their own transmissions may cause enough interference to the RTS receiver in question. This mechanism works only with RTS/CTS scheme and it requires nodes to listen to both RTS and CTS frames.

We have noticed some rather common problems among these approaches. The first is that these proposals rely on the RTS/CTS handshake. In reality the RTS/CTS handshake is turned off in most deployments, which makes these proposals inapplicable in such environments. The next issue is that these proposals do not take the aforementioned "capture frame" v.s. "capture signal" problem into consideration. As a result, many concurrent transmissions will not be received by their intended receivers, not because the signals are not strong enough, but because the received bits are cast into the wrong frame and become incomprehensible.

Recent works [133, 139, 124] proposed the control of spatial reuse in the network by varying the carrier sense threshold. Authors in [139] adjust the carrier sense threshold to the optimal value that maximizes the spatial reuse given a minimum required signal-to-noise ratio or a regular topology. Work in [133] extends that work by exploring the interactions between MAC and PHY layers and identifying the impact of MAC overhead on the choice of optimal carrier sense range as well as the associated impact on the aggregate throughput. ECHOS architecture is introduced in [124] to exploit the spatial heterogeneity of users and flows in order to improve the IEEE 802.11 capacity in hotspots. Authors devise *Access Point Carrier Sense Threshold* algorithm that allows access points to set their carrier sense threshold and those of its clients appropriately such that more flows can co-exist in the same channel without interference where possible. This solution addresses situations in a hotspot where neighboring cells are assigned the same channels due to the limited number of orthogonal channels available in 802.11b/g. Adjusting the carrier sense threshold in infrastructure networks is possible because of the existence of the central node (access point) where all connections are one hop and go through it. A considerable overhead is needed to apply this mechanism in a distributed manner for ad hoc networks. In addition to the complication of this mechanism, none of these works considered the effect of capture phenomena that exists in IEEE 802.11 networks that been confirmed by several published studies as shown in Chapter 2.

Our own modification to the IEEE 802.11 DCF protocol is partly inspired and motivated by the above listed works. We name our modification the Location Enhanced

DCF (LED).

5.2 Performance of Capture Effect in 802.11 Networks

Before going into the details of LED, in this section we provide an explanation for why the 802.11 DCF carrier sense based blocking assessment algorithm is overly conservative. Then we analyze the probability that a node's can transmit with the presence of a nearby transmission without corrupting this transmission, if frame capture is supported by all the receivers. This probability quantifies how much potential throughput gain there is to improve over the IEEE 802.11 DCF. We assume a free space omni-directional propagation channel model [105], described in Chapter 2.

An important aspect, which has not been questioned by many of the previous works that needs some discussion before we proceed further, is the capturing of a *signal* versus capturing of a *frame*. We consider the case when the new (stronger) frame arrives after the receiver begins to receive the weaker frame. A receiver being able to capture a stronger signal does not necessarily mean it can capture the stronger frame. Whether a receiver can capture a stronger frame also depends on several other factors such as: the arrival moment of the beginning of the stronger frame, the current receiving state of the receiver, the capability of the receiver to realize that it is seeing the beginning of a new (stronger) frame, and the capability of the receiver to jump to the appropriate receiving state for beginning to process the new frame. If the receiver is not able to realize that it has just seen the beginning of a new frame and reset its receiving state accordingly, the bits of the new frame may be interpreted as the bits of the weaker frame, which typically results in

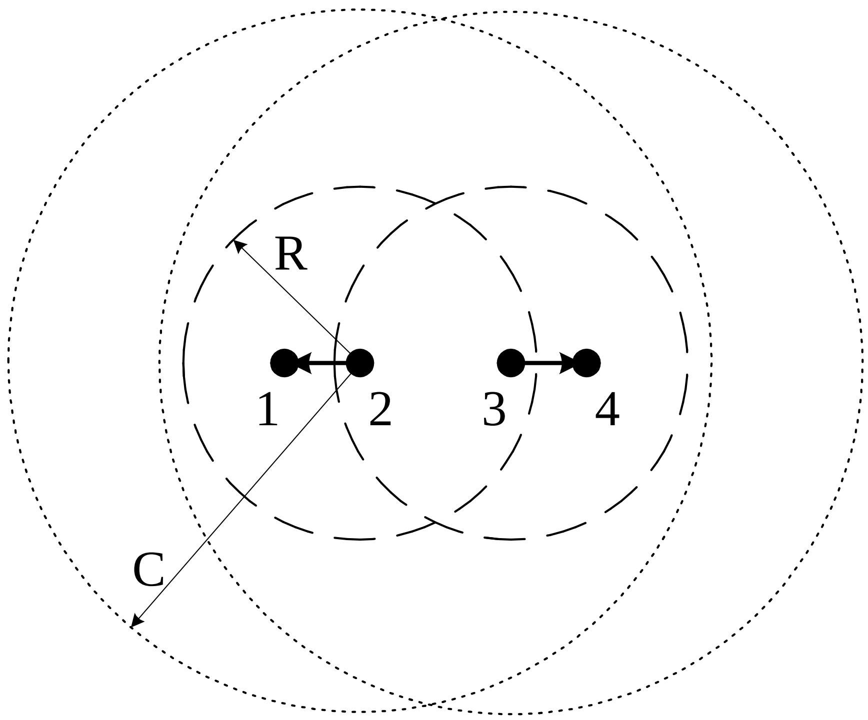

Figure 5.1: Example of network with 4 nodes, where R is transmission range and C is the carrier sense range

failure of the weaker frame's forward error checking and frame rejection.

We are interested in capture effect because we believe that it can be used to our advantage to improve channel sharing efficiency. Consider the following example as shown in Figure 5.1. Two concurrent connections share the same wireless communication channel. The first connection is from node 2 (source) to node 1 (destination) and the second is from node 3 to node 4. In the current IEEE 802.11 DCF, whichever connection acquires the channel first gets to complete its data frame delivery message exchange because nodes of the other connection would have detected the carrier signals of this connection, or received reservation messages (RTS/CTS) of this connection, and remain blocked.

However, if nodes are positioned in such a way that the transmission power levels of

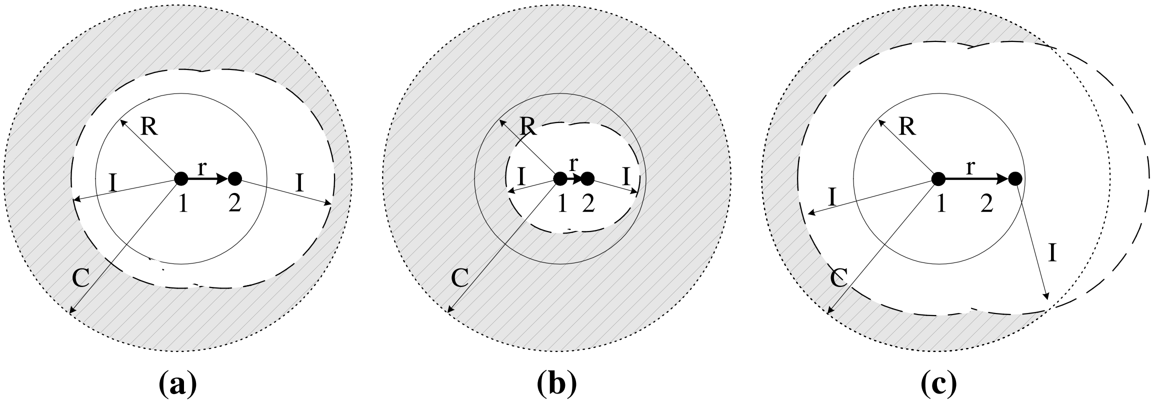

Figure 5.2: Blocking effectiveness of carrier sense range for different scenarios. The ineffectiveness is measured by the percentage of the shaded area to the carrier sense area (πC^2).

nodes 3 and 4, as measured at nodes 1 and 2, are not strong enough to prevent nodes 1 and 2 from capturing each other's transmissions; nodes of the second connection should be permitted to communicate, even after nodes of the first connection have begun their frame transmissions. Similarly nodes 1 and 2 can do the same if nodes 3 and 4 have acquired the channel first. One thing to note is that of course to do this the design of the node receivers must support the capture of stronger *frame*, as will be shown later, regardless when it arrives.

5.2.1 Inefficiency of Carrier Sense Mechanism

In this subsection, we start our analyze on why the IEEE 802.11 DCF's carrier sense blocking assessment approach is overly pessimistic.

Let direct our attention towards the example shown in Figure 5.2. In this example, node 1 is transmitting to node 2. The three sub-figures illustrate three scenarios of different transmitter-to-receiver distances. Under DCF, all nodes within radius C of node

1 will sense the carrier as busy and block their own transmissions, if any. C is called the carrier sense range and the area within radius C of node 1 is called the carrier sense zone.

Assuming r is the distance between nodes 1 and 2. From Equation 2.1 and Equation 2.2, it is easy to derive that node 2 captures the transmitted frames from node 1 correctly as long as there is no other node transmitting within the range $r\sqrt{\alpha}$ of node 2. We call this "quiet range" the interference range I.

$$\mathrm{I} = r\sqrt{\alpha} \tag{5.1}$$

Similarly, node 1 captures the reverse direction transmissions from node 2, i.e. ACK, correctly as long as there is no node transmitting within range I of node 1. The region that is within radius I of either node 1 or 2, or both, is called the interference zone.

On the other hand, carrier sense range is the maximum distance away from a transmitting node that a node can still detect that the carrier is busy. Typically, carrier sense range is larger than the transmission range, which the maximum distance away from a transmitting node that a receiver node can correctly receive the transmitter frame.

We denote the carrier sense zone as area A_C and the interference zone as area A_I. Nodes inside of $(A_C - A_I)$, the area that is inside of the carrier sense zone but outside of the interference zone, are unnecessarily blocked due to the overly conservative blocking behavior of the IEEE 802.11 DCF. This area is shown as the shaded areas in Figure 5.2.

We define the inefficiency IE of the carrier sense mechanism as follow:

$$\mathrm{IE} = \frac{A_C - A_I}{A_C} \times 100\% \tag{5.2}$$

A_C is calculated as $A_C = \pi C^2$ while A_I is calculated as follow:

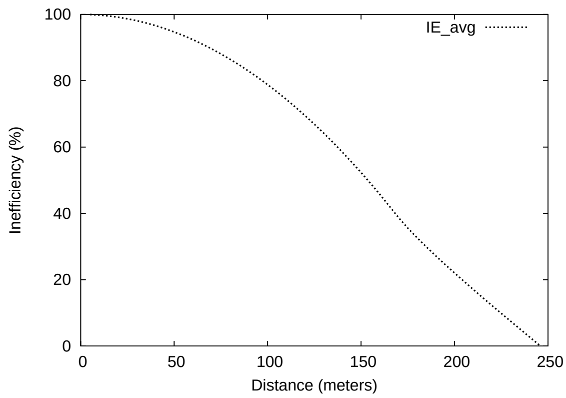

Figure 5.3: Inefficiency of carrier sense mechanism versus distance without exploiting the capture phenomena

$$A_I = \begin{cases} 2\pi I^2 - 2(I^2 \arccos(\frac{r}{2I}) - \frac{r\sqrt{4I^2-r^2}}{4}) & C \geq I + r \\ 2\pi I^2 - 2(I^2 \arccos(\frac{r}{2I}) - \frac{r\sqrt{4I^2-r^2}}{4}) - (I^2 \arccos(\frac{\aleph}{I}) - \aleph\sqrt{I^2 - \aleph^2}) & \\ \quad +(C^2 \arccos(\frac{\Im}{C}) - \Im\sqrt{C^2 - \Im^2}) & C < I + r \end{cases} \tag{5.3}$$

where $\aleph = \frac{C^2-r^2-I^2}{2r}$ and $\Im = \frac{C^2+r^2-I^2}{2r}$.

Figure 5.3 plots IE versus r when $C = 550m$ and $\alpha = 5$. Assuming the distance between the transmitter and the receiver is randomly selected from the range $[0, R]$, where R is the transmission range, the average IE is calculated as:

$$IE_{avg} = \int_0^R \frac{E}{R} dr \tag{5.4}$$

For $\alpha = 5$, $R = 250m$, and $C = 550m$, we get IE_{avg} is about 60%. This large value indicates how the carrier sense mechanism is inefficient when the capture phenomena could be exploited.

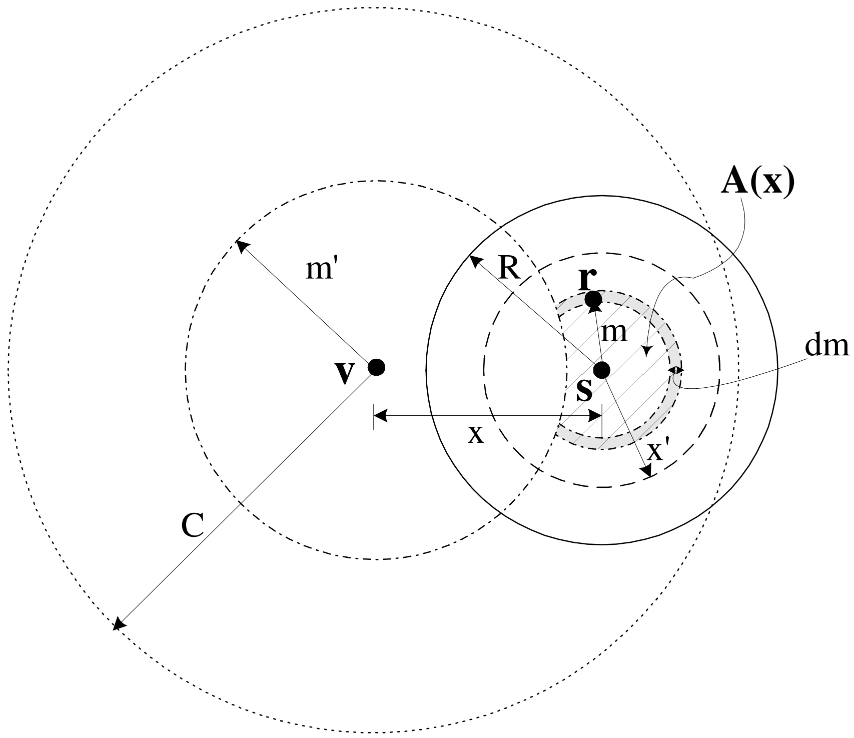

Figure 5.4: Capture analysis where $x' = \frac{x}{\sqrt{\alpha}}$ and $m' = \sqrt{\alpha}m$

5.2.2 Probability of Non-interfering Transmission

We now study the probability of non-interfering transmission despite the presence of sense signals. We assume that nodes are uniformly distributed over an area with a density of δ. Each node has a transmission range R and a carrier sense range C. For the ease of analysis, we assume that all nodes have the same traffic model and all data packets are of the same length. Each packet requires transmission time τ, and is randomly destined to one of the sender's 1-hop neighbors. One data packet is generated at a randomly selected time within every time interval T, where $T \gg \tau$. We also assume that all transmitters use the same transmission power and transmitter and receiver antenna gains are the same.

We are concerned about the scenarios where a node v may cause interference to another node r which is receiving a data frame delivery from node s as shown in

Figure 5.4. Node v transmits only if its transmission doesn't affect the reception of DATA frame at r and ACK frame at s. Using the Friis radio propagation model as in equation 2.1 and receiver capture model as in equation 2.2, to allow nodes s and r to capture correctly each other's frames in the presence of any transmission from node v, the following should hold:

$$(\overline{v.s} > \sqrt{\alpha}\,\overline{s.r}) \text{ AND } (\overline{v.r} > \sqrt{\alpha}\,\overline{s.r}) \tag{5.5}$$

where $\overline{a.b}$ is the distance between node a and node b, and α is the capture ratio. We only use the Friis propagation model for the sake of analysis simplification.

Figure 5.4 illustrates the situations for both r to capture s' transmissions (DATA) and for s to capture r's transmissions (ACK) in the presence of v's transmission. For r to capture s' transmissions, given m being the distance between s and r, the distance between v and r must be greater than $\sqrt{\alpha}\,m$. For s to capture r's transmissions, given x being the distance between v and s, r must be within a circle of radius $min(R, \frac{x}{\sqrt{\alpha}})$. Considering both conditions, r must be located within the shaded area $A(x)$ in the figure. Hence, the probability that v's transmission *doesn't* corrupt the communication between s and r is:

$$P(B|x) = \frac{A(x)}{\pi R^2} \tag{5.6}$$

where the area $A(x)$ is calculated as follow:

$$A(x) = \int_0^{min(R, \frac{x}{\sqrt{\alpha}})} 2(\pi - \arccos(\frac{x - \frac{x^2 - m^2 + (\sqrt{\alpha} m)^2}{2x}}{m}))m\,dm \tag{5.7}$$

Since we only worry about potential interferers within the carrier sensing range, by unconditioning x we obtain:

$$P(B) = \int_0^C \frac{A(x)}{\pi R^2} \frac{2x}{C^2}\, dx \tag{5.8}$$

Based on the traffic model, the probability that none of the nodes within the carrier sensing range of a node will transmit is obtained by:

$$P_1 = [1 - \frac{\tau}{T}]^{\delta \pi C^2} \tag{5.9}$$

and the probability that v's transmission will not interfere with other transmissions (if any) in the carrier sense range is:

$$P_2 = [1 - \frac{\tau}{T} + \frac{\tau}{T} P(B)]^{\delta \pi C^2} \tag{5.10}$$

Therefore, the probability P_b that v can transmit with the presence of a nearby transmission without corrupting this transmission is given by:

$$P_b = P_2 - P_1 \tag{5.11}$$

Note that the calculated P_b is still conservative because of the following assumptions:

1. Only the Friis propagation model is used in the analysis because we assume $C < D_{cross}$. However, in practice C may be greater than D_{cross} and thus the distance x could also be greater than D_{cross}. In this case, the two-ray ground model may be used instead, which further reduces the probability of the interference and consequently increases the P_b.

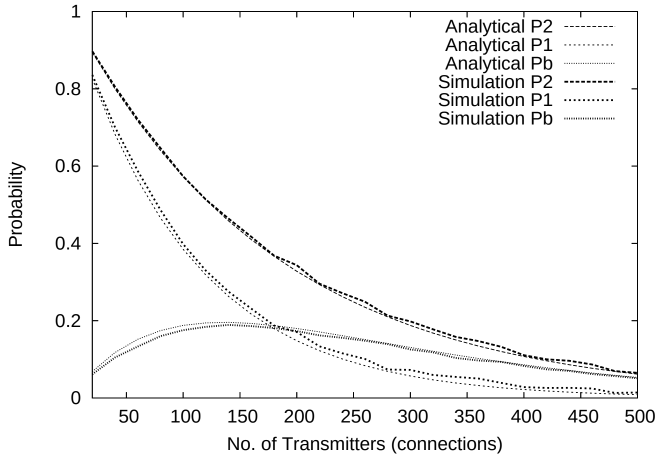

Figure 5.5: The analytical and simulation values of the probabilities P_1, P_2, and P_b

2. In the analysis, for simplicity, we assume that all nodes in the vicinity of v have the freedom of transmission. We do not take into account that some of these nodes will have to block because of other ongoing transmissions in their vicinities. Accounting for these blocked nodes would increase P_b.

3. In many other studies such as the [76], researchers have observed that in many scenarios, the propagation model for non-line-of-sight path has a path exponent factor greater than what the Friis model uses. This also reduces the probability of the interference and consequently increases the P_b.

We have verified our analytical results by generating random network topologies and traffic patterns and studying the interference situation in each case. We have also studied how our simplified assumptions stated in the previous paragraph affect our blocking probability estimation by relaxing them in simulation runs.

For constructing each random network, we place the v node at the center of an area of 1000×1000. Transmitter nodes are distributed uniformly in this area. Each

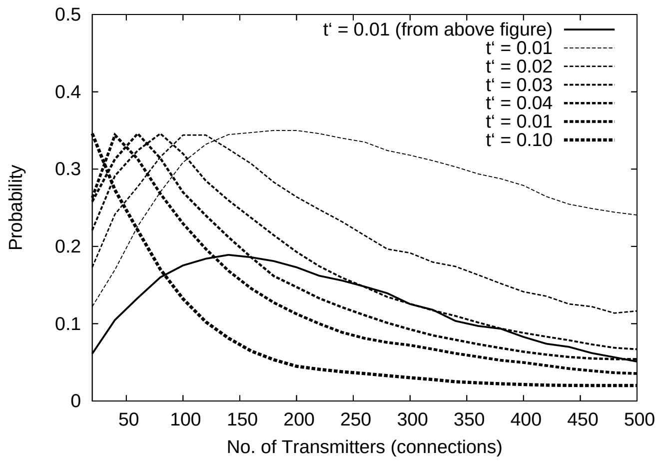

Figure 5.6: The probability P_b with different load values t' where $t' = \tau/T$

transmitter is paired with a corresponding receiver, whose location is randomly picked within a circular area which is centered at the transmitter and with radius R. Then each transmitter starts transmitting following the traffic model described before: all packets require transmission time τ and they are generated randomly at a constant rate: one packet every time interval T, where $T \gg \tau$. When v has a frame to send, we study if it will be blocked under the current IEEE 802.11 operations and when blocked if indeed v's transmission will harm other communications. The number of situations where the IEEE 802.11 suggests unnecessary blocking is then divided over the total number of simulated situations to derive the probability of unnecessary blocking, which is compared to the analytical result.

Figure 5.5 plots both the analytical and the simulated values of P_1, P_2, and P_b for R=250, C=550, α=5, τ/T=0.01, and different numbers of nodes (thus varying the node density δ). As we can see, the simulation results closely match the analytical results that validate our analysis.

Figure 5.6 plots the simulation of P_b with the simplification assumptions relaxed. In addition, this figure plots P_b with different packet load values. The P_b plot with these assumptions, which is directly copied from Figure 5.5, is also included for easy comparison. The plots show that our analytical results are conservative.

As expected the probability above only takes into account whether the node's transmission may corrupt other ongoing data deliveries. It does not address if the intended receiver will receive this transmission correctly. This transmission may still fail at its receiver if other ongoing data deliveries produce enough interfering energy there.

The above analysis shows that the unnecessary blocking probability of DCF is large enough (as high as 35%) to motivate us to consider modifying the MAC layer to exploit the capture phenomena of the physical layer. In the following section, we will describe the newly proposed modification to the IEEE 802.11 DCF.

5.3 Location Enhanced DCF Protocol

In this section, we describe our Location Enhanced DCF (LED) for IEEE 802.11 by first giving an overview of the LED mechanism. Then, we describe the design of the needed physical layer. Finally, we present the proposed modifications to the IEEE 802.11 MAC with the details of LED mechanism. Before we introduce our approach of using location information and capture effect to improve channel efficiency, several terms that will be used during the description, need to be clarified to avoid confusion.

In our description, we use the term "delivery" for the whole handshake procedure for delivering a unicast data frame. Depending on the frame size and network configuration, a “delivery” may involve the full RTS-CTS-DATA-ACK 4-way frame exchange sequence or just DATA-ACK 2-way exchange. A “source” is the node having data to send during a delivery. The “destination” of a delivery is the node to whom the source wishes to send data. While “source” and the “destination” regard data frames only, the terms “sender” and “receiver” on the other hand refer to the sender and the receiver of *any* individual frame, RTS, CTS, DATA, or ACK. For instance, the senders of CTS and ACK frames are actually the destinations. In addition to the above, “transmitter” is used interchangeably with “sender”, and “connection” is used to refer to both the source and destination nodes collectively.

5.3.1 Protocol Overview

Our approach is: to include more information about each transmission in the transmission itself so that any other nodes overhearing the transmission are able to better assess whether their own transmissions may harm this ongoing delivery. Among various relevant parameters, the locations of the transmitters and receivers are the most important. We assume that each node is capable of acquiring its own location, e.g. by GPS [37] or other RF based localization methods [10, 68]. A node can retrieve other communication parameters regarding its own transmitter/receiver easily as they are typically configuration parameters.

When the above parameters are included in each transmission, an overhearing node of a data delivery can compute the received power level of the frames belonging to the same data delivery at their receivers, using a propagation model suited for the surrounding environment. Then, if the receiver's capture ratio is known; using its own location, antenna gain, and transmission power, the node can make a prediction of whether its own transmission may affect this ongoing data delivery. If the result is negative, this node should not block its own transmissions, if any, despite the presence of the ongoing data delivery. This is the core of the LED mechanism. When the LED predictions are accurate, each transmissions will not affect the correct receptions of others at their corresponding receivers if these receivers are capable of frame capture. Network wide, more concurrent transmissions are permitted by LED and the overall network throughput is improved.

The use of propagation model to predict interference may introduce certain limitations on how LED can be applied in real world applications. For instance, as [76] points out, path-loss in in-door environments tends to be very dependent on building structure and construction. Thus a propagation model, no matter how well it may work for one deployment, may not be a good choice for other deployments. Note that the protocol operations of LED are not affected by the choice of underlying propagation model. Thus, a LED-based system design may wish to build in the flexibility of plugging in different propagation models under different operation environments. Additional measurement-based control mechanisms may also be included in such a system in an open-loop fashion so that the prediction model can be better "tuned" for non-distance induced fading conditions.

This is a rather simplified estimation model as each node considers only the effects from its own potential transmission. It may occur that several nodes simultaneously predict that their own transmissions will not cause collision to the ongoing delivery. In this event, the aggregated energy from all these side transmissions may actually change the result of the capture effect and cause enough interference with the ongoing delivery. We slightly addressed this issue at the performance evaluation section. However, we postpone further studies for this issue to future works.

One particular issue we should point out is that in the current model, a node is only concerned if its own transmission will affect any ongoing deliveries. The prediction model does not consider if the node's own transmissions can be received correctly by the intended receivers. This optimistic approach is largely for keeping the model simple at its current stage. Also from MAC perspective, a node can always learn if its data frames have been received correctly by observing the reception of ACK frames.

5.3.2 Physical Layer Design

As we have pointed out, the current IEEE 802.11 standard does not require a receiver modem to be able to capture a new (stronger) frame after the receiver has been tuned to receive another frame, even if the signals of the new frame are strong enough to be captured. As we explained before, unless the frame capture capability is specifically designed into the receivers, they usually are not able to correctly capture the new frame. This may cause problems in our approach. If a node decides to transmit after it estimates that its own transmission will not interfere with an ongoing delivery, it will begin to send its own frame. However, chances are that the intended receiver of this frame is already engaged in receiving another frame, one of the frames of the ongoing delivery. As a result, this receiver will not receive and interpret the new frame correctly even if the signals are strong enough.

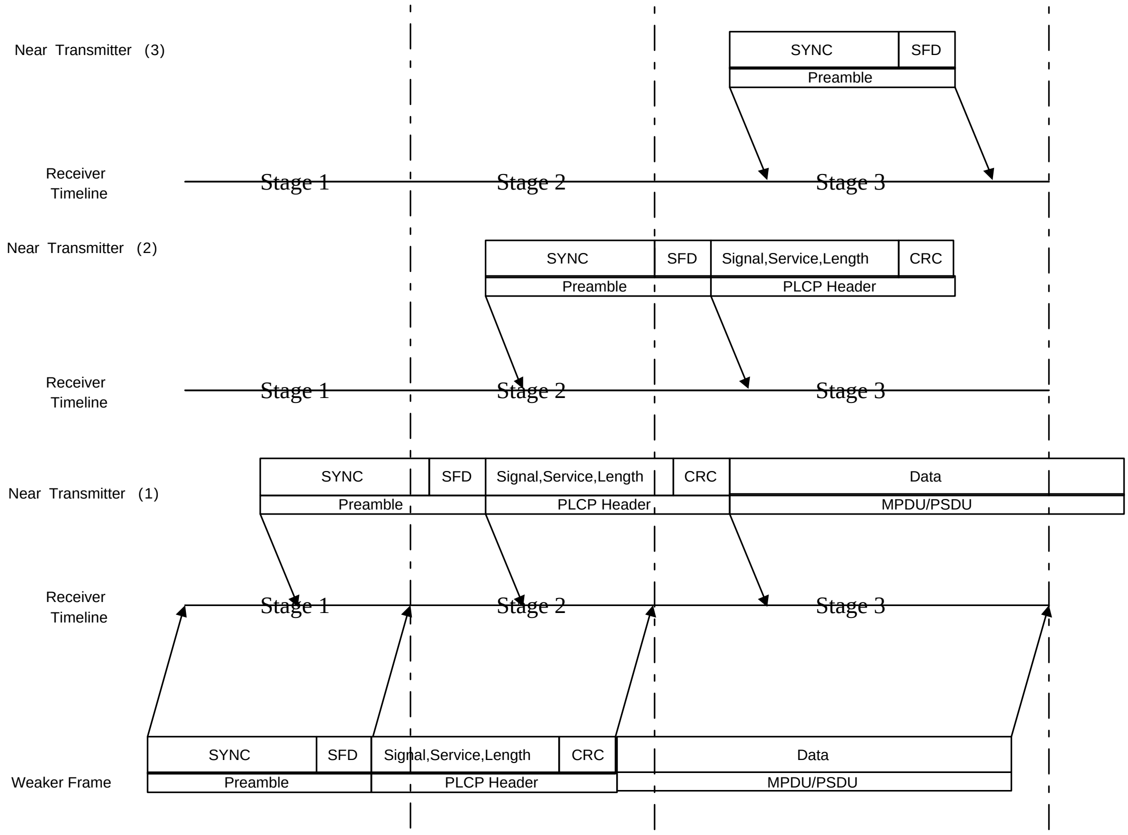

Figure 5.7: Packet Capture of IEEE 802.11

Let us consider more detailed analysis of what may happen at a receiver, which does not provide support for frame capturing, when a stronger frame arrives after the receiver has begun receiving a weaker frame. Depending on what moment the beginning of the stronger frame arrives during the reception of a weaker frame, there are three different situations as shown in Figure 5.7. Each IEEE 802.11 DSSS frame has three sections based on their affects on receiver's physical and MAC layer operations: the Physical Layer Convergence Protocol (PLCP) Preamble section is used to train the receiver modem for synchronization, the PLCP Header section contains medium (DSSS) dependent information such as modulation choice and frame length, and the PSDU section contains the actual MAC layer data.[1] Accordingly, the reception of a frame is also broken into three stages.

1. If the stronger frame arrives during the training period of the modem towards receiving the weaker frame (stage 1), the modem is able to be retrained and switch to reception of the new stronger frame.

2. If the stronger frame arrives during the reception stage of the weaker frames PLCP header, or stage 2 in the illustration, the new signal would likely destroy the data contained in the weaker frames PLCP header and result in PLCP reception error or CRC failure, in which case the receiver goes back to idle state. Then, if this happens soon enough, the receiver may still be able to detect the new carrier for the stronger frame and be trained for receiving it, if the stronger transmission is still in

[1] In the original IEEE 802.11 standard, this section is called MAC Protocol Data Unit (MPDU). The later IEEE 802.11b standard changes it to PSDU (PLCP Service Data Unit).

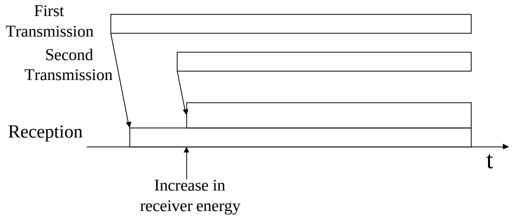

Figure 5.8: Message-In-A-Message

its SYNC portion of the frame.

3. If the stronger frame arrives during the reception stage of the weaker frames PSDU (stage 3), it would most likely destroy the reception due to two major reasons. First, the demodulation algorithm the receiver is currently engaged in for the weaker frame may be different from the modulation used by the stronger frame. Second, the bits of the stronger frame, even correctly demodulated, are interpreted as part of the PSDU of the weaker frame and passed up for MAC processing. After the whole message is received, the MAC forward error detection mechanism will fail and the frame is dropped. Unless the stronger transmission is still in its SYNC section and the receiver can catch it quick enough, the stronger frame will not be received correctly either.

For nodes that have received a frame in error, obviously, they cannot determine the duration of the reservation, they need to wait for an Extended Inter-Frame Space (EIFS) after the carrier becomes idle. The EIFS will leave enough time for the on-going frame exchange to finish.

Fortunately, receiver designs, which do support the capture of a new frame after the receiver has already begun to receive another frame, do exist. One example of such

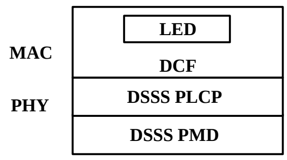

Figure 5.9: PHY-MAC layer structure

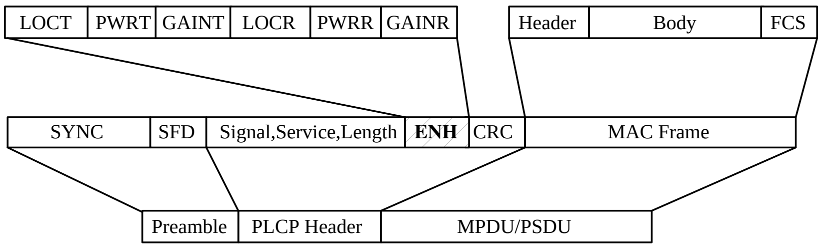

Figure 5.10: Frame structure

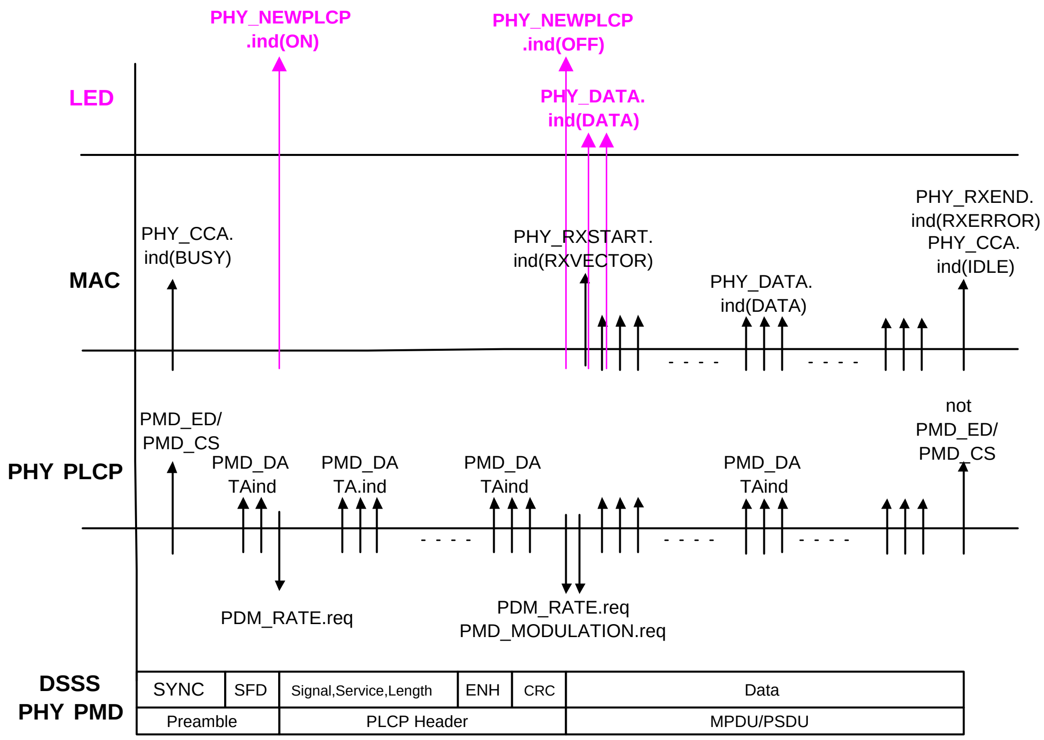

Figure 5.11: PHY-MAC interactions

a receiver physical Layer (PHY) design is Lucent's PHY design with "Message-In-A-Message" (MIM) support [17]. In this design, the newly arrived frame is referred to as the "(new) message in the (current) message".

A MIM receiver is very similar to the normal IEEE 802.11 PHY designs except that it continues to monitor the received signal strength after the PHY transits from receiver training state to data reception state. If the received signal strength increases significantly during the reception of a frame, as shown in Figure 5.8, the receiver considers that it may have detected the beginning of a MIM frame and hence switches to a special MIM state to handle the new frame.

While under the MIM state, the receiver tries to detect a carrier for a new frame. If the carrier signal is detected, the receiver begins to decode the initial portion of the new frame and retrains to synchronize with the new transmission. If no carrier, preamble, or frame delimiter is detected, which indicates that the energy increase is likely caused by noise, the PHY will remain in this MIM state until either a carrier is detected or the scheduled reception termination time for the first frame is reached.

With a MIM-capable design, a receiver is able to correctly detect and capture a strong frame regardless of the current state of the receiver, unlike the regular IEEE 802.11 PHY designs where the strong frame can only be correctly captured while the PHY is under certain (i.e. receiver training) states during its reception of a weak frame.

5.3.3 MAC Layer Design

Our enhanced design for a DCF MAC stands atop a MIM-capable PHY. Figure 5.9 illustrates the layered structure of the relevant entities. The IEEE 802.11 Physical Medium Dependent (PMD) layer performs wireless medium transmission and receiving services. The Physical Layer Convergence Protocol (PLCP) layer adapts the raw services of PMD to PHY-MAC data and control interface. The new LED is a part of the MAC layer function. Figure 5.10 shows the frame format to support the enhanced functionalities of the new MAC.

We propose to insert a block of information called ENH ("Enhanced") to provide the additional information needed for the LED. Since the earlier the ENH block is received, the sooner the receiver can decide if it needs to block its own transmission, the ENH block should be inserted before the true MAC data section, also known as the PLCP Service Data Unit (PSDU). In the current design, we have the ENH as part of the PLCP header instead of at the beginning of PSDU mainly due to two reasons. Firstly, the PLCP header has its own CRC field so the contents of the ENH block can immediately be verified and utilized. Secondly, all nodes within the service set can understand the ENH block since the PLCP header is transmitted at a base rate.

The ENH block is further divided into six fields. The LOCT field contains the location of the frame transmitter, the PWRT field describes the transmission power of the transmitter, and the GAINT field specifies the transmission antenna gain. The LOCR, PWRR, and GAINR fields contain the same pieces of information for the receiver.

If RTS/CTS exchange is needed for a data delivery, a source starts its unicast data delivery by sending out an RTS frame to reserve the channel. In the ENH block of this frame, the source fills the LOCT, PWRT, and GAINT fields with its own parameters, and the LOCR, PWRR, and GAINR with the destination's parameters, if known. Any unknown parameters are set to NULL. Upon receiving the RTS, the destination of the data delivery copies the LOCT, PWRT, and GAINT fields into the corresponding fields of its CTS frame. It also fills or updates the LOCR, PWRR, and GAINR fields of the CTS frame with its own parameters. In subsequent DATA and ACK frames, full descriptions of both the source and the destination are included. In case of the frame size being less than the RTS/CTS threshold and no RTS/CTS handshake being conducted, the DATA frame will have its fields set in the same fashion as the RTS frame, and the ACK frame is filled the same way as the CTS frame.

A parameter cache may be maintained by nodes to store the location, power, and antenna information of already known nodes. This way when sending data to a node in cache, the cached parameters may be used in the corresponding fields of the ENH block instead of NULL values. Cache entries are updated if newer information is received from their corresponding nodes. Cache entries are removed after the expiration time.

In the standard IEEE 802.11, normally the PHY (PLCP in particular) will signal three evens to the MAC layer during frame reception: carrier busy, begin receiving PSDU, and end receiving PSDU. It does not deliver any data bits to the MAC layer until the PSDU reception has begun. Then the receiver will proceed until the end of the frame (unless interrupted by carrier loss in the middle of the reception). Received bits are passed to the MAC layer as they are decoded and assembled into the MAC frame. At the end of the PSDU is the forward error detection CRC block called Frame Check Sequence (FCS).

If the MAC frame passes the CRC check; it is accepted and passed up for further IEEE 802.11 MAC processing. If the CRC fails, the frame is dropped.

In addition to the above interactions, the LED defines two new mechanisms for the PLCP layer to interact with the LED. They are illustrated by Figure 5.11. The first is an indicator called PHY_NEWPLCP. The PLCP layer turns on this indicator after it finishes receiving the Start Frame Delimiter (SFD) field of a frame's Preamble section. The meaning of this indicator is that the PHY is affirmative that it has begun receiving a new frame, and the next thing it expects is the PLCP header of the frame. Upon receiving this indicator, the LED needs to block transmission so the PLCP header can be received without interruption. The PLCP layer will turn off the PHY_NEWPLCP indicator after it finishes receiving the CRC field of the PLCP header. The second mechanism is for the PLCP layer to pass up the PLCP header contents to the LED, as soon as the PLCP is verified to be correct by CRC checking. After receiving the PLCP header from the PLCP layer, the LED will make a decision if the physical layer should block its own transmission.

During the blocking decision-making process, a non-receiver node (denoted as node i) of the frame calculates if its own transmissions will cause enough interference to interrupt the data delivery to which the just received frame belongs. The node needs to calculate the power level of its own transmission at both the source, denoted as P_i^s, and the destination, denoted as P_i^d, of the ongoing data delivery using an appropriate propagation model (i.e. Equation 2.1). The node also needs to calculate the received power level of the destination node's transmission at the source, denoted as P_d^s, and that of the source transmission measured at the destination, P_s^d. If $(P_d^s > \alpha P_i^s)$ and $(P_s^d > \alpha P_i^d)$, the node should not block its own transmissions. Otherwise, it should block its transmissions. In the case that the communication parameters of either the source or the destination are unknown, the assessing node assumes the worst and blocks its own transmission.

If the node decides to block its own transmission due to worries that the transmission may affect the correct reception of some frames of the ongoing data delivery, it remains in receiving state and continues the receiving procedure as specified by the standard. It disables any transmission request from upper layer, and sets its NAV value according to the Duration field of the frame, which is set to the time required for the full data delivery exchange sequence to finish. One thing to note is that on the intended receiver of the frame, the blocking estimation implicitly will always produce positive result.

On the other hand, if the node decides not to block, the receiving may continue but upper layer transmission requests are not disabled. No NAV is set in this case either. If there is indeed any outgoing frame ready, the modem can accept the request by switching to transmission state and starting the transmission. A PHY reset signal is needed in this case to force the PHY to leave the receiving state and enable PHY_TXSTART signal when the MAC has a frame to send.

If the LED decides not to block, the handling of the physical carrier sensing mechanism, i.e. the Clear Channel Assessment (CCA) indicator produced by the physical layer, requires careful consideration. CCA is set to busy when there is carrier being detected. Since the frame is still being transmitted in the air, the CCA will remain busy. It needs to be temporarily ignored. The overriding of CCA in LED layer is accomplished by proposing a new vector called CCA-Suppression Vector (CSV), which is a suppression timer. CSV is set to the end of reception of the current frame, calculated based on the length field contained in the received PLCP header of the frame.

During the reception of a frame, if a new stronger frame arrives and captures the receiver, the PHY will again pass up the PLCP header to the LED upon successfully verifying the CRC. The LED will estimate interference again using the new PLCP header. If the LED decides to block transmission for this new data delivery, NAV is set to the end of *this* new delivery, if it is later than the current NAV expiration time. Start-to-transmit requests are disabled as well. If the LED decides not to block for this new delivery, the NAV value is not changed but the CSV expiration time remains or set to the end of the new frame, whichever is later.

At the source or the destination node of the ongoing delivery, according to the IEEE 802.11 standard, the NAV is not set for the duration of the delivery. In LED, this specification is still followed. However, in LED the source and the destination nodes of a data delivery do need to set their CSV's to the estimated end of the delivery. The reason is as follows. LED permits concurrent transmissions by other nodes as long as they do not produce enough interference to disturb the ongoing delivery. If any other node indeed decides to transmit, the energy of the transmission may cause the source and the destination of the ongoing data delivery to sense that CCA is busy and thus abort the data delivery frame sequence. Hence, the CCA should be suppressed on the source and destination nodes till the end of the data delivery.

In total, a LED node has four indicators related to the transmission blocking estimation. The CCA is the physical carrier indicator. It is "TRUE" when the PHY layer detects carrier (or energy exceeding threshold, or both, depending on equipment vendor implementation). The NAV indicator is the virtual carrier indicator. It is “TRUE” when there is a channel reservation which needs to be honored. That is, if this node transmits, then the transmission will interfere with the ongoing delivery. The PHY_NEWPLCP indicator is on while a PLCP header is being received. Finally, the CSV indicator tells the node if it should ignore the physical layer CCA. It is “TRUE” when the suppression timer is running. More precisely, the decision of whether this node should block its own transmission or not, is made as follow:

if (PHY_NEWPLCP *or* ((CCA *and* (*not* CSV)) *or* NAV)) *then* BLOCK

Another issue occurs if a channel-assessing node only detects carrier but cannot decode the frame. In this case, a node is not able to estimate whether its transmission will affect this ongoing transmission. Either an aggressive approach or a conservative approach can be taken. In the aggressive approach this node will not block its own transmission in the event of “detecting a carrier but not being able to decode the frame”, while in the conservative approach this node will block its own transmission.

5.4 Performance Evaluation

In this section, we present extensive simulation-based studies on the performance of the LED mechanism. The performance comparisons are done using the *ns-2* simulator [3], enhanced with the CMU-wireless extensions [2]. The underlying link layer is IEEE 802.11b with 11 Mbps data rate [5]. In doing this, we have extended ns-2 as follows:

- We have modified the capture model to allow receivers to capture the stronger packet out of the weaker packet(s), as in Equation 2.2, if the stronger packet comes after the weaker to reflect the MIM PHY design as discussed in the previous section.

- Current implementation of ns-2 allows the nodes to compare the newly-arriving packet only with the one it is receiving. In order to implement the capture Equation 2.2, we extended the PHY layer in ns-2 to allow each node to keep track of all its incoming packets and the aggregated background signals. Also in order to create a more realistic environment, we allow each node to aggregate the signals that have lower values than the CSThresh_ [2] used by ns-2.

- We have enhanced the IEEE 802.11 MAC layer by extending it with the implementation of our LED mechanism.

5.4.1 Simulation Environment

Each of our simulated networks consists of a set of connections that are constructed as pairs of stationary sender and receiver nodes. The senders and receivers are placed in a $1000m \times 1000m$ area in the same fashion as the simulations described before in Section 5.2. We assume that each sender has already cached the location of its corresponding receiver. Other parameters such as transmission power levels and antenna gains are also assumed to be fixed and known to all nodes therefore not included in simulation. In simulation, the ENH header only contains LOCT and LOCR fields of 32 bits each.

[2] CSThresh_ is the power value of a transmitted signal measured at the boundary of its carrier sense range C

In ns-2, we adopted the propagation channel model described in Equation 2.1. With this model, the transmission power P_t is set to 0.282W while $RXThresh\_$ [3] and $CSThresh\_$ are set to configure the transmission radius R of a node to 250m and the carrier sense radius to 550m. Each connection is a flow of UDP packets that are 1000 bytes in size and transmitted at 11Mbps. To simplify the simulation implementation, base rate is also set to 11Mbps. Such a simplification should not affect the correctness of the evaluation method since we are more interested in relative performance improvement. Each simulation is run for a fixed duration of 50 seconds. Each point on the curves to be presented is an average of 5 simulation runs.

We have not been able to find any IEEE 802.11 equipment specification with capture ratio information. The capture ratio used in simulation is derived by the following method. To achieve a specific Bit Error Rate (BER) the required Signal to Noise Ratio (SNR) for a particular modulation technique can be calculated. In the case of 11Mbps CCK modulation, according to calculations described by [105], it can be determined that 18dB of SNR is needed to achieve 10^{-8} BER, as specified by Orinoco wireless cards. The 11 Mbps CCK uses 8 chip/symbol, which is 9dB spreading gain. In addition, CCK coding provides about 2dB additional coding gain. All together, the processing gain is 11dB. When only considering signals before receiver processing, the SNR requirement is 7dB. Roughly, this maps to 5 times of signal power over interference. We adopt the same number as the capture ratio. In our model, when a node is in the middle of receiving frame A and frame B arrives, one of the following will happen. If the received power of

[3] RXThresh_ is the power value of a transmitted signal measured at the boundary of its transmission range R

frame A, P_A, is more than 5 times of P_B, the receiver continuously receives frame A. If P_B is more than 5 times of P_A, the receiver drops frame A and begins receiving frame B. In all other situations, packets collide and no frame is received correctly.

We have modeled various scenarios of different node densities, workloads, transmission and carrier sense ranges (transmission power levels), and errors in location estimation and their effects on performance. To study the performance of our suggested schemes, we compare our LED with both the ***Original*** IEEE 802.11 DCF and ***MACAW*** mechanisms[4]. The reason for using MACAW is that comparing to the schemes in [20] and [29] MACAW is less restrictive when making blocking decisions, and consequently the MACAW scheme outperforms the two aforementioned schemes. As described in Section 5.3, we experiment with two different flavors of LED: ***LED_CS*** and ***LED_RX***. LED_CS mechanism is an aggressive (optimistic) version of LED mechanism in which when a node receiving a frame it cannot decode [5], it simply assumes that its transmission will not interfere with that ongoing data delivery and therefore should not block. On the other hand, LED_RX is a conservative (pessimistic) version of LED in which a node assumes its transmission will interfere with the ongoing data delivery under the same situation.

During the simulation runs, we take the following measurements:

1. **Effective Throughput:** This counts the total number of data received by all the receiver nodes over the simulation period.

[4]Both Original and MACAW mechanisms use the extended ns-2 capture model as described earlier.

[5]In ns-2 this is the situation where the received signal level is lower than the RXThresh_.

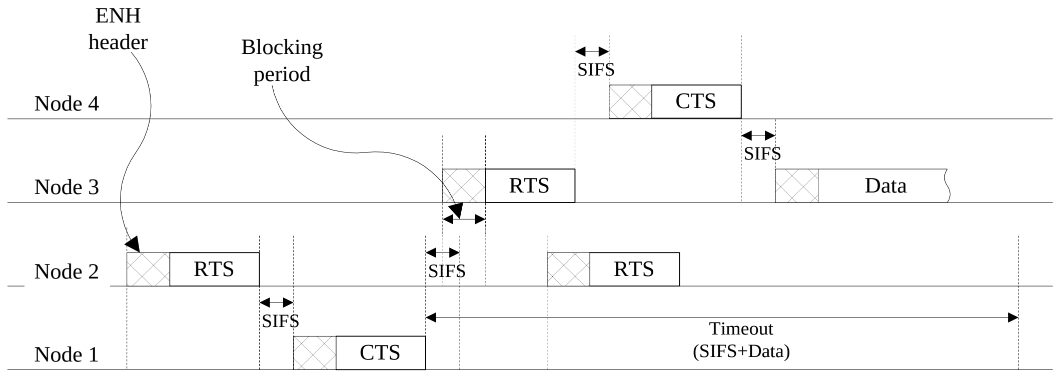

Figure 5.12: Medium under utilization scenario of LED mechanism

2. **Collision Packets:** This counts the total number of observed collisions that involve data and ACK packets by all the attempted deliveries over the simulation period.

3. **Fairness Index:** To measure the bandwidth sharing of the connections under different mechanisms, we use Jain's fairness index [26, 59] that is defined as follows:

$$F = \frac{(\sum_{i=1}^{N} \gamma_i)^2}{N \sum_{i=1}^{N} \gamma_i^2} \tag{5.12}$$

   where N is the number of connections and γ_i is the number of received packets for connection i.

We have experimented using both RTS/CTS and basic access modes. In RTS/CTS access mode, although the LED mechanism forces each node to be blocked during the ENH header of each received frame, we found that forcing the node to be blocked during the RTS/CTS period of the other connections would increase the network throughput. The reason for this is more related to the IEEE standard 802.11 and the corresponding ns-2 implementation of the physical layer. To explain this, consider Figure 5.1 in which node 2 and node 3 have packets to send to node 1 and node 4 respectively. Assume node 2 would start the transmission cycle by transmitting RTS packet to node 1 as shown in Figure 5.12. When node 1 receives the RTS packet, it waits for SIFS period and, if the medium is still idle, transmits the CTS to node 2. After CTS transmission, the ns-2 implementation of node 1 sets a timer for period equal to a SIFS period plus the period for the data packet transmission. If node 1 doesn't receive the expected data packet during this time period, it timeouts and marks the failure of the current transmission cycle. As in Figure 5.12, node 3 detects the CTS packet, figures out that its transmission will not affect the on going transmission, and hence decides to start its own transmission cycle by transmitting the RTS packet that happen to be within the SIFS period after the CTS packet of node 1. Since LED mechanism forces each node to be blocked during the ENH header of each received frame, node 2 will be blocked during the ENH period of the RTS of node 3 which happen to last more than the SIFS period. Therefore, node 2 won't be able to transmit the data packet and marks the failure of its current transmission cycle. After waiting for DIFS and a doubled contention window, node 2 tries to start another transmission cycle by sending new RTS packet to node 1 as shown in the Figure. However, the IEEE 802.11 standard does not specify how a node should react when it receives non-data packet while it is expecting to receive a data packet during a certain time period. In ns-2 implementation, a node drops any non-data packet (e.g. RTS packets) during the period it is expecting a data packet. Therefore, node 1 that is expecting data packet drops the RTS of node 2. Consequently, node 2 timeouts for CTS packet and detects an unsuccessful transmission and. Again, after a DIFS period and new doubled contention window, node 2 tries again to send a new RTS packet. This mechanism/implementation under utilizes the medium and hence reduces the network throughput. To enhance the

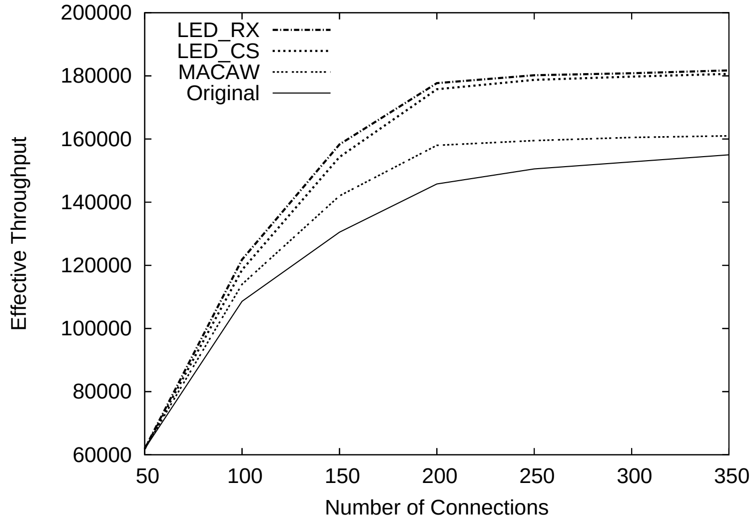

Figure 5.13: Effective throughput versus node density using RTS/CTS access mode

network performance by eliminating such problem, we forced each node to be blocked during the transmission period of RTS/CTS cycle. This could be done by including the blocking duration information in the ENH header or set one of the locations in ENH to null to force the nodes to be blocked for the whole packets and then set NAV to the end of RTS/CTS cycle instead of the while transmission cycle. Back to Figure 5.12, with this mechanism, node 3 will block its transmission during the RTS/CTS exchange between node 1 and node 2 in addition to at least a DIFS period. This guarantees that node 2 be able to transmit its data packet with its ENH block and hence the on going transmission cycle will not be disturbed.

5.4.2 Impact of Node Density

Figure 5.13 shows the effective throughput of the networks with different numbers of connections. The data traffic between each pair of source and destination is a constant

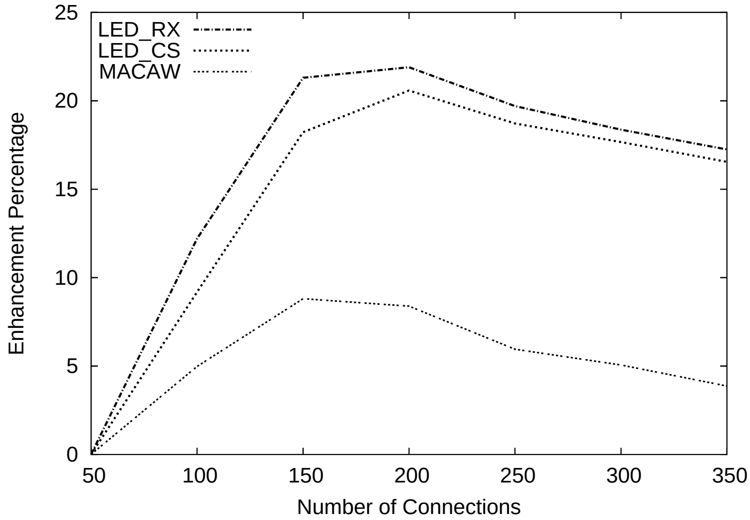

Figure 5.14: Throughput enhancement over Original mechanism versus node density using RTS/CTS access mode

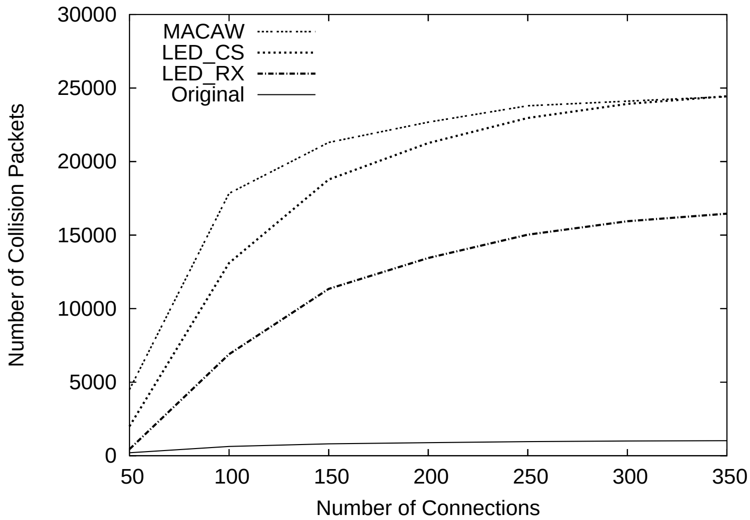

Figure 5.15: Packet collisions versus node density using RTS/CTS access mode

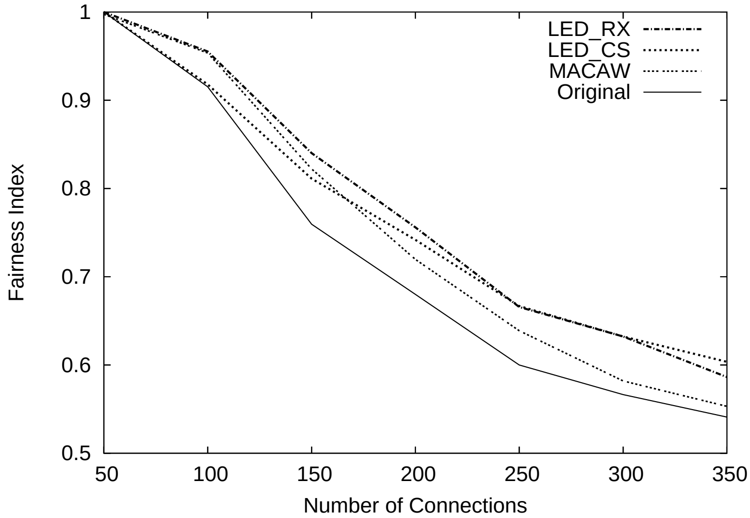

Figure 5.16: Fairness index versus node density using RTS/CTS access mode

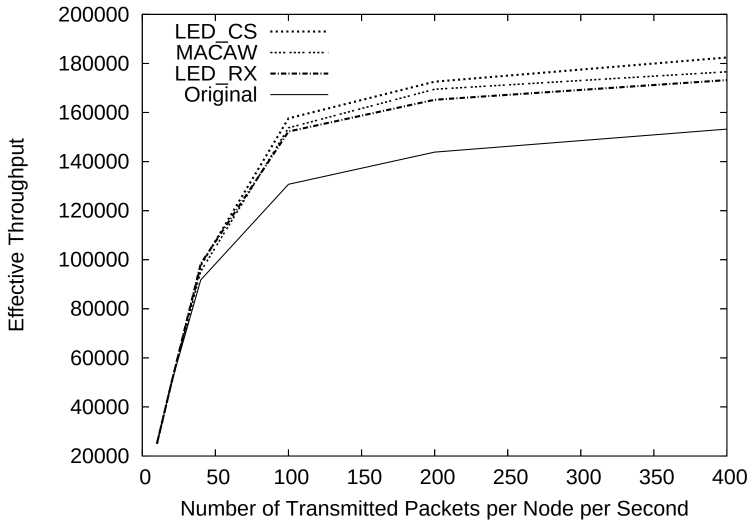

Figure 5.17: Effective throughput versus network load using RTS/CTS access mode

bit rate (CBR) UDP flow at a rate of 20 packets per second. As shown, the LED_CS, LED_RX, and MACAW mechanisms all have higher data throughput than the Original mechanism. Figure 5.14 further illustrates the improvements by showing the percentage throughput gain of using the LED_CS, LED_RX, and MACAW over the Original. At their peaks, the LED_CS could achieve about 20% more throughput than the Original and the LED_RX could reach 22% higher throughput while the MACAW could see 8% throughput gain. The LED_RX yields higher throughput than the LED_CS for because of its aggressive nature. Figure 5.15 shows the total number of collisions that occur in the networks occurred at intended frame receivers, as an indication of the level of transmission concurrency within the network. Since the LED_CS is more aggressive than the LED_RX, as expected its collision count is higher. However, simply trying harder may not help in this case because more transmissions may result in more collisions at frame receivers, which actually brings the throughput down.

Lacking more detailed knowledge regarding the ongoing transmissions, the MACAW does not spatially reuse the channel as intelligently as the LED mechanisms. A node using the MACAW blocks it transmission only if it overhears CTS frames. As the simulations show, oftentimes such an assessment is incorrect. Although the MACAW tries very hard, as indicated by the high number of collisions in Figure 5.15, its throughput does not increase as hoped. As the node density increases, the MACAW performance approaches Original since the CTS frames will cover most of the network area, just like the RTS and CTS frames of the Original. Figure 5.16 shows the fairness index of different mechanisms: LED_CS, LED_RX, and MACAW. The newly proposed mechanisms of the LED have better fairness levels than the Original. An explanation for this is that the LED

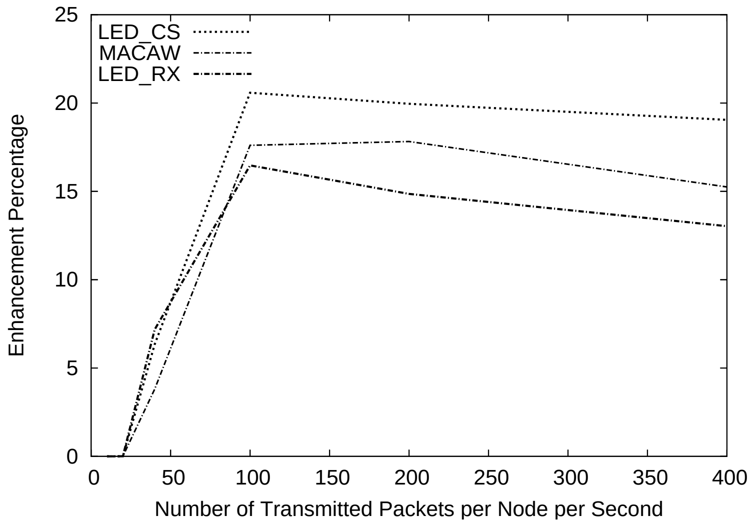

Figure 5.18: Throughput enhancement over Original mechanism versus network load using RTS/CTS access mode

mechanisms reduce the well known “exposed node” problem in the Original mechanism which is one of the major sources for the unfairness.

5.4.3 Impact of Network Load

Next, we experiment with different network packet loads to see their effects on performance. We fix the number of connections in the network to 50 and vary the packet generation rate at each source node between 10 to 400 packets per second. Figures 5.17 and 5.18 show the effective throughput and the relative enhancement of each mechanism over the Original respectively. As shown, different from the previous results, the LED_CS has the highest throughput over the LED_RX and the MACAW. The LED_RX performs not as well as the LED_CS and the MACAW under high packet loads. With high packet loads, the chance that there are some frames being transmitted nearby increases. Thus, it is more likely for the LED_RX to decide to block. This is opposite to the LED_CS that

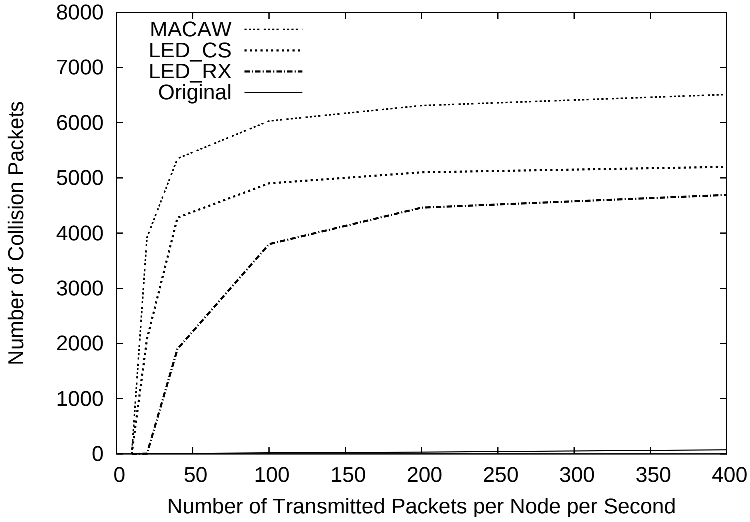

Figure 5.19: Collision packets versus network load using RTS/CTS access mode

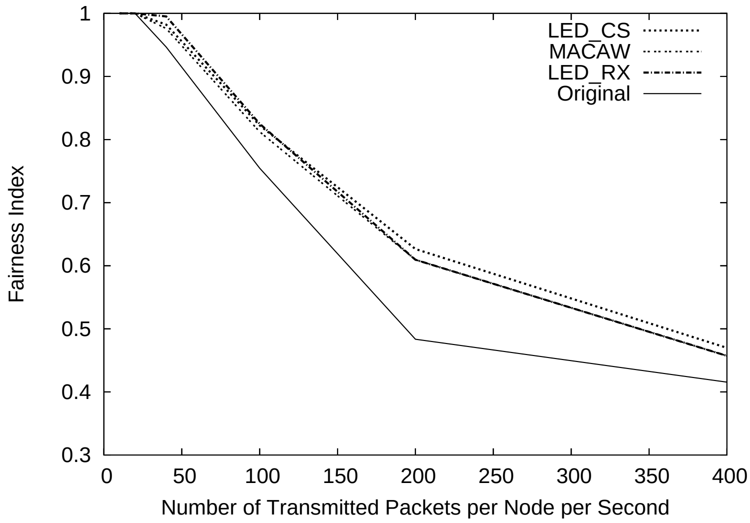

Figure 5.20: Fairness index versus network load using RTS/CTS access mode

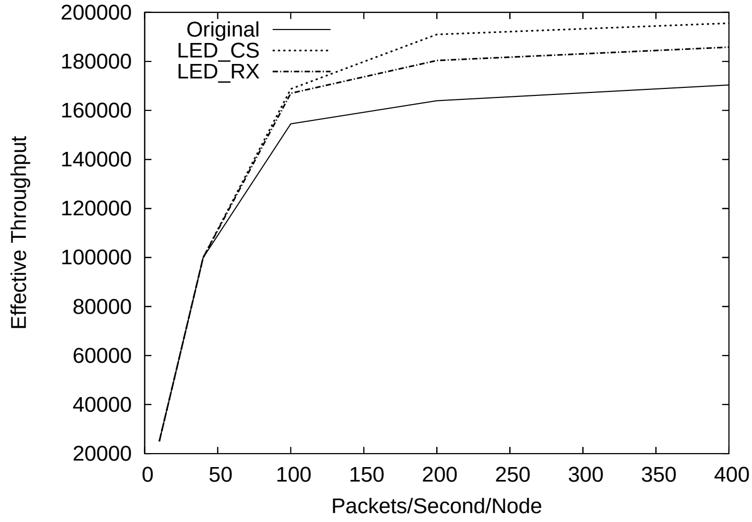

Figure 5.21: Effective throughput versus network load using basic access mode

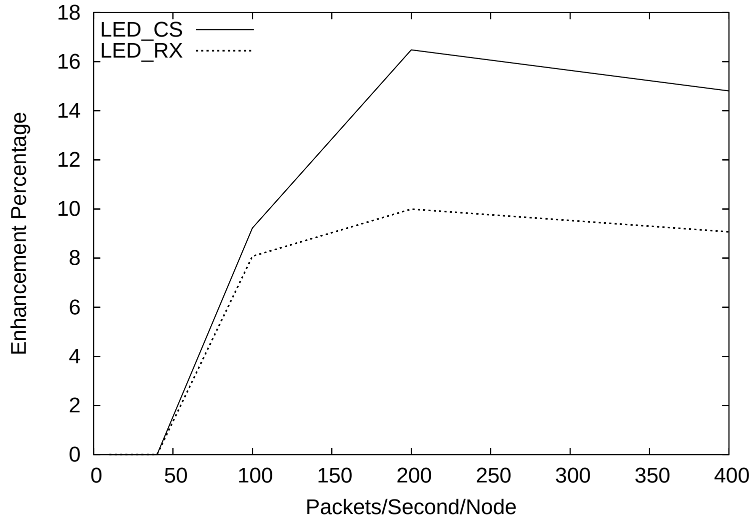

Figure 5.22: Throughput enhancement over Original protocol versus network load using basic access mode

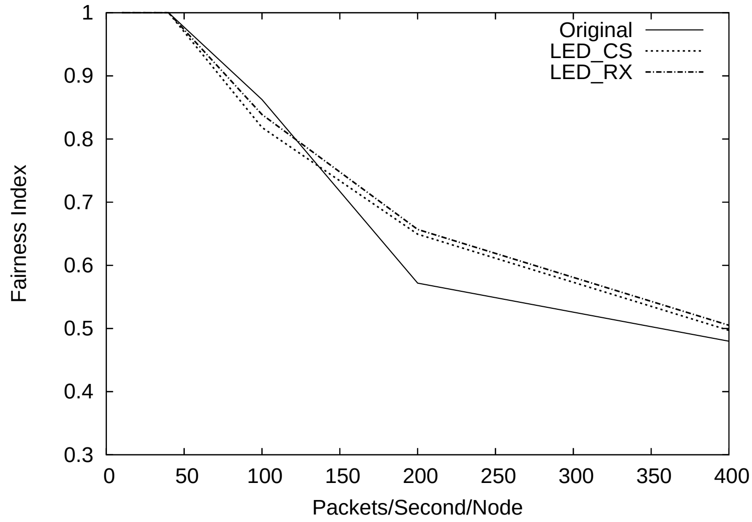

Figure 5.23: Fairness index versus network load using basic access mode

takes advantage of its aggressive mechanism to squeeze in more transmissions.

The packet collisions for the different mechanisms are shown in Figure 5.19. MACAW mechanism has the highest number of packet collisions because of its high aggressiveness as described earlier. Comparing the aggressive LED_CS with the conservative LED_RX, the LED_CS mechanism experiences more packet collisions than the LED_RX mechanism. However, the aggressiveness of the LED_CS in networks with small number nodes is justified by the significant large number of successful transmissions in comparison to the number of collisions. Therefore, the LED_CS mechanism has higher total throughput than the LED_RX mechanism as shown in Figure 5.17.

Figure 5.20 shows the fairness index of all the mechanisms under different packet loads. The LED_CS, LED_RX, and MACAW mechanisms have similar fairness index measurements that are higher than the Original mechanism. An explanation for this is that these mechanisms reduce the "exposed node" problem in the Original mechanism

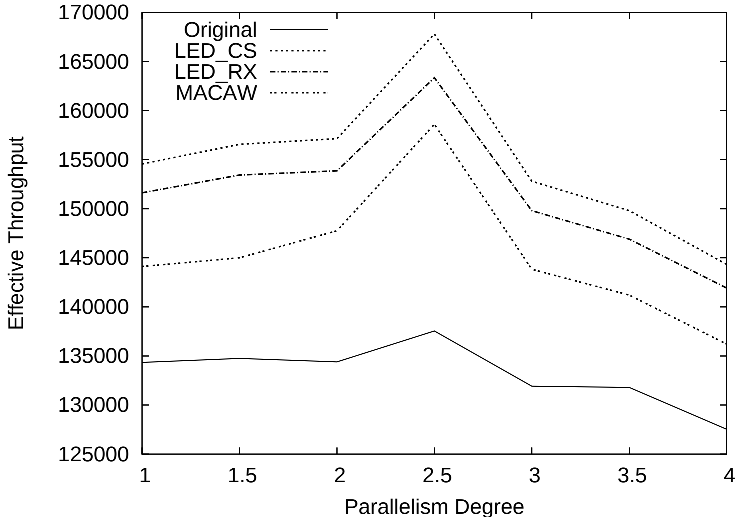

Figure 5.24: Effective throughput versus network degree using RTS/CTS access mode

which is one of the major sources for the unfairness.

Basic access mode shows similar performance to the RTS/CTS mode when we experimented it using different network packet loads. Figures 5.21 and 5.22 show the effective throughput and the relative enhancements of each mechanism over the Original respectively. Similarly, Figure 5.23 shows the fairness index of all the mechanisms. Note that MACAW protocol cannot be applied in the basic access mode.

5.4.4 Impact of Network Degree

We experiment with the network degree to study their effect on the protocol performance. We measure the network degree by the average number of ongoing and outgoing links per node. For example, when the parallelism degree is 1, it means that each node has one link either outgoing (sender) or ingoing (receiver). We use 50 connection pairs in a network of 100 nodes as the basic configuration with parallelism degree of 1. For higher

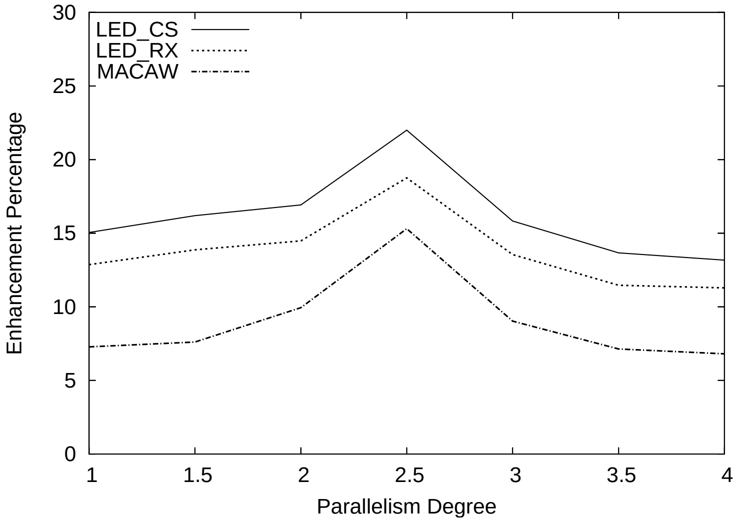

Figure 5.25: Throughput enhancement over Original protocol versus network degree using RTS/CTS access mode

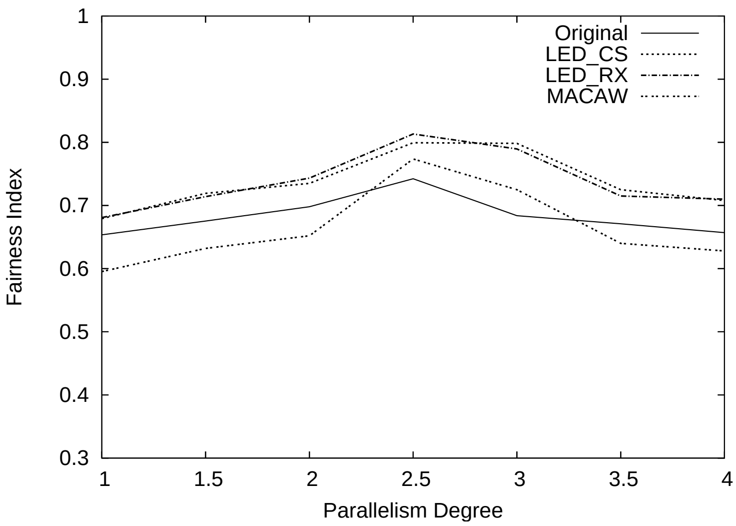

Figure 5.26: Fairness index versus network degree using RTS/CTS access mode

parallelism degree, we add additional connections to the original connections. To add a new connection, a node is selected randomly as the sender side of the connection while the receiver side node is selected randomly from the neighbor node set of the sender node. In this experiment, we fix the packet transmission rate on each connection to 150 packets per second. Figures 5.24 and 5.25 show the effective throughput and the relative enhancements of each mechanism over the Original respectively. As shown, LED_CS has the highest throughput over LED_RX and MACAW. LED_RX performs not as well as LED_CS since it is a conservative mechanism and with small number of nodes as in our experiment (100 nodes), a node will block long period while it can transmit within such period with no interference with other transmissions. This is opposite to LED_CS that takes an advantage of its aggressive mechanism and avoid such blocking periods. Figure 5.26 shows the fairness index of all the mechanisms. LED_CS and LED_RX protocols have similar fairness index measurements, which are higher than the Original and MACAW protocols since both LED_CS and LED_RX try to resolve the exposed node problem.

5.4.5 Capture Factor β

As pointed out earlier, it may occur that several nodes simultaneously predict that their own transmissions will not cause interference to the ongoing delivery and hence start their own transmissions. In this event, the aggregated energy from all these side transmissions may change the result of capture effect and cause interference with the ongoing delivery. To further study this problem, we multiply the capture ratio α used in Equation 2.2

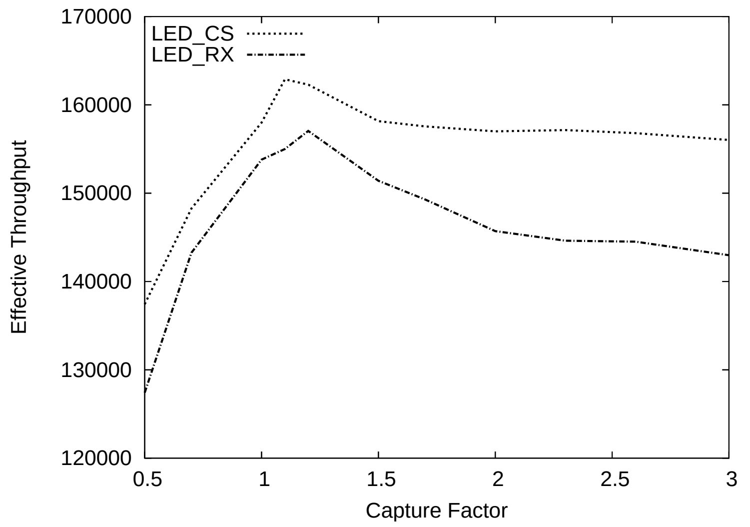

Figure 5.27: Effective throughput versus capture factor (β) using RTS/CTS access mode

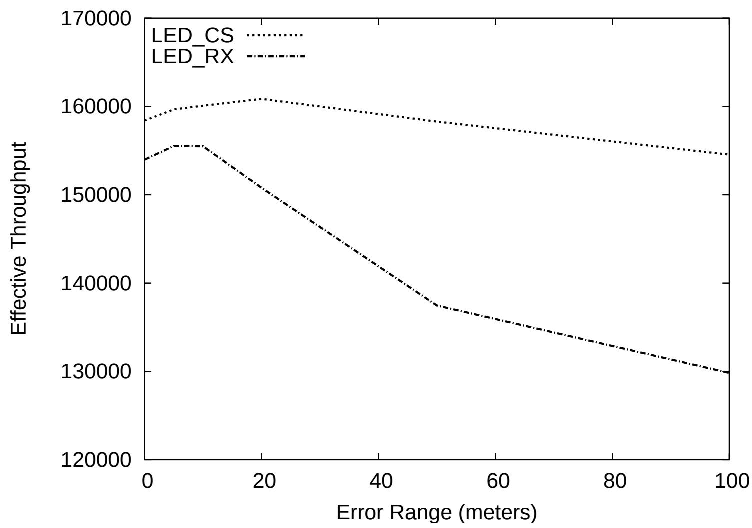

Figure 5.28: Effective throughput versus error range using RTS/CTS access mode

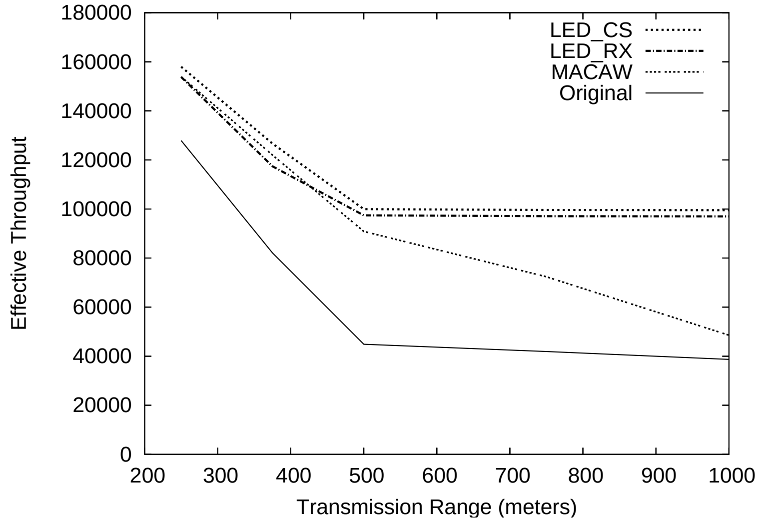

Figure 5.29: Effective throughput versus transmission range using RTS/CTS access mode

by capture factor β. By increasing β value over 1, we decrease the chance that the aggregated energy from all these side transmissions would interfere with the ongoing transmission. At the same time, increasing β has the same effect of increasing the capture ratio in reducing the network throughput. Figure 5.27 shows the LED_CS and LED_RX performance over different values of β for 50 connections with CBR traffic of 100 packets per second.

Setting β to values less than 1 degrades the performance of both mechanisms since there are more chances for channel competing nodes to decide to transmit and result in frame collision at receiver. As β increases over 1, the throughput increases since we reduce the number of interferences caused by the aggregated signals. However, increasing β to large values has a negative effect on the throughput since it under-utilizes the capture mechanism. What is more interesting is that for our experiment configurations, using $\beta = 1.2$ results in the optimal performance.

Transmission Power	*Transmission Range (R)*	*Carrier Sense Range (C)*
0.282W	250m	550m
1.427W	375m	825m
4.510W	500m	1100m
22.829W	750m	1650m
72.151W	1000m	2200m

Table 5.1: Different transmission powers and their corresponding ranges used by ns-2.

5.4.6 Impact of Errors in Node Locations

Next, we study the effect of errors in node locations due to the inaccuracy of the location estimation systems. We again experiment with network configuration of 50 connections with CBR traffic of 100 packets per second. Each node adds an error, selected randomly from the range $[-Err, Err]$, to the X and Y position of the node. We test using different values of Err as shown in Figure 5.28. Surprisingly, the effective throughput increases with small values of Err. This could be explained as using small random errors emulates the effect of using the capture factor β as described earlier in reducing the interference possibility. However, just like β, with high errors the performance of the LED mechanisms degrades. The performance degradation of the LED_RX is higher than that of the LED_CS since the LED_RX effectively depends on the location information only in deciding of the blocking status while LED_CS depends on the signal energy in addition to the location information.

5.4.7 Impact of Transmission and Carrier Sense Ranges

All the mechanisms under consideration are based on the transmission and the carrier sense ranges in the network. To examine the performance of those mechanisms under different ranges, we fix the maximum distance for a connection to be within 250m while changing the node transmission power. Table 5.1 shows the used transmission powers and their corresponding transmission and carrier sense ranges used in our ns-2 experiments using the propagations channel model defined by Equation 2.1. Figure 5.29 shows the effective throughput of the network versus the transmission ranges for network configuration of 50 connections with CBR of 100 packets per second. Although performance of the LED mechanism depends on the transmission range and node locations, the effective throughput of LED_CS decreases as the transmission range increases. This is due to: 1) with large ranges, more nodes hear the transmission and have to block during the RTS/CTS exchange, and 2) as the transmission range increases, many of the unblocked nodes which were not able to decode the transmission frames before become able to decode those frames now and may find that they have to block during those transmissions. On the other hand, increasing the number of decoded frames in LED_RX mechanism results in many unblocked nodes that formerly would block unnecessarily because of their inability to decode frames. However, increasing the transmission power still reduces the LED_RX throughput as shown in the figures because of: 1) similarly, using large transmission ranges force more nodes to hear the transmission and to block during the RTS/CTS exchange, and 2) as the transmission power increases, the carrier sense range increase and additional nodes become able to hear the transmission but unable to decrypt

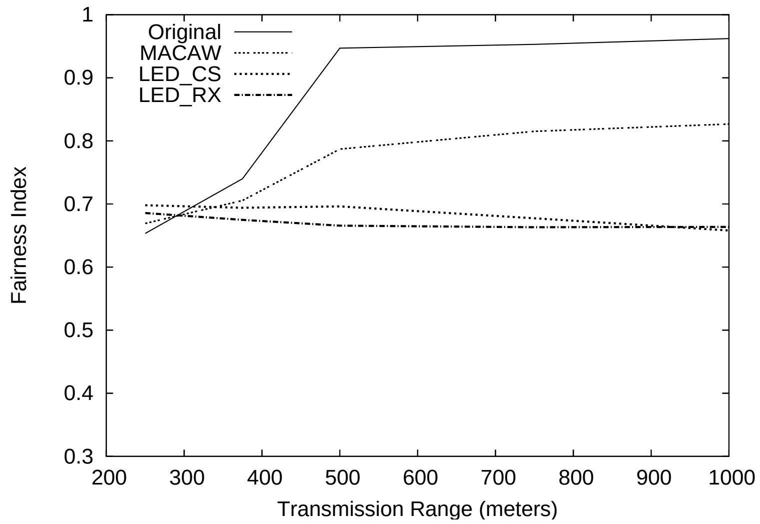

Figure 5.30: Fairness index versus transmission range using RTS/CTS access mode

it and hence force the nodes to block. As the transmission range increases, the area where the nodes are unable to decode the frames becomes smaller since we conduct experiments within a fixed square region and hence the performance of LED_RX becomes similar to the LED_CS performance. On the other hand, the performance of Original and MACAW keep degrading as the transmission range increases because now a single RTS/CTS frame exchange will block more nodes. For Original, more nodes will also be blocked because they sense the carrier as busy. As shown in the figure, when the transmission range is large, the performance of LED mechanisms is superior to the Original and MACAW mechanisms.

Figure 5.30 shows the effect of transmission ranges on fairness index. LED mechanisms experience fixed fairness index over the different transmission ranges while both Original and MACAW mechanisms have increase in their fairness index as the transmission range increases since the hidden and exposed node problems are reduced. Similar

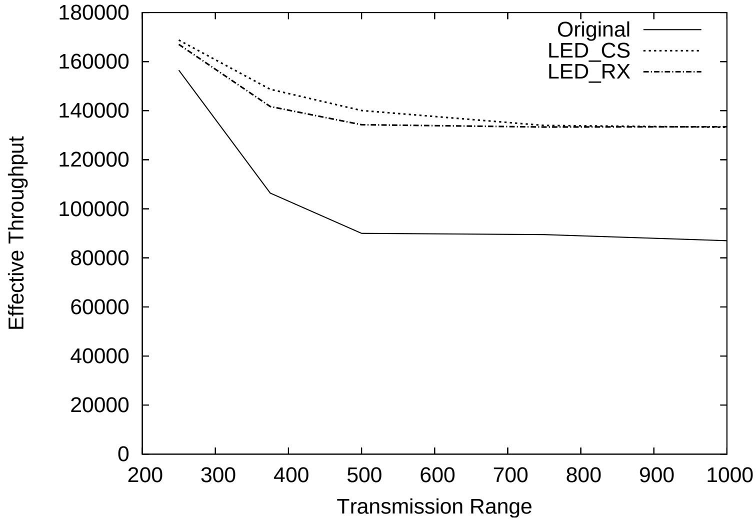

Figure 5.31: Effective throughput versus transmission range using basic access mode

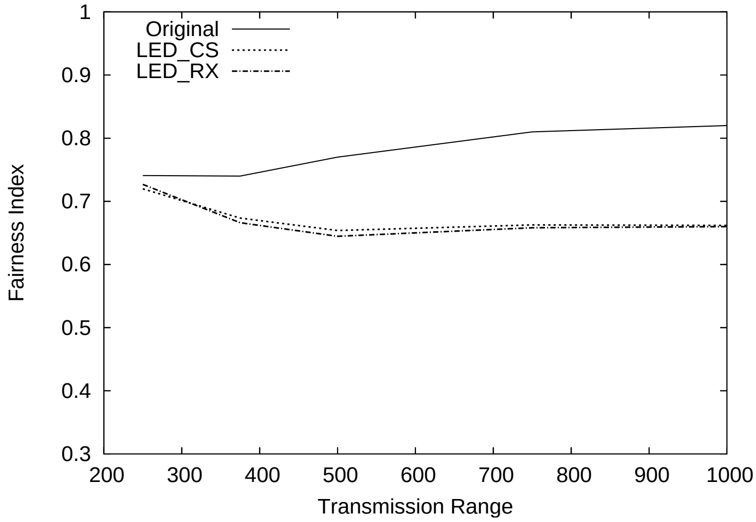

Figure 5.32: Fairness index versus transmission range using basic access mode

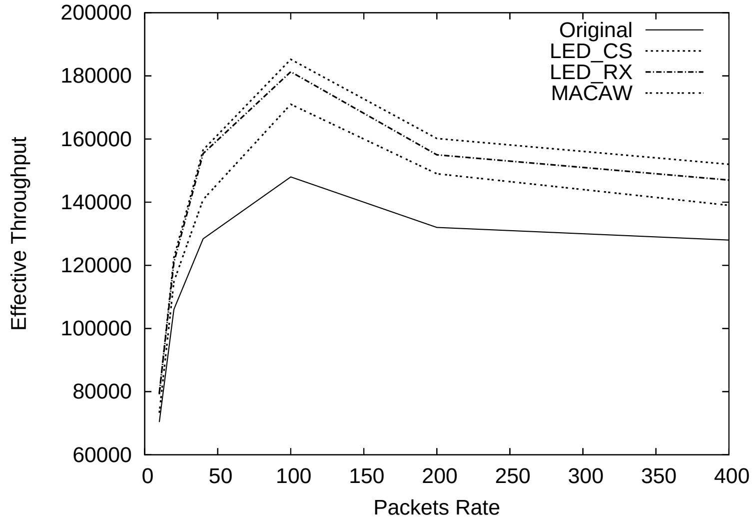

Figure 5.33: Effective throughput of infrastructure configuration versus packet rate using RTS/CTS access mode

results has been shown by the basic access mode with different transmission ranges. Figure 5.31 shows the effective throughput of the network while Figure 5.32 shows the fairness index for the basic access mode with different transmission ranges for network configuration of 50 connections with CBR of 100 packets per second.

5.4.8 Experimenting with Infrastructure Networks

Here we present the result for the 802.11 infrastructure network configurations. In this configuration, we placed 10 access points (APs) randomly in the $1000m \times 1000m$ area in which each AP has 20 clients placed randomly within the transmission range. For each AP, half of its clients are transmitting flows to the AP while the other half are receiving flows from the AP. Bi-direction flows are established for any two APs in the transmission range of each other. Note that all the APs and the clients have identical transmission and interference ranges in addition to use the same data packet transmission rate varying

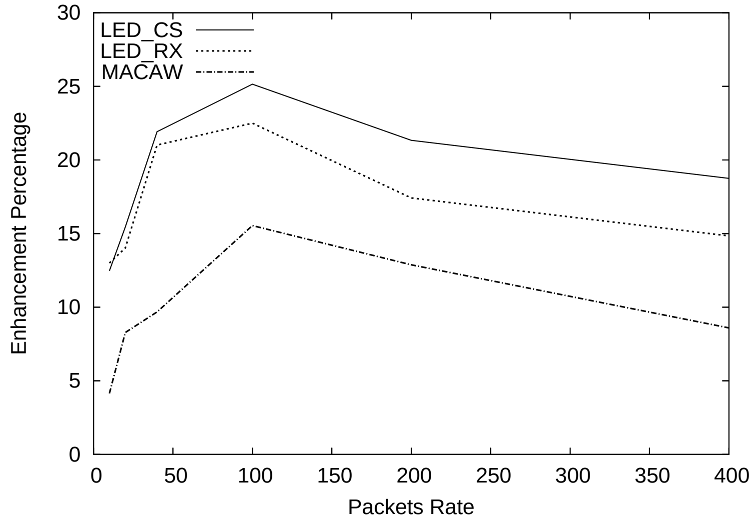

Figure 5.34: Throughput enhancement over Original protocol of infrastructure configuration versus packet rate using RTS/CTS access mode

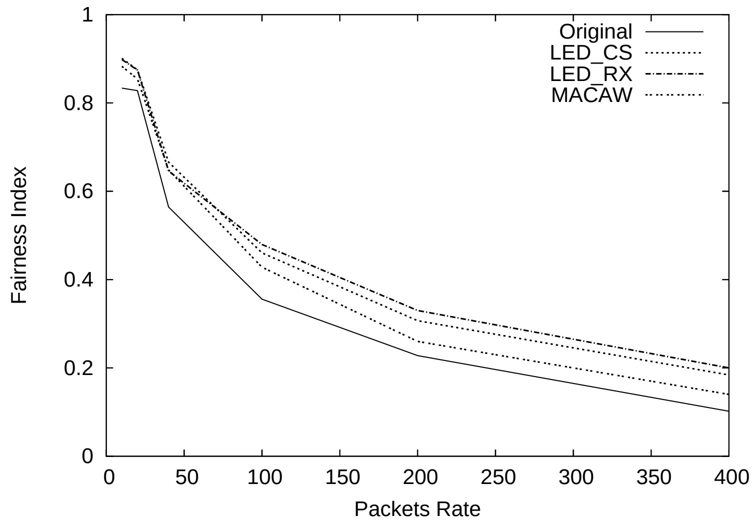

Figure 5.35: Fairness index of infrastructure configuration versus packet rate using RTS/CTS access mode

from 10 packets per second to 400 packets per second. Figures 5.33 and 5.34 show the effective throughput and the relative enhancements of each mechanism over the Original respectively. As expected, LED_CS has the highest throughput over LED_RX and MACAW. The low performance of the LED_RX in comparison with LED_CS could be traced to its conservative nature as explained above in the parallelism degree experiments. Figure 5.35 shows the fairness index of all the mechanisms. Similarly, LED_CS and LED_RX protocols have similar fairness index measurements, which are higher than the Original and MACAW.

5.5 Conclusion

In this chapter, we have introduced an enhancement of the IEEE 802.11 DCF. This enhancement, known as the Location Enhanced DCF, includes communication parameters especially the locations of transmitters and receivers in each frame. These parameters may assist nodes to better assess the channel availability. We have shown that the 802.11 DCF is conservative in terms of collision estimation, with as much as 35% of unnecessary blocking assessments. On the other hand, our LED may improve throughput as much as 22% over DCF with better fairness at the same time as shown in simulations.

Chapter 6

Opportunistic Mechanisms for IEEE 802.11 Networks using Directional Antennas I: Opportunistic Carrier Sense Transmission

Directional antennas have been introduced to improve the performance of IEEE 802.11 based wireless networks [66, 108, 137, 118, 27]. A station equipped with directional antennas can beamform data in a specific direction with a gain larger than that of omni-directional antenna. The transmitter beamforms the data in the direction of the receiver with diminished interference in the remaining directions. Thus, the network capacity is increased as a consequence of the spatial spectrum reuse.

IEEE 802.11 [5], and carrier sensing protocols in general, was developed with omni-directional antennas in mind. It assumes that all the packets (RTS/CTS/DATA/ACK packets) are transmitted as omni-directional signals that are received by all nearby nodes.

Deploying IEEE 802.11 in a directional antennas environment does not fully exploit the directional antennas characteristics. The main reason is that IEEE 802.11 stations are *conservative* in blocking their own transmissions in favor of the ongoing transmissions, although their transmissions will not result in interferences with other transmissions. Thus, many modifications (e.g., [119, 27, 39, 36]) were introduced to allow IEEE 802.11 based protocols to exploit the intrinsic features of directional antennas to increase throughput.

In this chapter and the next chapter, we propose two novel *opportunistic* enhancements to IEEE 802.11 to increase the number of simultaneous data transmissions, and thus, improve the overall wireless network throughput. The term *opportunistic* refers to mechanisms that exploit the directional antennas characteristics by taking immediate advantage of any circumstances of possible benefit.

The first enhancement, described in this chapter, is to augment the MAC protocol with additional information (location of the nodes) that gives a node the flexibility to transmit data while there are ongoing transmissions in its vicinity. To achieve this, we developed a protocol, called OPP_{CS}, that can determine more flexibly, based on the locations of transmitters and receivers of the ongoing transmissions, whether to transmit data or not. The second enhancement, described in the next chapter, is to change the access routines of the MAC data queue.

The rest of this chapter is organized as follows. Section 6.1 describes briefly our antenna model and the related work. Section 6.2 discusses the problem under consideration. Section 6.3 analyzes the blocking probabilities using the opportunistic MAC schemes to show potential performance improvement. Section 6.4 describes the implementations of OPP_{CS} scheme. Section 6.5 illustrates our performance analysis of the scheme. Conclusion is given in Section 6.6.

6.1 Related Works

The goal of directional antennas is to increase the capacity of wireless ad hoc networks since it allows independent communications between nodes to occur in parallel, even if the nodes are within range of each other. However, mutual interference by simultaneous transmissions limits the maximum number of such concurrent communications, and poses bounds on the amount of capacity gain.

Previous works address the capacity of wireless networks using directional antennas such as [117, 137]. Bhagwat et al., in [117], calculate upper bounds for the capacity gains of using directional antennas. The calculations of the interference based capacity bounds are given for a generic antenna model as well as a real-world antenna model. On the other hand, authors in [137] focuse on discovering the lower bounds of capacity improvement that directional antennas can provide relative to the traditional omni-directional antennas.

Different RTS/CTS handshake mechanisms with their corresponding analysis for directional antennas are addressed in several works [66, 119, 91, 39, 118, 131] to allow simultaneous transmissions that are disallowed when using only omni-directional antennas. In D-MAC [66], two schemes are proposed: 1) DRTS scheme that utilizes a directional antennas by sending the RTS packets in a particular direction (DRTS), whereas CTS packets are transmitted in all directions (OCTS), and 2) DRTS/ORTS scheme where a node may send omni-directional RTS (ORTS) if none of its directional antennas is blocked or DRTS provided that the desired directional antenna is not blocked. Other have studied the effect of using different combination of omni/directional transmissions for one or both of RTS/CTS frames [119, 39, 131, 108, 112, 91, 118].

All the above mechanisms follow the CSMA mechanism in forcing a node sensing a busy carrier to postpone its transmission although it may not affect the ongoing transmission. DBTMA/DA [57] addresses this problem by avoiding the carrier sense mechanism through splitting a single channel into two sub-channels and used directional busy-tones to accomplish the virtual sensing instead of the physical carrier sense. Using directional transmitting busy tones, it shares the similar feature of the directional RTS frame schemes in that it reserves the network capacity in a finer grain and thus relieves the exposed terminal problem. In the meantime, by using directional receiving busy tones, it realizes a similar functionality of blocking the corresponding antenna element in the direction from which omni-directional CTS frame is received. However, this mechanism requires the use of two separate sub-channels that does not follow the IEEE 802.11 standards.

Recently, there are several works on opportunistic scheduling for exploiting multiuser diversity gains [14, 74, 75, 60, 111]. Multiuser diversity refers to a type of diversity present across different users in a fading environment. This diversity can be exploited by scheduling transmissions so that users transmit when their channel conditions are favorable. For example, Bhagwat et al., in [117], propose the Channel State Dependent Packet Scheduling (CSDPS) in [14]. The basic idea of CSDPS is that, when a wireless link experiences burst errors, it defers transmission of packets on this link and transmits those on other links. Medium Access Diversity (MAD) scheme [60] leverages the benefits of rate adaptation schemes by aggressively exploiting multiuser diversity. Along with that, the Opportunistic Auto Rate (OAR) [111] transmits multiple packets (by treating them as fragments) when the channel condition permits higher data rates, thus achieves the high throughput. Liu and Knightly, in [75], provide a general formulation for the wireless

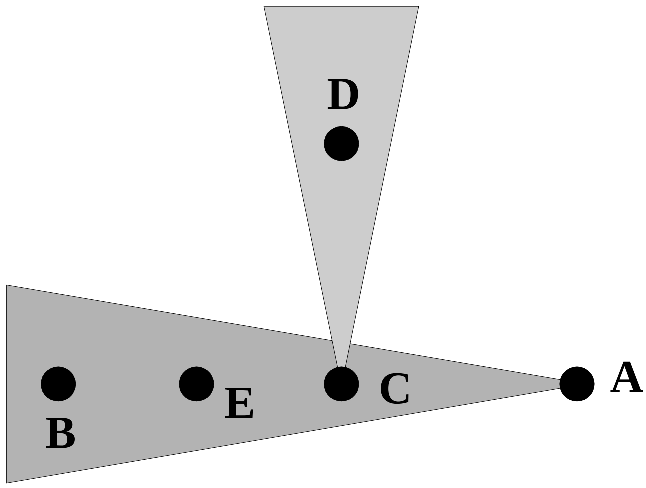

Figure 6.1: Opportunistic MAC example

opportunistic fairness scheduling over multiple channels.

Viewed in this light; our scheme OPP_{HOL}, which will be described later, can be interpreted as performing opportunistic beamforming where transmission is scheduled to the user which is available.

6.2 Problem Formulation

We propose a novel enhancement to IEEE 802.11 to decrease the number of unnecessary blocking. This increases the number of simultaneous data transmissions, and thus, improves the overall wireless network throughput.

The enhancement is to augment the MAC protocol with additional information (e.g., locations of the sender and the receiver) that gives a node the flexibility to transmit data in the presence of ongoing transmissions in its vicinity. In the original IEEE 802.11 protocol, a node blocks its transmission when it senses a busy carrier. However, under certain circumstances, this blocking seems unnecessarily, because the direction of transmission does not interfere with the ongoing transmissions. The node, using the locations of transmitters and receivers, can determine whether its transmission will interfere with these ongoing transmissions. We assume that each node is capable of acquiring its own location, for exmaple, by GPS [37], or by other RF based localization methods [10, 68].

For example, node A is engaged in a transmission by beamforming data in the direction of node B as in figure 6.1. Node C wants to beamform data to node D, but this transmission is blocked because of the ongoing transmission between A and B. Since the C-D transmission direction would not interfere with A-B transmission, node C should not block.

To achieve this, we developed a scheme, called OPP_{CS} scheme where a node could determine more flexibly, based on directional sensing and locations of the nodes, whether to block its transmission or not. Network wide, more concurrent transmissions are permitted by OPP_{CS} and the overall network throughput can be improved. We calculate analytically the potential gain of transmitting while sensing signals in the neighborhood and then prove this gain via simulation studies. Finally, we study the performance of OPP_{CS}.

In the remaining of the chapter, we use the terms “sector” and “direction”, and “sender” and “transmitter” interchangeably.

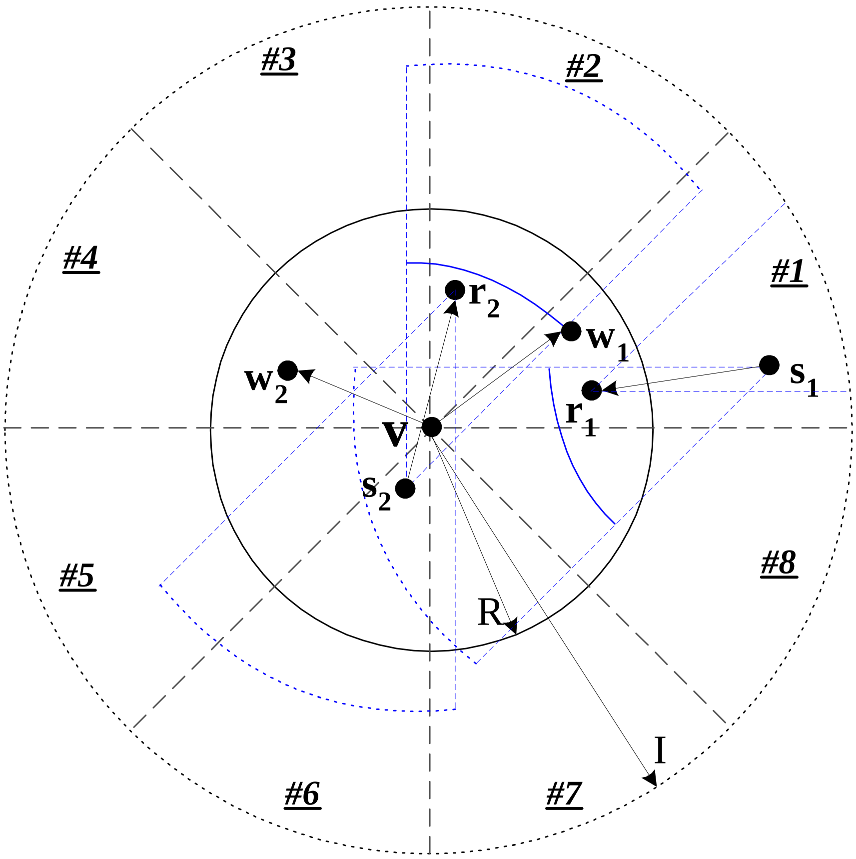

Figure 6.2: Blocking analysis where R is the transmission range and C is the carrier sense range

6.3 Analysis of Blocking Probabilities with OPP_{CS}

In this section, we derive the probability that a node has an opportunity to transmit directionally despite the presence of transmissions in its vicinity. This probability shows the potential gain for using OPP_{CS} scheme. Next, we verify the analytical results against the simulation results, and show the potential improvements of the original DCF in terms of MAC opportunistic transmissions.

6.3.1 Model Assumption

Although we adopt the steering-beam model in the implementation in section 6.4, and in the simulations in section 6.5, the analytical model depends on the switched-beam model for the sake of analytical simplicity. In this model, the space of each station is divided into n sectors (figure 6.2 shows a node with 8 sectors).

To model the directional transmission of each sector, we adopt the free space propagation channel model [105]; a model in which many channels, especially outdoor channels, have been found to fit in practice. For the sake of simplicity, we assume no energy leakage from sector sides, and no back lobes.

We have two sets of nodes: one for transmitters, and another for receivers. Each connection has a distinct pair of nodes, that is, each transmitter establishes a connection with a distinct receiver. We assume that transmitter nodes, and consequently connections, are uniformly distributed over an area with a density of δ. Each node has a transmission range R within which frames sent by the node can be received and decoded, and a carrier sense range C along the directional transmission, which is the range within which transmissions of the node can be detected (channel busy).

All nodes have the same traffic model, and all data packets are of the same length. Each packet requires transmission time τ, and is randomly destined to a 1-hop neighbor. The neighbors of a node are distributed over m sectors of the n possible sectors. One data packet is generated at a randomly selected time within every time interval T, where $T \gg \tau$. All transmitters use the same transmission power.

6.3.2 Analysis of OPP_{CS} Probability

Sometimes, a node *unnecessarily* blocks its transmission, because either its physical or virtual carrier sense indicates a busy channel. We say *unnecessarily* because, despite sensing a busy carrier, a node can still transmit without interfering with any of the ongoing transmissions.

Consider a scenario (see figure 6.2), where node v establishes a connection with node $w2$ on sector #4. The IEEE 802.11 standard forces node v to block its transmission once it senses (either physically or virtually) the ongoing transmission between station s_1 and station r_1, or between station s_2 and station r_2. However, the directional transmission from node v to node $w2$ would not affect any of those ongoing directional transmission, and thus node v should not block its transmission to $w2$. To avoid interfering with the ongoing transmissions of DATA and ACK packets, node v should block its transmission in a specific sector i (e.g., sector #4) only if: 1) a sender node s in sector i is transmitting, and node v is in the transmission cone of s (to avoid interfering with ACK), or 2) a node r in sector i is receiving, and node v is in the reception cone of r (to avoid interfering with DATA). In case of omni-reception, the condition for v being in the transmission or reception cone is not needed.

Assuming that a node v wants to transmit directionally to a sector i with an angular sector $\eta = \frac{2\pi}{n}$, define the following:

- $P(CS_{Tr})$ is the probability that, for all the connections that have their transmitters inside sector i and their corresponding receivers outside sector i, every single transmitter is either not transmitting, or transmitting and v is outside its transmission cone. This number of connections is equal to $\delta\frac{\eta}{2}C^2 - \frac{\delta}{n}\frac{\eta}{2}C^2$. This negative term is equal to number of connections that have both their transmitters and receivers in the sector i.

- $P(CS_{Rcv})$ is the probability that, for all the connections that have their transmitters outside sector i and their corresponding receivers inside sector i, every single receiver is either not receiving, or receiving and v is outside its reception cone. This number of connections is equal to $\delta\frac{\eta}{2}C^2 - \frac{\delta}{n}\frac{\eta}{2}C^2$.

- $P(CS_{TrRcv})$ is the probability that, for all the connections that have their transmitters and receivers inside sector i, every single transmitter is either (1) not transmitting (and, thus, the receiver is not receiving), or (2) transmitting and v is outside both the transmission and reception cones of the transmitter and the receiver respectively. This number of connections is equal to $\frac{\delta}{n}\frac{\eta}{2}C^2$.

- $P(CS_{Idle})$ is the probability that sector i is not blocked and, thus, station v is able to carry out a directional transmission through sector i. $P(CS_{Idle})$ equals the multiplication of $P(CS_{Tr})$, $P(CS_{Rcv})$ and $P(CS_{TrRcv})$.

$$
\begin{aligned}
P(CS_{Idle}) &= P(CS_{Tr}) \times P(CS_{Rcv}) \times P(CS_{TrRcv}) \\
&= [(1-\frac{\tau}{T}) + \frac{\tau}{T}\frac{2\pi-\eta}{2\pi}]^{(\delta-\frac{\delta}{n})\frac{\eta}{2}C^2} \\
&\quad \times[(1-\frac{\tau}{T}) + \frac{\tau}{T}\frac{2\pi-\eta}{2\pi}]^{(\delta-\frac{\delta}{n})\frac{\eta}{2}C^2} \\
&\quad \times[(1-\frac{\tau}{T}) + \frac{\tau}{T}\frac{2\pi-\eta}{2\pi}\frac{2\pi-\eta}{2\pi}]^{\frac{\delta}{n}\frac{\eta}{2}C^2} \\
&= [(1-\frac{\tau}{T}\frac{1}{n})^{\frac{\delta(n-1)}{n}\frac{\pi}{n}C^2}]^2 \\
&\quad \times[(1-\frac{\tau}{T}) + \frac{\tau}{T}(\frac{n-1}{n})^2]^{\frac{\delta}{n}\frac{\pi}{n}C^2} \qquad (6.1)
\end{aligned}
$$

In the IEEE 802.11 standard, a node v blocks its transmission to sector i if v is in transmission cone of a transmitter in any sector, or v is in the reception cone of a receiver in sector i.

- $P(Std_{Tr})$ is probability that, for all connections that have their receivers outside sector i, every single transmitter is either not transmitting, or transmitting and v is outside its transmission cone. This number of connections is equal to $\frac{\delta(n-1)}{n}\pi C^2$.
- $P(Std_{Rcv})$ is the probability that, for all connections that have their receivers inside sector i, every single transmitter is either not transmitting, or transmitting and v is outside both the transmission and reception cones of the connection. This number of connections is equal to $\delta\frac{\eta}{2}C^2$.
- $P(Std_{Idle})$ is the probability that sector i is not blocked, and equals to the multiplication of $P(Std_{Tr})$ and $P(Std_{Rcv})$.

$$\begin{aligned} P(Std_{Idle}) &= P(Std_{Tr}) \times P(Std_{Rcv}) \\ &= [(1 - \frac{\tau}{T}\frac{1}{n})^{\frac{\delta(n-1)}{n}\pi C^2}] \\ &\quad \times[(1 - \frac{\tau}{T}) + \frac{\tau}{T}(\frac{n-1}{n})^2]^{\delta \frac{\pi}{n} C^2} \end{aligned} \tag{6.2}$$

Therefore, $P(OPP_{CS})$, which is the probability that node v blocks unnecessarily, is given by:

$$P(OPP_{CS}) = P(CS_{Idle}) - P(Std_{Idle}) \tag{6.3}$$

6.3.3 Verification of OPP_{CS} Model

We verified this analytical model by generating random network topologies and traffic patterns, and then studying the blocking probabilities in each case. For constructing each random network, we place the node v at the center of an area of $1000m \times 1000m$. Transmitter nodes are distributed uniformly in this area. Each transmitter is paired with a corresponding receiver. The receiver is randomly located within a circular area of radius R that is centered at the transmitter. Each transmitter starts transmitting as follows. All packets require transmission time τ, and are generated randomly at a constant rate: one packet every time interval T, where $T \gg \tau$. The transmission beam width is set to $2\pi/n$ where n is the number of sectors of a node. When node v has a frame to send, it selects randomly a sector to transmit to. Then, v checks if it can transmit its frame according to both the original IEEE 802.11 and OPP_{CS} mechanisms. For the original IEEE 802.11 mechanism, the number of runs in which node v was able to transmit its frame is then divided over the total number of transmission attempts to derive $P(Std_{Idle})$. Similarly,

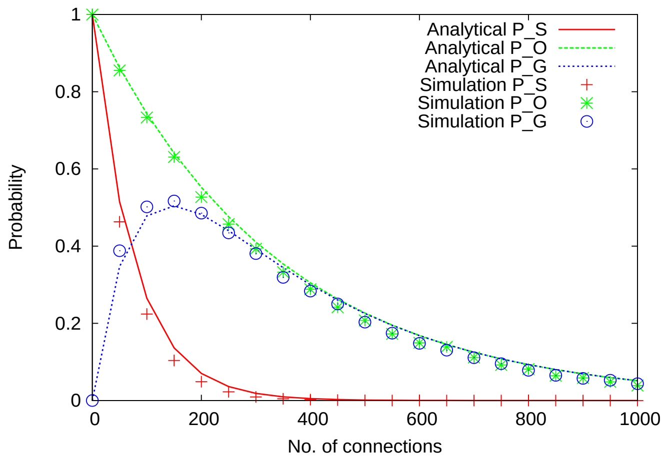

Figure 6.3: The analytical and simulation values of the probabilities P_S=$P(Std_{Idle})$, P_O=$P(CS_{Idle})$, and P_G=$P(OPP_{CS})$

we can determine $P(CS_{Idle})$. Finally, we compare $P(CS_{Idle})$ and $P(Std_{Idle})$, in addition to $P(OPP_{CS})$, to those calculated from the analytical result.

Figure 6.3 plots both the analytical and the simulated curves of $P(CS_{Idle})$, $P(Std_{Idle})$ and $P(OPP_{CS})$ for $R = 250m$, $C = 550m$, $n = 8$, $m = 4$, $\tau/T = 0.1$ and different numbers of nodes (thus varying the node density δ). Figure 6.3 shows that the simulation results closely match the analytical results which validates our analysis. It shows, also, that there is a room for improvement using OPP_{CS}.

Note that the calculated $P(OPP_{CS})$ is still conservative because we assume, for simplicity, that all nodes in the vicinity of v have the freedom of transmission. We do not take into account that some of these nodes have to block because of other ongoing transmissions in their vicinities. Accounting for these blocked nodes would increase $P(OPP_{CS})$. To analyze how our simplified assumptions affect our opportunistic probability estimation, we relaxed these assumptions in the simulation runs. Figure 6.4 plots the simulation of $P(OPP_{CS})$ with relaxing the simplification assumptions. This figure,

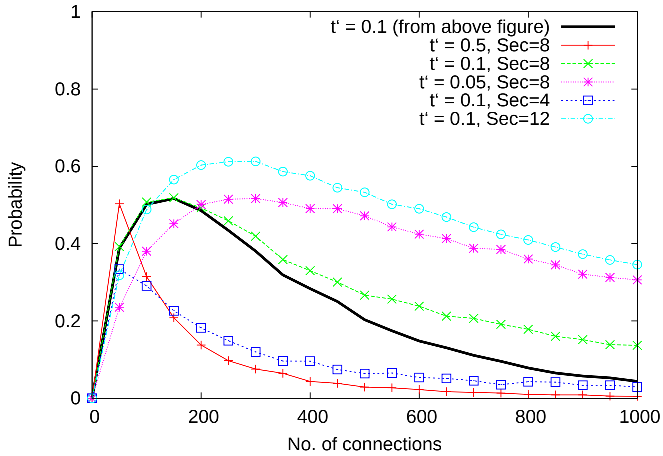

Figure 6.4: The probability $P(OPP_{CS})$ with different load values t' where $t' = \tau/T$ and different number of sectors n

also, plots $P(OPP_{CS})$ with different packet load values and different sector numbers to show how different parameters affect the $P(OPP_{CS})$. The $P(OPP_{CS})$ plot with conservative assumptions, which is directly copied from Figure 6.3, is also included for easy comparison.

These figures show that the unnecessary blocking probability of a node using the standard IEEE 802.11 DCF is large enough when using directional antennas (as high as 60%) and hence it motivates us to consider modifying the MAC layer to exploit the directional antennas. In the following section we will describe the newly proposed modification to the IEEE 802.11 DCF for OPP_{CS} mechanism.

6.4 Implementation of OPP_{CS}

In this section, we describe our opportunistic enhancement for IEEE 802.11. First, we describe the design of the needed physical layer. Next, we present the proposed modifi-

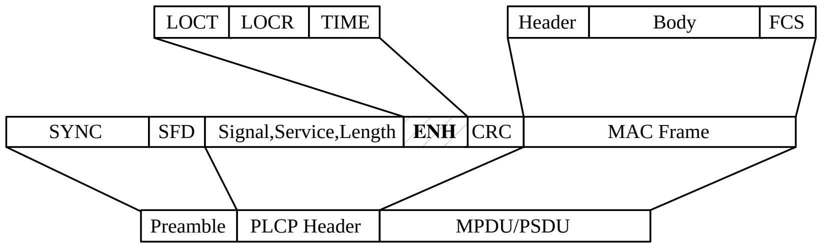

Figure 6.5: Frame structure

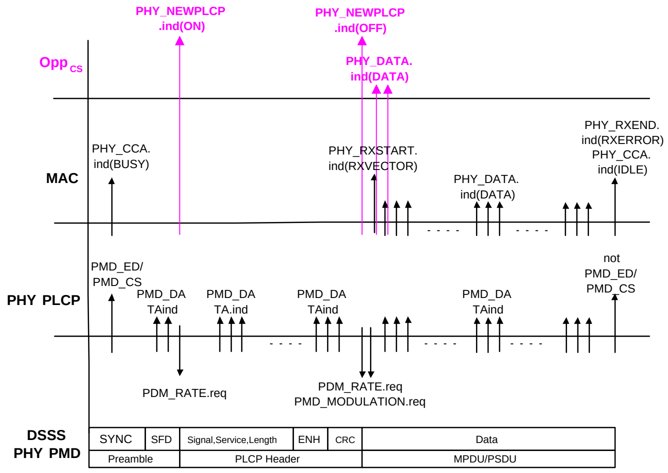

Figure 6.6: PHY-MAC interactions

cations to the IEEE 802.11 MAC with the details of proposed mechanisms.

6.4.1 Physical Layer Design

In our OPP_{CS}, a node is only concerned if its own transmission affects any ongoing transmission. Our models do not consider if the nodes own transmissions can be received correctly by the intended receivers, or even if they are able to reply back by CTS or ACK frame. This optimistic approach is largely for keeping the model simple at its current stage. The current IEEE 802.11 standard does not require a receiver PHY modem to be able to capture a new stronger frame after the receiver has been tuned to receive some other frame. This causes problems in our approach since this intended receiver will not receive and interpret the new frame correctly even if the signal is strong enough to allow this frame to be captured correctly. Therefore, as we did with LED in previous chapter, we assume the use of Lucent's PHY design with Message-In-A-Message (MIM) support [17] that supports the capture of a new frame after the receiver has already begun to receive another frame do exist.

6.4.2 MAC Layer Design

Our enhanced design for a DCF MAC stands atop a MIM-capable PHY. The new proposed mechanism OPP_{CS} is a part of the MAC layer function. In this subsection, we will describe the needed modifications in the the IEEE 802.11 MAC layer.

Figure 6.5 shows the frame format to support the enhanced functionalities of the new MAC. We insert a block of information called ENH (Enhanced). Similar to LED in Chapter 6.4, the ENH is inserted as part of the PLCP header instead of at the beginning of PLCP Service Data Unit (PSDU) due to the following reasons. First, the PLCP header has its own CRC field so the contents of the ENH block can immediately be verified and utilized. Second, all nodes within the service set can understand the ENH block since the PLCP header is transmitted at a base rate. Third, the receiver can decide faster whether it needs to block its own transmission, because it received the ENH block earlier than PSDU.

The ENH block consists of three fields. The LOCT and LOCR fields contain the locations of the frame transmitter and receiver respectively, and the TIME field specifies the total duration period for the delivery. When a source starts its unicast data delivery by sending out a RTS frame in case of RTS/CTS mechanism, or the DATA frame in case of basic mechanism, it fills the LOCT, LOCR and TIME fields with the corresponding parameter values, if known. If LOCR parameter is unknown at this time, it is set to NULL. Upon receiving this frame, the destination of the data delivery copies the LOCT field into the corresponding fields of its reply frame (CTS or ACK). It also fills or updates the TIME and LOCR fields with its own parameters. Note that TIME field is updated to reflect the remaining duration period of the delivery in a fashion similar to updating the DNAV time field. For any subsequent frames of the delivery, full location descriptions of both the source and the destination are included as well as the duration period of remaining delivery.

A node may maintain a parameter cache in order to store the location information of already known nodes. So when a node sends data to an arbitrary node, the cached parameters may be used in LOCR instead of NULL.

As described in the previous chapter, the PHY (PLCP in particular), in the standard IEEE 802.11, signals three events to the MAC layer during frame reception: carrier busy (PHY_CCA), begin receiving PSDU (PHY_RXSTART), and end receiving PSDU (PHY_RXEND). It does not deliver any data bits to the MAC layer until the PSDU reception has begun. Then the receiver proceeds until the end of the frame (unless interrupted by carrier loss in the middle of the reception). Received bits are passed to the MAC layer as they are decoded and assembled into the MAC frame. At the end of the PSDU, there is a forward error detection CRC block called Frame Check Sequence

(FCS). If the MAC frame passes the CRC check, it is accepted and passed up for further IEEE 802.11 MAC processing. If the CRC fails, the frame is dropped.

Similar to our LED approach in Chapter 5, in addition to the above interactions, the OPP_{CS} interact with the PLCP layer using an indicator, called PHY_NEWPLCP, as illustrated by Figure 6.6. The PLCP layer turns on the PHY_NEWPLCP indicators after it finishes receiving the Start Frame Delimiter (SFD) field of a frame's Preamble section, and turns it off after receiving the whole PLCP header.

Now, we will illustrate the OPP_{CS} algorithm. The original IEEE 802.11, once the PHY_CCA is triggered, the node blocks its transmission, and freezes its counting down counter till the end of the frame reception. In OPP_{CS} mechanism, the node reacts similarly until the PHY_NEWPLCP is turned off. That's when it starts the decision making process by calculating $((|\gamma - \alpha_i^s| > \frac{w}{2})$ and $(|\gamma - \alpha_i^d| > \frac{w}{2}))$. Variables α_i^s and α_i^d are the angle between itself and both the source and the destination of the ongoing data delivery, γ is the angle to the intended destination of its transmission, and w is the beam width.

If formula is false, the station should block its transmission, else the station should not block its own transmission. In the case that any of the parameters corresponding to the ENH fields is unknown, the assessing node assumes the worst, and blocks its own transmission similar to the carrier sense in the IEEE 802.11 standards.

If the node decides to block its own transmission, it remains in the receiving state and continues the receiving procedure as specified by the standard. It disables any transmission requests from upper layer, and updates its DNAV value in the direction of the transmitter and the receiver of this frame[1] based on the frame's Duration field, which is set to the time required for the full data delivery frame exchange sequence to finish. Unlike the required conditions to block a certain direction as described in section 6.3, a node updates its DNAV regardless of whether it is within the transmission/reception cone of the transmitting/receiving nodes of the ongoing transmission, for the sake of simplicity and to cope with the DNAV described in the literature [119, 27]. Since the intended receiver of the frame has to block during the transmission of the frame, it has to compare the LOCR field to its own location. If its location is within a certain range threshold, the node blocks during the reception of the frame. We choose this range to be 5 meters in our simulations.

If the node decides not to block, the receiver may continue, but the upper layer transmission requests are not disabled. DNAV is updated similar to the case when the station decides to block. If there is indeed any outgoing frame ready, the PHY modem can accept the request by switching to transmission state and starting the transmission. A PHY reset signal is needed in this case to force the PHY to leave the receiving state, and to enable PHY_TXSTART signal when the MAC has a frame to send.

If the OPP_{CS} decides not to block, the Clear Channel Assessment (CCA) indicator produced by the physical layer, needs to be temporarily ignored. The overriding of CCA in OPP_{CS} layer is accomplished by proposing a new vector called CCA-Suppression Vector (CSV), which is a suppression timer. CSV is set to the end of reception of the current frame, calculated based on the length field contained in the received PLCP header

[1]The directions of the transmitter and the receiver are calculated using the location information of those nodes extracted from the PLCP header.

of the frame.

In total, a OPP_{CS} node uses four indicators related to the transmission blocking estimation. The CCA indicator, which is the physical carrier indicator, is “TRUE” when the PHY layer detects carrier (or energy exceeding threshold, or both depending on equipment vendor implementation). The DNAV indicator, which is the virtual carrier indicator, is “TRUE” when there is a channel reservation, which corresponds to the desired transmission direction, that needs to be honored. That is, if this node transmits toward a desired direction, then the transmission will interfere with the ongoing delivery. The PHY_NEWPLCP indicator is “TRUE” while a PLCP header is being received. Finally, the CSV indicator tells the node whether it should ignore the physical layer CCA. It is “TRUE” when the suppression timer is running.

More precisely, the decision of whether this node should block its own transmission or not is made as follow:

if (PHY_NEWPLCP *or* ((CCA *and* (*not* CSV)) *or* DNAV)) *then* BLOCK

Another issue occurs if a channel-assessing node only detects carrier but cannot decode the frame. In this case, a node is not able to estimate whether its transmission will affect this ongoing data delivery. We use an aggressive approach, that is, a node will not block its own transmission in the event of “detecting a carrier but not being able to decode the frame”.

6.5 Performance Evaluation

In this section, we present extensive simulation-based studies on the performance of the opportunistic mechanism OPP_{CS}. The performance comparisons are done using the *ns-2* simulator, enhanced with the CMU-wireless extensions [2]. The underlying link layer is IEEE 802.11b with 11 Mbps data rate. We have modified the capture model in ns-2 to allow receivers to capture the stronger packet out of the weaker packet(s) if the stronger packet comes after the weaker to reflect the MIM PHY design as discussed in the previous section. As in LED, we adopt the capture ratio value of 5 in our simulations. This means that when a node is in the middle of receiving frame A and frame B arrives, one of the following will happen. If the received power of frame A, P_A, is more than 5 times of power of frame B P_B, the receiver continuously receives frame A. If P_B is more than 5 times of P_A, the receiver drops frame A and begins receiving frame B. In all other situations, packets collide and no frame is received correctly.

The IEEE 802.11 MAC layer and PHY layer in ns-2 were enhanced to support directional antennas model we described in this chapter. We also enhanced the IEEE 802.11 MAC layer by extending it with the implementation of OPP_{CS} mechanism.

Each of our simulated networks consists of a set of connections, which are constructed as pairs of stationary sender and receiver nodes. The senders and receivers are placed in a $1000m \times 1000m$ area. We assume that each sender has already cached the location of its corresponding receiver(s). We assume that the transmission ranges in omni and directional transmissions are identical. This could be accomplished by either increasing the transmission power at the sender in case of omni transmission, or

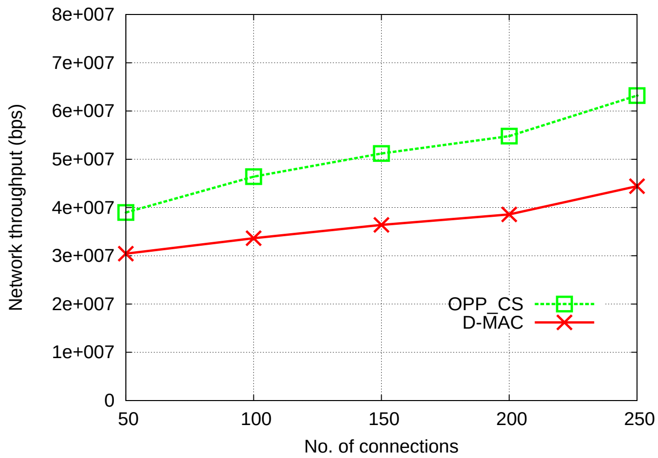

Figure 6.7: Network throughput versus number of connections

decreasing it in case of directional transmission. In simulation, each of the LOCT, LOCR, and TIME fields in the ENH header is of 32 bits.

In ns-2, we set the transmission radius R of a node to 250m and the carrier sense radius C to 550m. Each connection is a flow of UDP packets of size 1000 bytes transmitted at 11Mbps. Each simulation is run for a fixed duration of 250 seconds. Each point on the curves to be presented is an average of 10 simulation runs.

We have modeled various scenarios of different neighbor densities, workloads, beamwidths, and transmission and carrier sense ranges (transmission power levels). To study the performance of our suggested schemes, we compare OPP_{CS} with D-MAC [66] which is the extension of the original IEEE 802.11 DCF for the directional antenna. All mechanisms use the extended ns-2 capture model as described earlier.

During the simulation runs, we take the following measurements:

1. **Network Throughput:** This counts the total number of data bits received by all the receiver nodes per second.

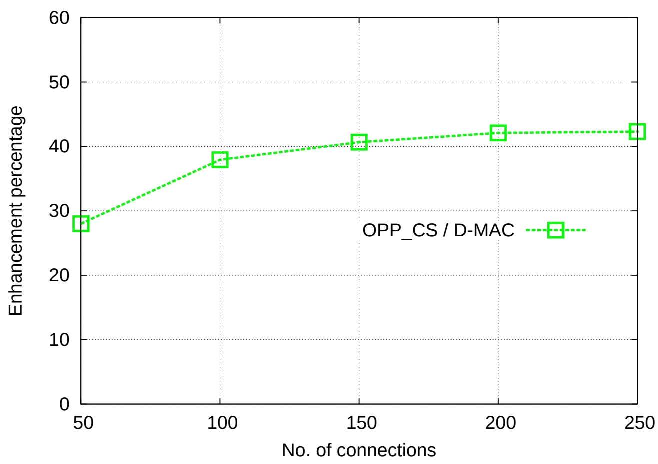

Figure 6.8: Throughput enhancement over D-MAC mechanism versus number of connections

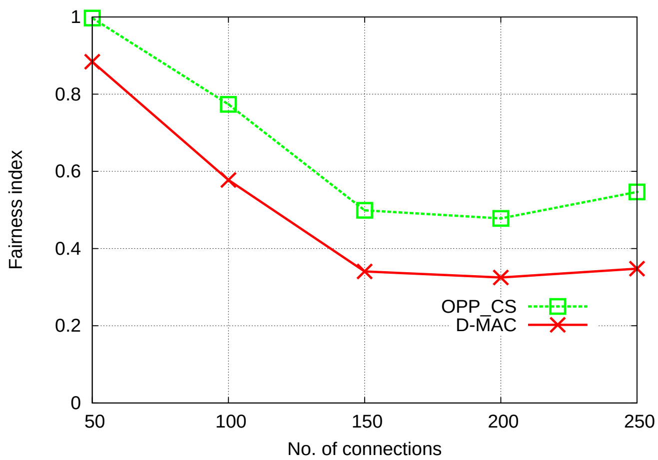

Figure 6.9: Fairness index for the network versus number of connections

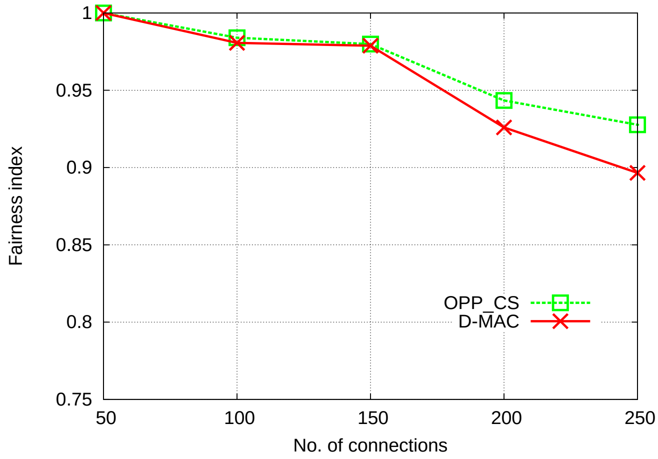

Figure 6.10: Fairness index for a node versus number of connections

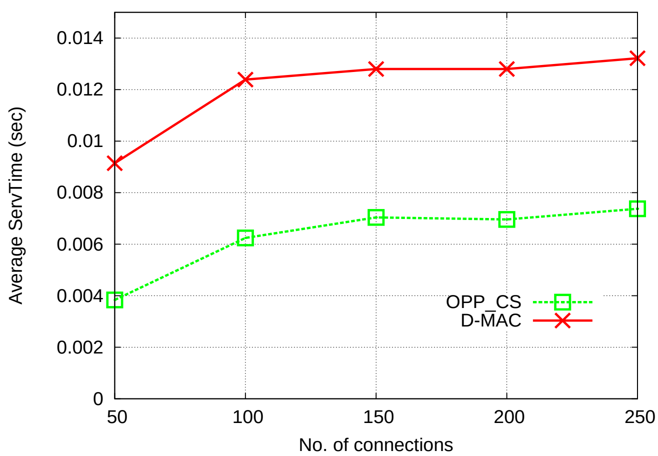

Figure 6.11: Average $ServTime$ versus number of connections

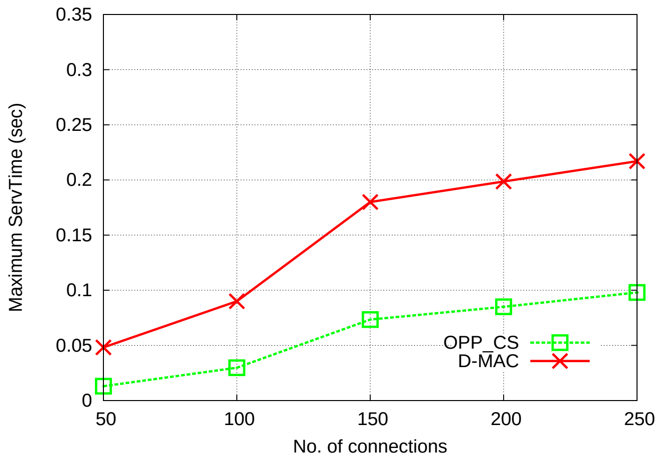

Figure 6.12: Maximum $ServTime$ versus number of connections

2. **Fairness index** measures under different mechanisms both: a) the bandwidth sharing of all the network connections, and b) the bandwidth sharing of node's connections averaged over all nodes in the network. We use Jain's fairness index [26, 59] which is defined as follows:

$$F = \frac{(\sum_{i=1}^{N} \gamma_i)^2}{N \sum_{i=1}^{N} \gamma_i^2} \tag{6.4}$$

where N is the number of connections and γ_i is the throughput of connection i.

3. **Service Time** measures the average value and the maximum value of $ServTime_i$, which is the service time needed to transmit successfully packet i, averaged over all packets transmitted successfully during the simulation period.

We have experimented both with and without RTS/CTS prior to data. One interesting observation regarding RTS/CTS is that forcing the nodes to be blocked during the whole RTS/CTS period of other deliveries will actually increase the network throughput. The reason is to increase chances for transmitting omni-directional RTS and CTS frames to let more nodes know about the ongoing transmissions and hence decrease the collision probabilities.

6.5.1 Impact of Network Degree

Network degree means the average number of connections that a node participates in as either a sender or a receiver. When the network degree is 1, each node participates in only one connection. As network degree increases, the number of connections a node is involved in increases too. Figure 6.7 shows the network throughput when the number of connections varies from 50 to 250 connections. This corresponds to a range of network degrees varies from 1 to 5, since we use 50 nodes for these scenarios. The data traffic between each pair of source and destination is a constant bit rate (CBR) UDP flow at a rate of 100 packets per second to overload the network and the beamwidth size is set to 30^0. As shown, the OPP_{CS} mechanism has higher data throughput than D-MAC mechanism. The enhancements of the mechanism over the original are shown in Figure 6.8 in terms of percentage throughput gain. As shown, OPP_{CS} could achieve about 42% more throughput than D-MAC. This enhancement is due to exploiting the directional antennas characteristics in increasing the spatial reuse of the medium by reducing the well known "exposed node" problem in D-MAC mechanism.

Figure 6.9 shows the network fairness index of different mechanisms. OPP_{CS} has higher fairness than D-MAC mechanism. An explanation for this is that these mechanisms reduce the "exposed node" problem in D-MAC mechanism which is one of the major sources for the unfairness. Figure 6.10 shows the fairness among the connections

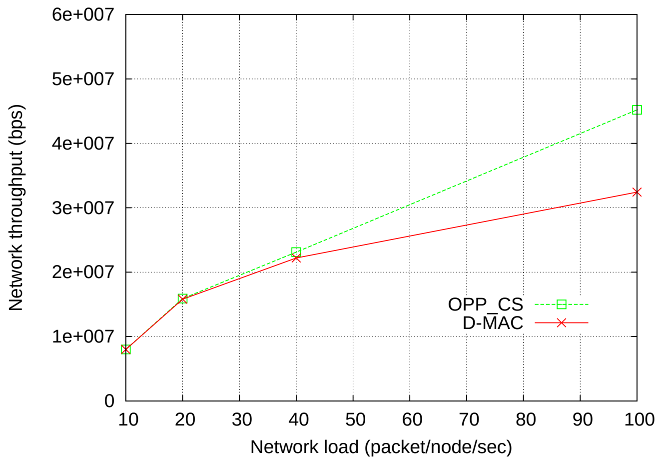

Figure 6.13: Network throughput versus network load

belonging to a node averaged over all nodes. OPP_{CS} has higher node fairness.

We also measure the average and maximum $ServTime$ for successfully transmitted packets under the different mechanisms and plotted them in Figures 6.11 and 6.12 respectively.

6.5.2 Impact of network load

We experiment with different network packet loads to see their effects on performance. We fix the number of connections in the network to 100, which make each node on average involved in two connections. We vary the packet generation rate at each source node between 10 and 100 packets per second. Figures 6.13 and 6.14 show the network throughput and the relative enhancement of OPP_{CS} mechanism over the D-MAC respectively. Similar to the previous results, OPP_{CS} outperform the original mechanism.

Figure 6.15 shows the network fairness index of different mechanisms whereas Figure 6.16 shows the fairness among the node connections where OPP_{CS} outperforms D-

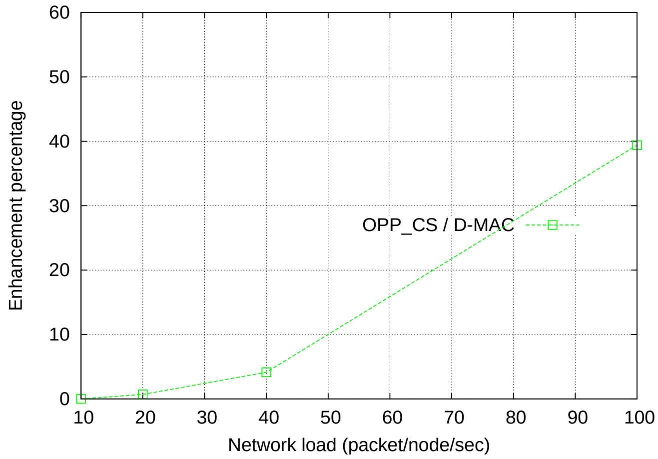

Figure 6.14: Throughput enhancement over D-MAC mechanism versus network load

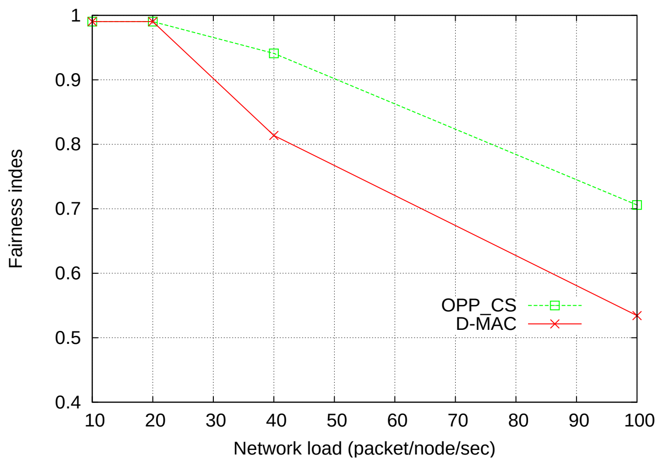

Figure 6.15: Fairness index for the network versus network load

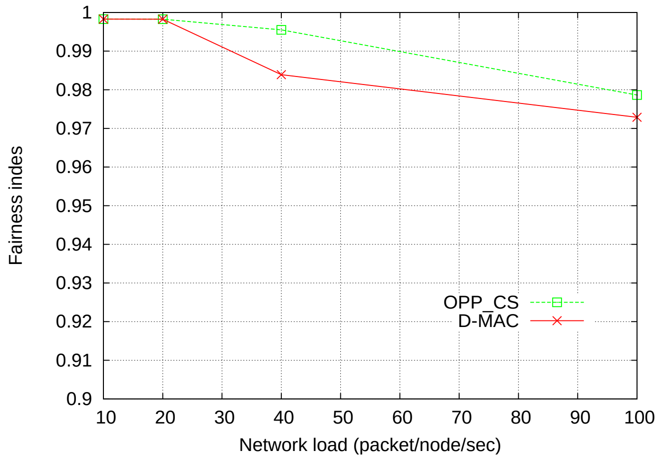

Figure 6.16: Fairness index for a node versus network load

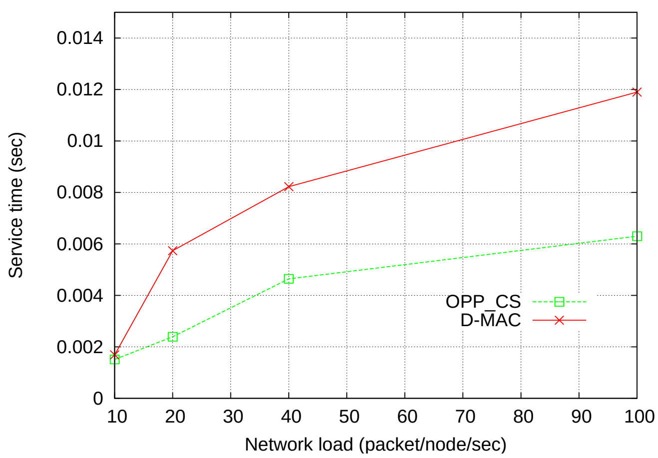

Figure 6.17: Average $ServTime$ versus network load

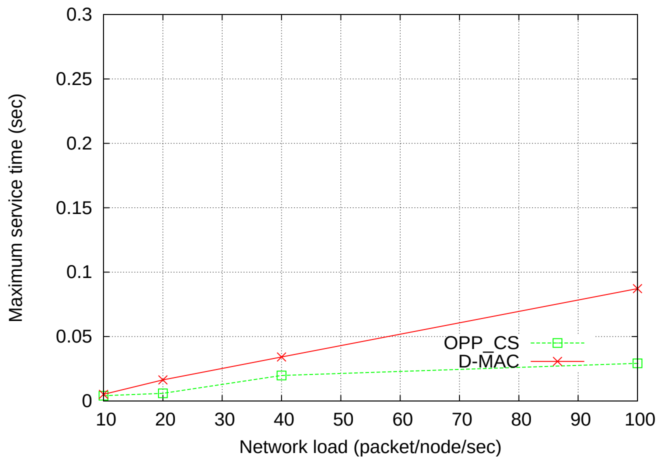

Figure 6.18: Maximum $ServTime$ versus network load

MAC for both. Figures 6.17 and 6.18 show the average and maximum packet $ServTime$ in which a similar pattern as previous are shown here.

6.5.3 Impact of Beamwidth Size

Next, we experiment with different beamwidth values to see their effects on performance. We fix the number of connections in the network to 100 (i.e. network degree is 2) and the rate of packet generation to 100 packets per second. We varied the beamwidth size from 30^0 to 120^0. Figures 6.19 and 6.20 show the network throughput and the relative enhancement of OPP_{CS} mechanism over D-MAC respectively.

Figures 6.21 shows the fairness among the node connections. Similar to previous results, OPP_{CS} outperforms D-MAC. Figure 6.22 shows the average $ServTime$ for the different mechanisms.

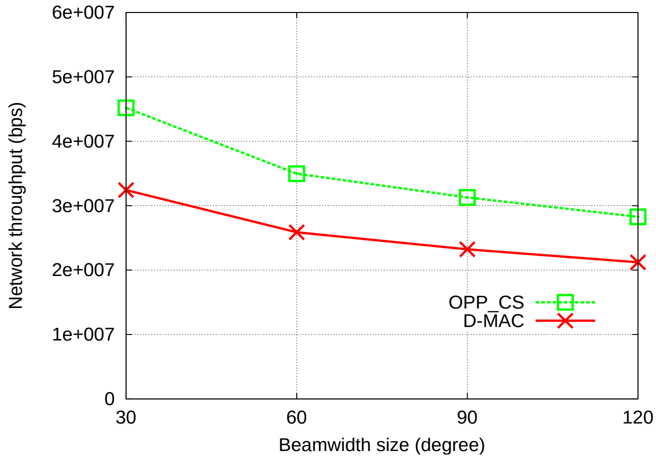

Figure 6.19: Network throughput versus beamwidth size

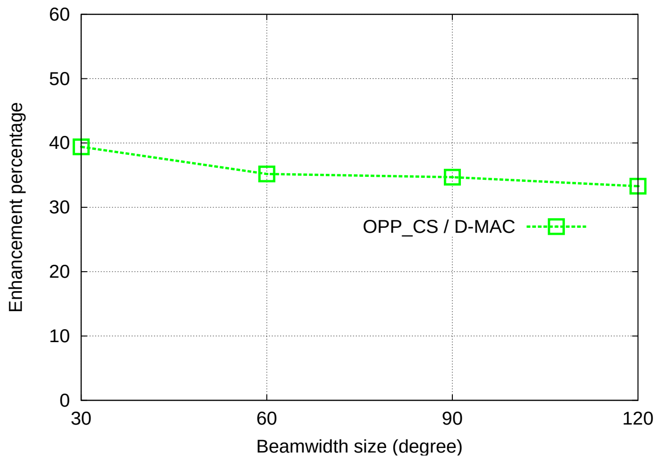

Figure 6.20: Throughput enhancement over D-MAC mechanism versus beamwidth size

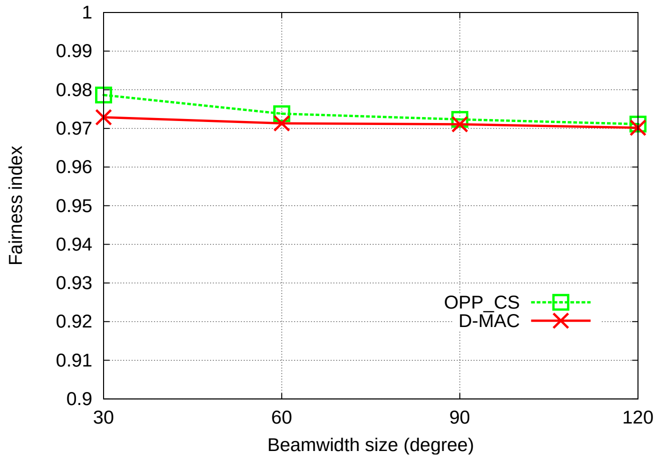

Figure 6.21: Fairness index for a node versus beamwidth size

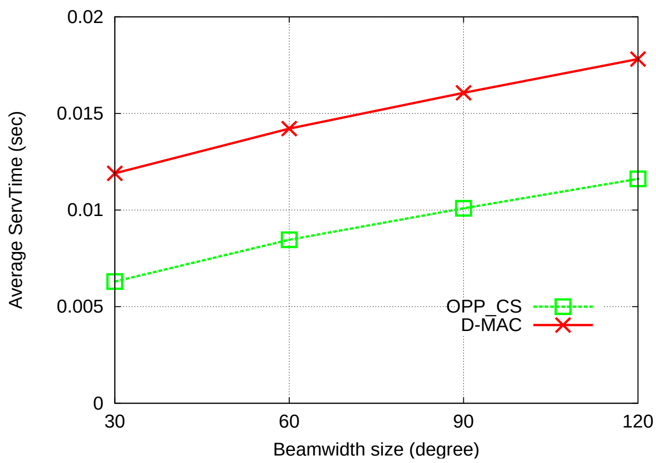

Figure 6.22: Average $ServTime$ versus number of connections

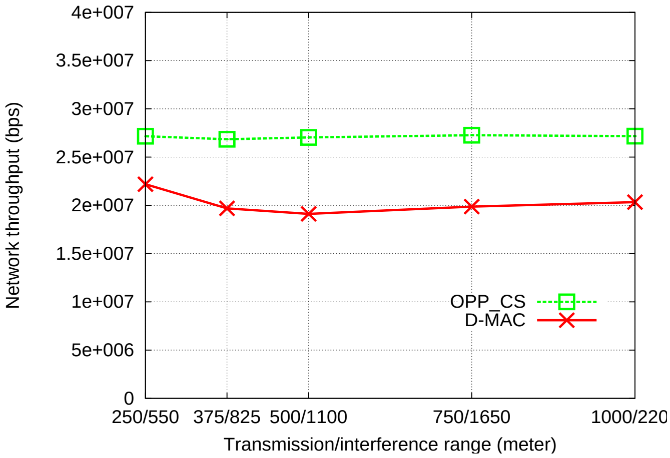

Figure 6.23: Network throughput versus transmission/carrier ranges

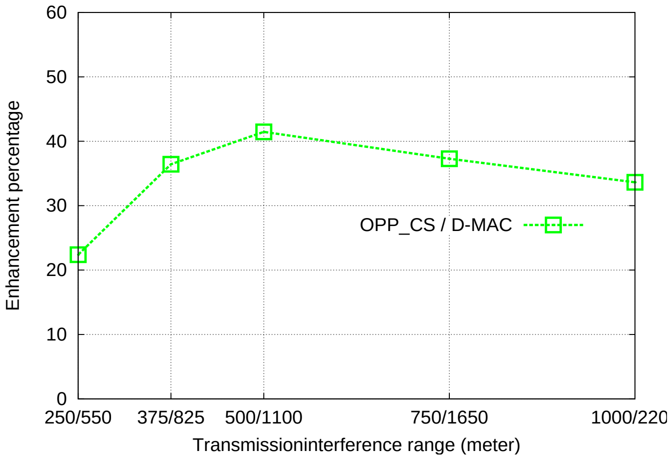

Figure 6.24: Throughput enhancement over D-MAC mechanism versus transmission/carrier sense ranges

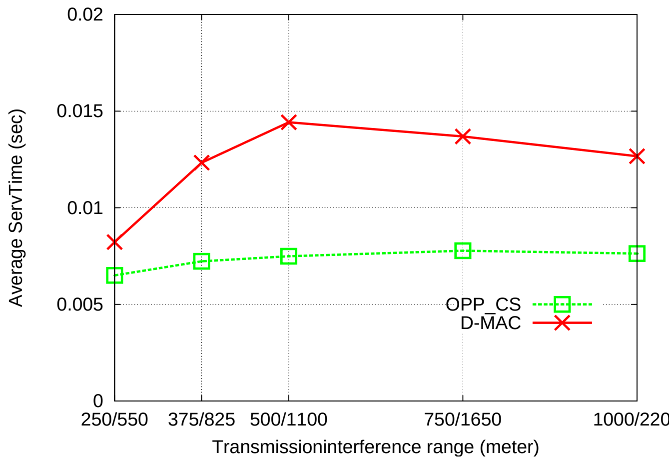

Figure 6.25: Average $ServTime$ versus transmission/carrier sense ranges

6.5.4 Impact of Transmission and Carrier Sense Range

All the mechanisms under consideration are based on the transmission and the carrier sense ranges in the network. To examine the performance of those mechanisms under different ranges, we fix the maximum distance for a connection to be within 250m while changing the node transmission/carrier sense range from 250m/550m to 1000m/2200m respectively. We fix the number of connections in the network to 100 (i.e. network degree is 2), the rate of packet generation to 40 packets per second, and the beamwidth size to 30^0. Figures 6.23 and 6.24 show the network throughput and the relative enhancement of each mechanism over D-MAC respectively. While throughput of D-MAC mechanism decreases as ranges increase, throughput of OPP_{CS} mechanism remains almost fixed. This indicates that the proposed opportunistic mechanisms scale with the transmission/carrier sense ranges. The average $ServTime$ for the different mechanisms is shown in Figure 6.25 which emphasize the previous observation.

6.6 Conclusion

We have introduced a novel opportunistic enhancement to the IEEE 802.11 networks using directional antennas. The enhancement, known as OPP_{CS}, augments communication parameters with the locations of transmitters and receivers in each frame. These parameters assist stations to better assess the channel condition, and allow increased number of concurrent transmissions to take place in presence of detecting busy carrier. The 802.11 node with directional antennas is conservative in terms of assessing channel availability. We have shown, analytically and by simulation, that our mechanism improves network throughput by up to 40% over original directional IEEE 802.11. The implementation details of integrate OPP_{CS} mechanism with the physical layer and the MAC layer of IEEE 802.11, as well as the needed interaction signals between the two layers, were given.

Chapter 7

Opportunistic Mechanisms for IEEE 802.11 Networks using Directional Antennas II: Opportunistic Head-of-Line Transmission

In this chapter, we describe another enhancement for directional antennas that is built over the OPP_{CS} enhancement described in the previous chapter. This enhancement changes the access routines of the MAC data queue.

In the omni-directional model, it is understandable that, if the topmost packet in the MAC queue is blocked, the node does not attempt to transmit any packet in the rest of queue. But this seems unnecessarily in the directional antennas model, because, if the transmission's direction of the topmost data item in the queue is blocked (due to some ongoing transmission), the node can transmit other packets in the queue if its transmission direction is not blocked. We developed a protocol, called OPP_{HOL} protocol, to handle the access routines of the MAC queue, while preserving the fairness properties of the queue. HOL stands for Head-Of-Line blocking problem aligned with the definition in [125].

7.1 Problem Formulation

When the transmission direction of the topmost data item in the queue is blocked (due to some ongoing transmission), the node checks whether the transmission's direction of the subsequent item in the queue is blocked. If not, then the node starts transmitting the data to the destination, else it goes on checking the next item and so on. For example, consider node A is engaged in a transmission by beamforming data to node B as in Figure 6.1 of Chapter 6. Node C wants to beamform data to E and then to D, but C-E transmission is blocked because of the ongoing A-B transmission. Since the C-D transmission direction would not interfere with A-B transmission, node C should not block, and transmit to D instead. To achieve this, we developed a scheme, called OPP_{HOL} scheme, where a node can transmit data, even if the direction of the topmost data item is blocked. Similar to OPP_{CS} scheme, we derive an analytical model to prove the potential gain, verify this model by simulation, and, finally, show the performance of OPP_{HOL} scheme.

7.2 Analysis of Blocking Probabilities with OPP_{HOL}

In this section, we derive the probability that a node has an opportunity to transmit directionally given that the destined sector of the packet at the topmost of the MAC queue is blocked. This probability shows the potential gain for using OPP_{HOL} scheme over OPP_{CS} described in the previous chapter. We use the same model assumption described in the previous chapter in Section 6.3.1.

7.2.1 Analysis of OPP_{HOL} Probability

Given the use of OPP_{CS} mechanism, it happens that the corresponding sector of the packet at topmost of MAC queue of a node v is blocked, while other sectors corresponding to other packets in the queue are not blocked. To improve network performance by increasing medium spatial reuse, a node should transmit one of the packets corresponding to a non-blocked sector instead of obeying the standard IEEE 802.11 by postponing transmissions until the transmission of packet at the queue's top.

Using the same example from the previous chapter in Figure 6.2, node v has two packets to transmit: the topmost packet of its queue is to be transmitted to node w_1 in sector $\#1$, and the next is to be transmitted to w_2 in sector $\#4$. Node v is blocked from transmitting to sector $\#1$, because of the transmission from node s_1 to node r_1. In the standard IEEE 802.11, node v has to postpone its transmission until sector $\#1$ becomes free. However, since sector $\#4$ is free while sector $\#1$ is blocked, node v should go ahead with its transmission to node w_2 first in order to increase the spatial reuse of the medium.

Let $P(HOL_{Idle})$ be the probability that at least one sector of the m neighbor sectors is idle (not blocked). Calculating $P(HOL_{Idle})$ is tricky, because the blocking probabilities of sectors are not independent, since a transmission may block either one or two sectors. For example, in Figure 6.2, sectors $\#2$ and $\#6$ are blocked because of the transmission between nodes s_2 and r_2. On the other hand, the transmission between nodes s_1 and r_1 blocks sector $\#1$ only. Since we are interested in the importance of the enhancements of using the MAC opportunistic mechanism, not the exact values, we calculate the upper bound of $P(HOL_{Idle})$ instead. The upper bound of $P(HOL_{Idle})$

is calculated by assuming that the blocking probabilities of the sectors are independent. Therefore, the upper bound probability of $P(HOL_{Idle})$ given m neighbors is calculated as:

$$P(HOL_{Idle}) = 1 - (1 - P(CS_{Idle}))^m \tag{7.1}$$

where $1 - P(CS_{Idle})$ is the probability that a sector is blocked. $P(CS_{Idle})$ is calculated in Equation 6.1 from the previous chapter.

Therefore, the upper bound of $P(OPP_{HOL})$, which is the probability of having at least one of the m neighbor sectors of node v being idle, given that the sector corresponding to the topmost packet of the queue is blocked, is given by

$$P(OPP_{HOL}) \;\; = \;\; P(HOL_{Idle}) - P(CS_{Idle}) \tag{7.2}$$

7.2.2 Verification of OPP_{HOL} Model

We verified our analytical results by generating random network topologies and traffic patterns similar to the one used in Section 6.3.3 in previous chapter. To simulate the transmission of node v, whenever v has a frame to send, we select ordered list of m sectors randomly from the n neighbor sectors assuming node v has queue of frames ready to be sent to their destinations in the corresponding m sectors.

Node v checks first if it can send its topmost queue frame. If it cannot, then it checks if it can send any other frame from its queue without affecting any of the ongoing transmissions. The number of situations where node v transmitted *the topmost* frame is then divided over the total number of transmission attempts to derive the probability of $P(Top_{Idle})$. Similarly, the number of situations where node v transmitted a frame

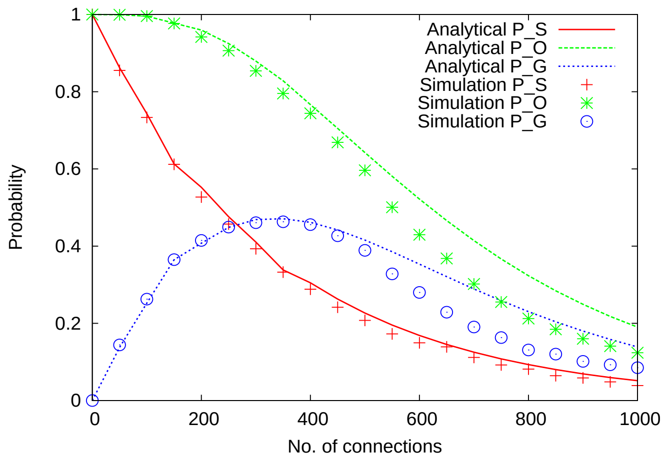

Figure 7.1: The analytical and simulation values of the probabilities P_S=$P(CS_{Idle})$, P_O=$P(HOL_{Idle})$, and P_G=$P(OPP_{HOL})$

is divided over the total number of transmission attempts to derive the probability of $P(HOL_{Idle})$. Both $P(CS_{Idle})$ and $P(HOL_{Idle})$, in addition to $P(OPP_{HOL})$, are compared to the analytical result.

Figure 7.1 plots both the analytical and the simulated values of $P(Top_{Idle})$, $P(HOL_{Idle})$, and $P(OPP_{HOL})$ for $R = 250m$, $I = 550m$, $n = 8$, $m = 4$, $\tau/T = 0.1$, and different numbers of nodes (thus varying the node density δ). Although the analytical $P(HOL_{Idle})$ and $P(OPP_{HOL})$ are upper bounds, the simulation results closely match those values specially at the peak values which is the point of our interests in this study. Therefore, the simulation validates our analysis. Similar to the analysis of $P(OPP_{CS})$ in the previous section, we used conservative assumptions to calculate $P(OPP_{HOL})$. Figure 7.2 plots the simulation of $P(OPP_{HOL})$ with those assumptions relaxed. The figure plots $P(OPP_{HOL})$ with different packet load values and different number of sectors.

In Equation 7.2, we calculated the gain of OPP_{HOL} enhancement with respect to the OPP_{CS} enhancement. To calculate the gain of OPP_{HOL} with respect to the

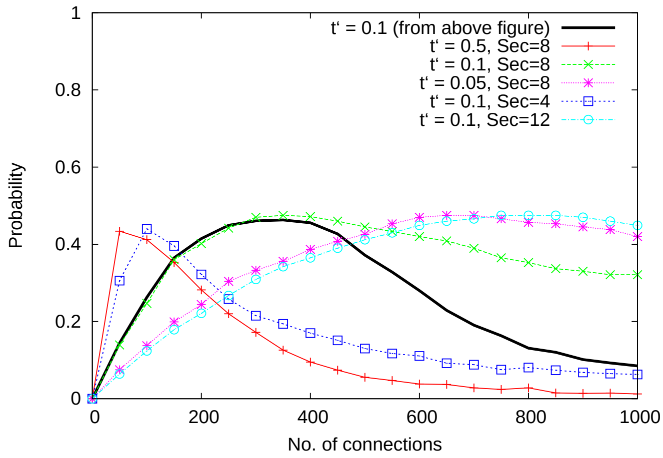

Figure 7.2: The probability $P(OPP_{HOL})$ with different load values t' where $t' = \tau/T$ and different number of sectors n, where $m = 4$

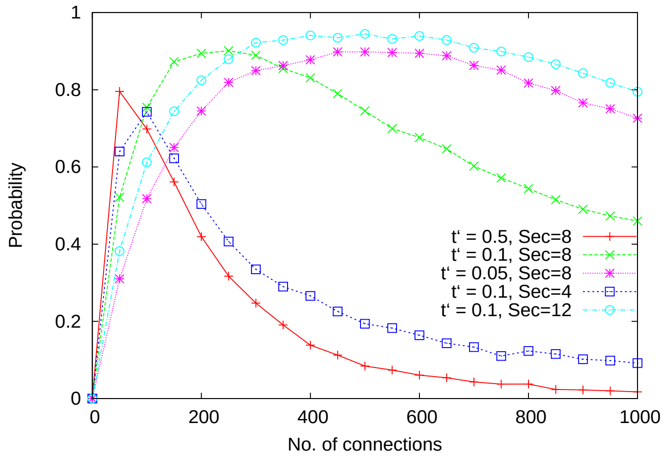

Figure 7.3: The total enhancement of OPP_{HOL} with respect to the original IEEE for different load values t' where $t' = \tau/T$ and different number of sectors n, where $m = 4$

original IEEE, as we did for OPP_{CS} in previous chapter, we replace the negative term in Equation 7.2 ($P(CS_{Idle})$) with the term $P(Std_{Idle})$ defined in Equation 6.2 in the previous chapter.

Figure 7.3 plots the simulation results of the total enhancement of node v by combining both mechanisms. The figure shows that the unnecessary blocking probability of a node using the standard IEEE 802.11 DCF is large enough when using directional antennas (as high as 90%) and hence it motivates us to consider modifying the MAC layer to exploit the directional antennas. In the following section we will describe the newly proposed modification to the IEEE 802.11 DCF for OPP_{HOL} mechanism.

7.3 Implementation of OPP_{HOL}

7.3.1 Physical Layer Design

Similar to OPP_{CS} in previous chapter, we assume that the physical layer applies Message-In-A-Message (MIM) support [17], which supports the capture of a new frame after the receiver has already begun to receive another frame do exist.

7.3.2 MAC Layer Design

The modifications for OPP_{HOL} are identical to the modifications used by OPP_{CS} in addition to modifying the procedure in which the MAC layer selects the next packet to transmit. In OPP_{CS}, MAC layer assumes at all times that the next packet to transmit is the packet at topmost of the MAC queue. However, this is not the case in OPP_{HOL}

in which a node may select packet other than the one at the topmost to be the next to transmit.

In OPP_{HOL}, a node does not maintain a distinct queue for every sector. Instead, it maintains a single queue that can be accessed as list. The node can iterate through the items in the list, and insert and delete any item.

Here is how the OPP_{HOL} algorithm works. A node checks if the direction of transmission of the topmost item in the queue is blocked. If it is blocked and the remaining blocking time (obtained from DNAV table) is greater than certain threshold, called $blkThres$, the node checks the transmission direction of the next item.

- If it is not blocked, the node sends this item, deletes it from the queue, and goes back to the topmost of the queue.

- If it is blocked and the remaining time of block is less than $blkThres$, the node waits for this time, then transmits the data, and goes back to the topmost of the queue.

- If it is blocked and the remaining blocking time is greater than $blkThres$, the node checks the transmission direction of the next item.

We assume that the check and the send times take a minor time with respect to $blkThres$. This guarantees that all packets will be delivered in order. If a node is sending items to some destination d and the first item of these items is blocked, the subsequent items to d will not be sent as their remaining time is still greater than $blkThres$. Another mechanism is, once blocking a transmission of an item to node d, all subsequent items are marked as blocked.

A node executes this algorithm under two situations. The first is after receiving a whole frame. The second is after receiving the PLCP header of new frame if the node is not the intended receiver of the frame.

A node maintains the following for each item i in the queue. $ServTime_i$, which is the service time of item i, denotes the total time spent in servicing this item, that is, the summation of the total time spent in checking whether or not to transmit this item, time to delete the item from the queue, and time spent in transmitting this item. Starvation time $StarvTime_i$ denotes the total time that the transmission of item i is delayed due to servicing the items that come afterwards in the queue (items$[i+1, ..., queue.size]$).

In short, whenever a node updates the $ServTime_i$ by δ, this δ is added to $StarvTime_{[0...i-1]}$. If the $StarvTime_i$ is greater than some threshold $Swap\_Thresh$, then the OPP_{HOL} does not check any item beyond i. This ensures that altering the order of transmission of the queue does not jeopardize the fairness of the transmission. In short, no node will starve forever. $Count_{NHi}$ denotes the number of items with index greater than i transmitted before item i. $ServTime$, $StarvTime$ and $Count_{NH}$ are the average of $ServTime_i$, $StarvTime_i$ and $Count_{NHi}$ over all packets, respectively. All these variables are used as metrics in the next section.

The final argument is how to handle CW of the backoff. For the sake of simplicity, we correlate the backoff with the node, not the packet. Thus, whenever a collision takes place during the transmission of any packet in the queue, the node applies the IEEE 802.11 backoff mechanism (double CW till a specified threshold).

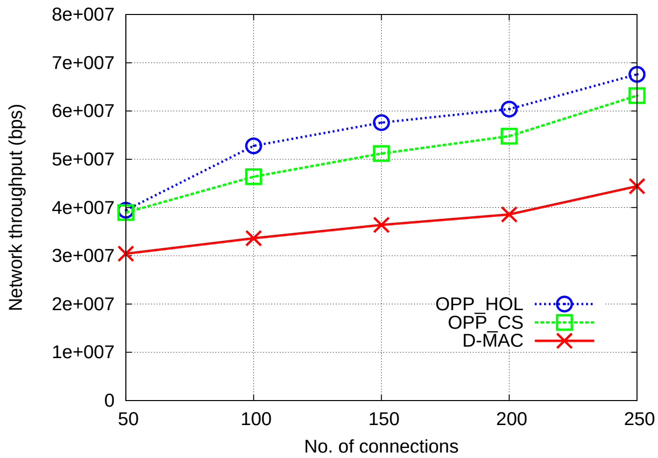

Figure 7.4: Network throughput versus number of connections

7.4 Performance Evaluation

We present extensive simulation-based studies, using ns-2, on the performance of the opportunistic mechanism OPP_{HOL}. We used the same simulation parameters and scenarios that were used for OPP_{CS} in the previous chapter. We extended the enhancement of the IEEE 802.11 MAC layer by the implementation of OPP_{HOL} mechanism in addition to OPP_{CS} mechanism.

To study the performance of our OPP_{HOL} scheme, we compare it with both OPP_{CS} and D-MAC which shoed in the previous chapter. All mechanisms use the extended ns-2 capture model as described earlier. In addition to the metrics defined in previous chapter, we also measure the average and maximum $StarvTime$ and $CountNH$, defined also in the previous section, averaged over all successfully transmitted packets for OPP_{HOL} mechanism. We set threshold $Swap\_Thresh$ to SIFS.

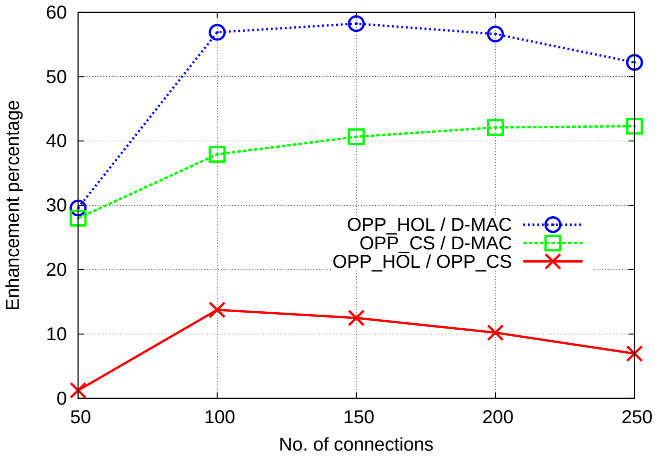

Figure 7.5: Throughput enhancement over D-MAC mechanism versus number of connections

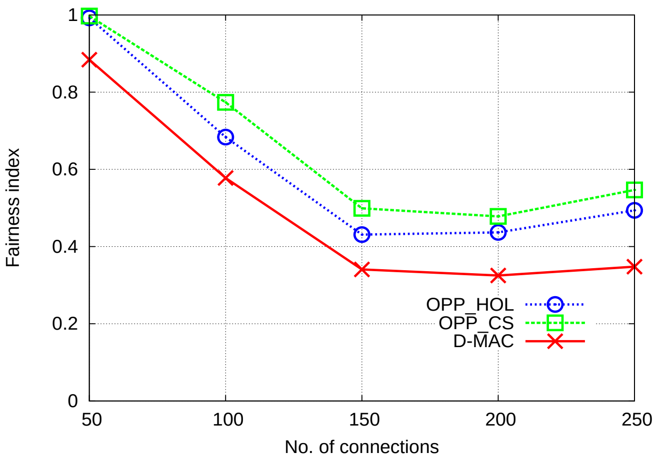

Figure 7.6: Fairness index for the network versus number of connections

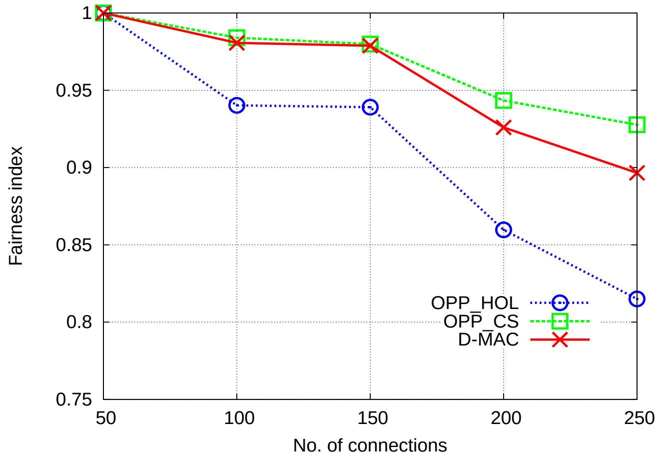

Figure 7.7: Fairness index for a node versus number of connections

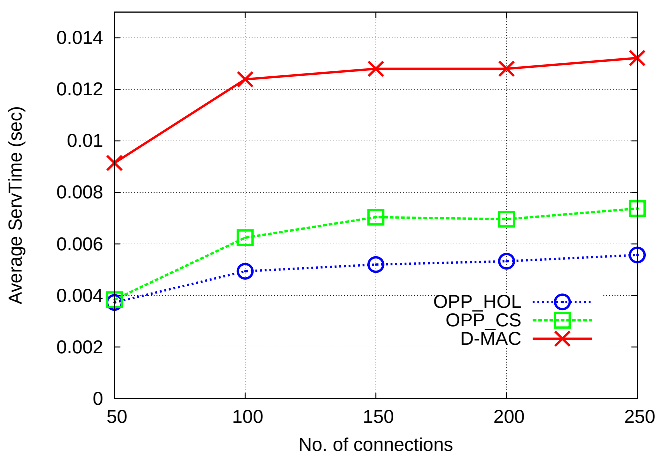

Figure 7.8: Average $ServTime$ versus number of connections

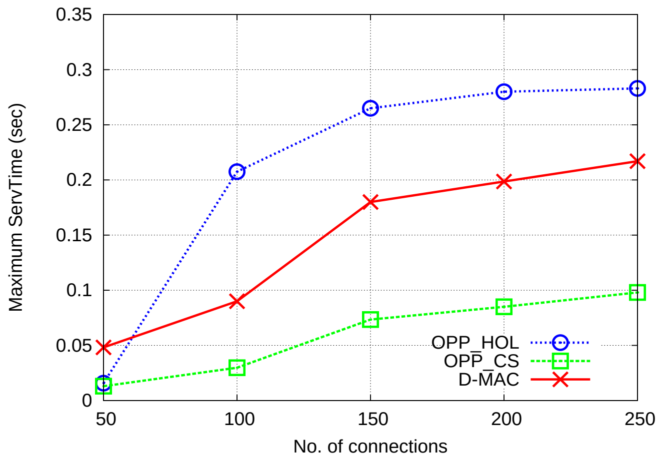

Figure 7.9: Maximum $ServTime$ versus number of connections

7.4.1 Impact of Network Degree

Figure 7.4 shows the network throughput when the number of connections varies from 50 to 250 connections. The data traffic between each pair of source and destination is a constant bit rate (CBR) UDP flow at a rate of 100 packets per second to overload the network and the beamwidth size is set to 30^0. As shown, the OPP_{HOL} mechanism has higher data throughput than the other two mechanisms. The enhancements of the mechanism over the original are shown in Figure 7.5 in terms of percentage throughput gain. While OPP_{CS} could achieve about 42% more throughput than D-MAC, OPP_{HOL} could reach 58% throughput gain. We also plotted the percentage improvement of OPP_{HOL} over OPP_{CS}. At the peak, OPP_{HOL} achieves about 14% over OPP_{CS} since it makes more spatial use of the medium. However, as the network load increases by increasing network degree, the space of improvements is reduced since the number of unblocked directions becomes smaller.

Figure 7.6 shows the network fairness index of different mechanisms. Although

	Average		Maximum	
Connections	$CountNH$	$StarvTime$	$CountNH$	$StarvTime$
50	0	0.0	0	0.0
100	15.5	0.1123	570.8	4.76
150	16.2	0.1329	680.1	5.80
200	20.76	0.1762	709.5	5.88
150	37.73	0.2610	877.3	6.50

Table 7.1: The average and maximum values of $CountNH$ and $StarvTime$ for number of connections.

OPP_{HOL} and OPP_{CS} have higher fairness than D-MAC mechanism, OPP_{HOL} has a lower fairness than the OPP_{CS}. Since different directions experience different blocking/unblocking share, OPP_{HOL} favors directions with higher unblocking share as described in the previous section. Thus packets, and consequently their corresponding connections, in certain direction starve in OPP_{HOL} mechanism and this reduces the fairness index of the mechanism. This is illustrated in Figure 7.7 shows the fairness among the connections belonging to a node averaged over all nodes. OPP_{HOL} has the lowest node fairness due to this starvation issue.

Figures 7.8 and 7.9 show the average and maximum $ServTime$ respectively. As shown, OPP_{HOL} has the best average $ServTime$, since the mechanism swaps the current packet it services with a ready-to-transmit packet as soon the direction of the original packet becomes blocked. As expected, OPP_{HOL} has the highest maximum $ServTime$ since some packets may experience several re-dequeue and re-enqueue before it is transmitted. Table 7.1 shows the average and maximum $CountNH$ and $StarvTime$ values.

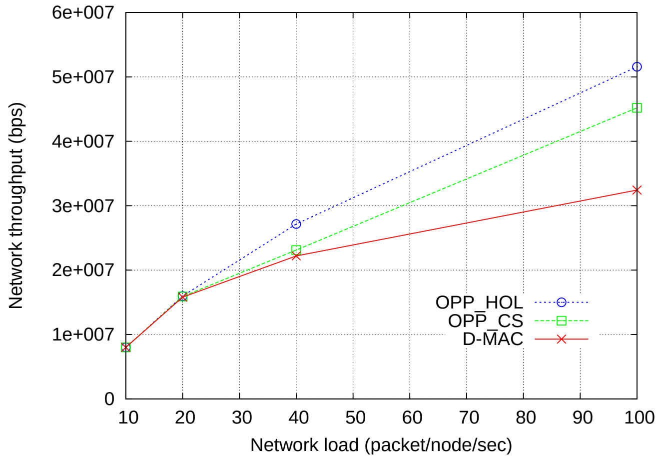

Figure 7.10: Network throughput versus network load

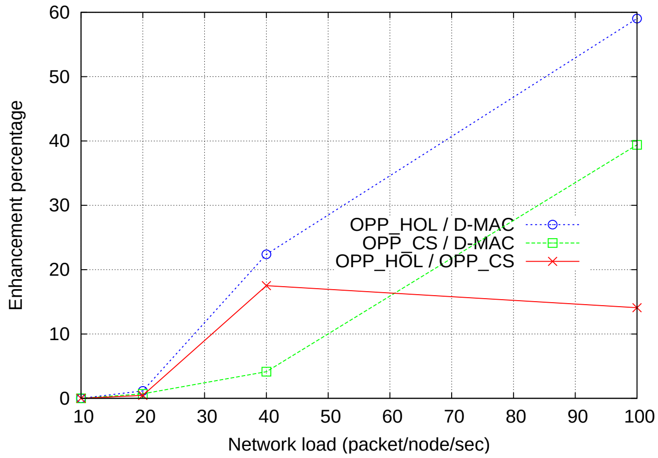

Figure 7.11: Throughput enhancement over D-MAC mechanism versus network load

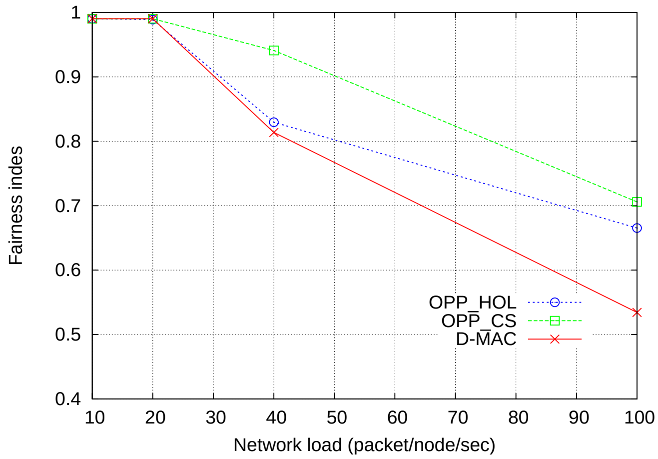

Figure 7.12: Fairness index for the network versus network load

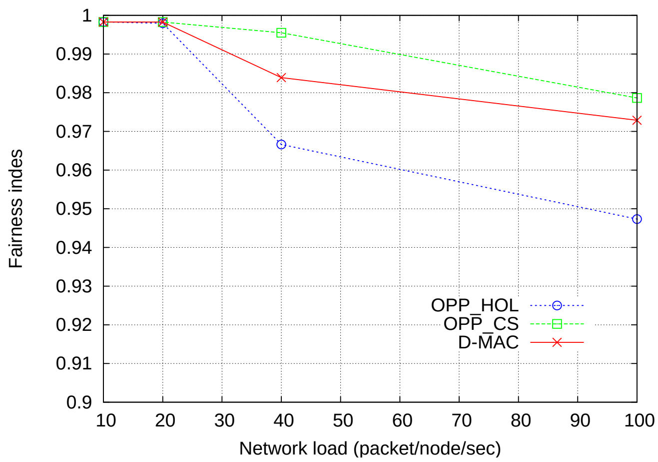

Figure 7.13: Fairness index for a node versus network load

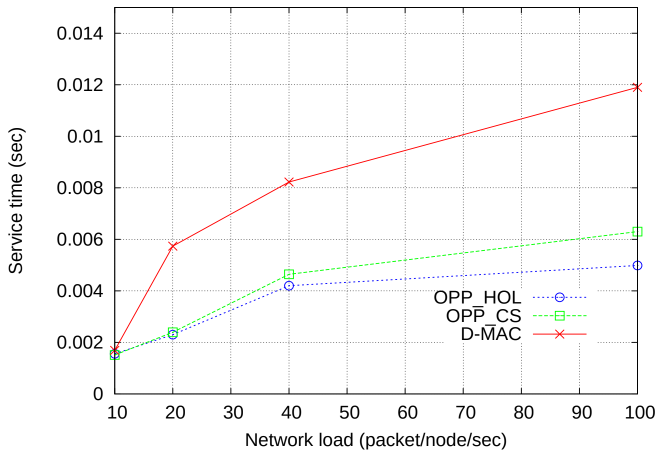

Figure 7.14: Average $ServTime$ versus network load

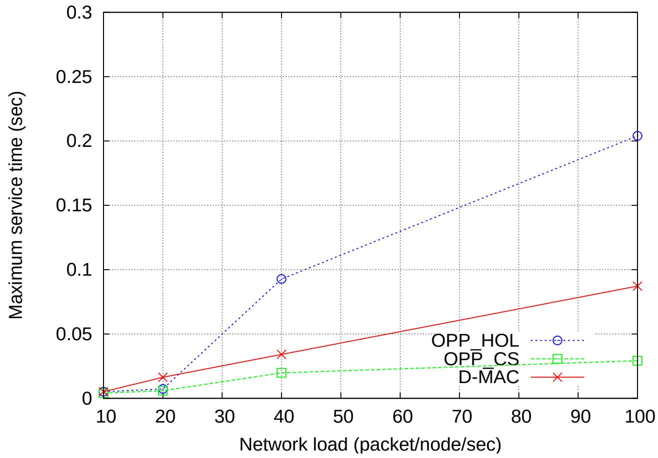

Figure 7.15: Maximum $ServTime$ versus network load

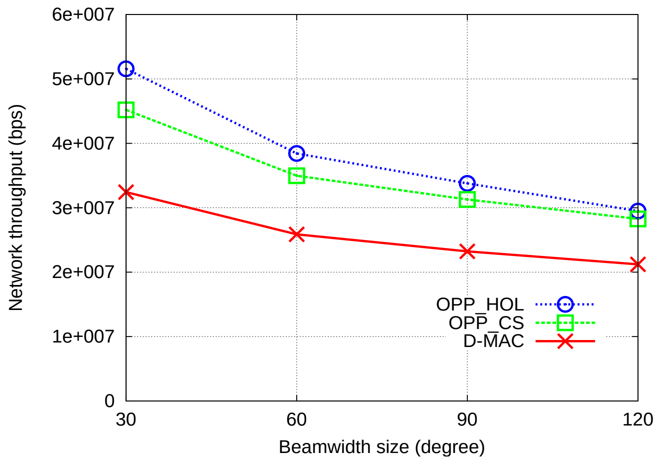

Figure 7.16: Network throughput versus beamwidth size

7.4.2 Impact of network load

Figures 7.10 and 7.11 show the network throughput and the relative enhancement of OPP_{HOL} and OPP_{CS} mechanisms over the D-MAC respectively. OPP_{HOL} outperforms OPP_{CS} mechanism especially with moderate load where the peak enhancement reach 20% over OPP_{CS} mechanism. With high packet loads, the chance that the all the transmission directions are blocked increases. Thus the enhancement of OPP_{CS} over OPP_{HOL} decreases.

Figure 7.12 shows the network fairness index and Figure 7.13 shows the fairness among the node connections. Since OPP_{HOL} try to maximize the spatial reuse by using the unblocked directions, nodes favor some directions and their corresponding transmissions in which OPP_{HOL} can not achieve as much fairness as OPP_{CS} mechanism. This is more illustrated in Figure 7.13 where OPP_{CS} has the lowest node fairness among all other mechanisms. Figures 7.14 and 7.15 show the average and maximum packet service time in which a similar pattern as previous are shown here.

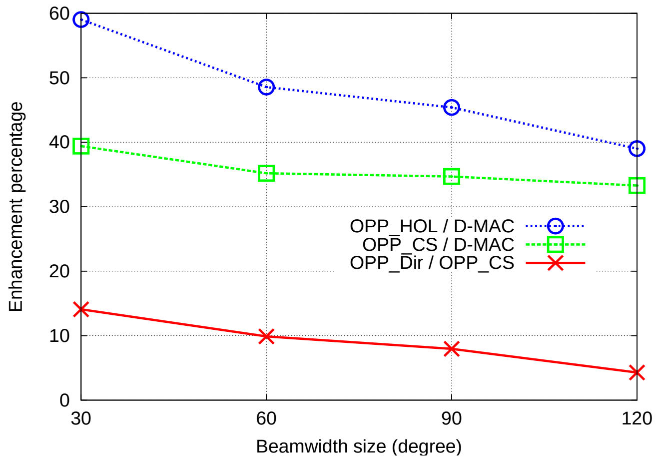

Figure 7.17: Throughput enhancement over D-MAC mechanism versus beamwidth size

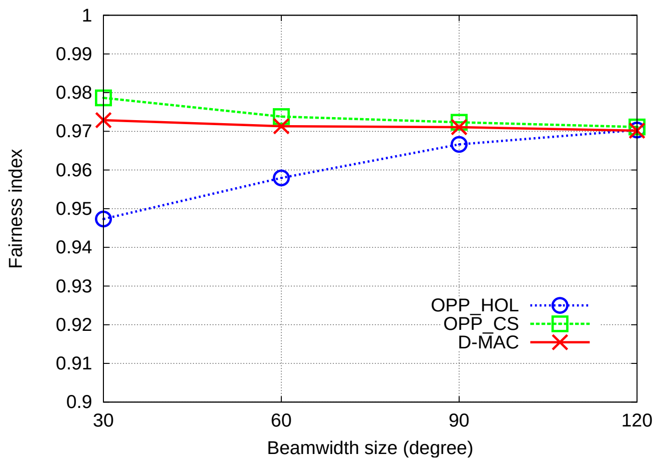

Figure 7.18: Fairness index for a node versus beamwidth size

Beamwidth size	$CountNH$	$StarvTime$
30^0	16.86	0.1116
60^0	3.95	0.0286
90^0	1.33	0.0154
120^0	0.28	0.0041

Table 7.2: The average and maximum values of $CountNH$ and $StarvTime$ for different beamwidth sizes.

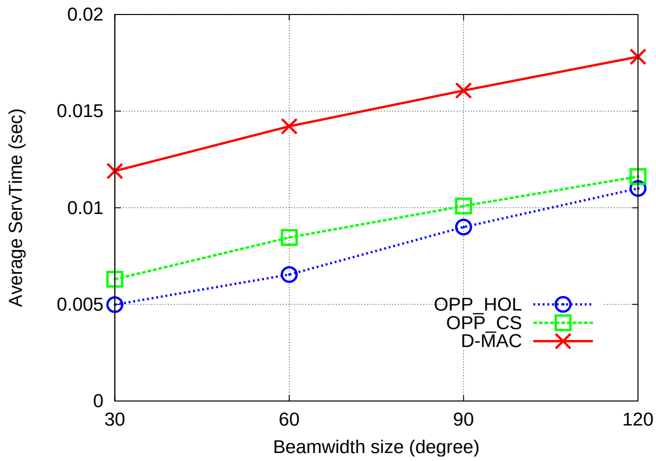

Figure 7.19: Average $ServTime$ versus number of connections

7.4.3 Impact of Beamwidth Size

We experiment with different beamwidth values to see their effects on performance. We fix the number of connections in the network to 100 (i.e. network degree is 2) and the rate of packet generation to 100 packets per second. We varied the beamwidth size from 30^0 to 120^0. Figures 7.16 and 7.17 show the network throughput and the relative enhancement of OPP_{HOL} and OPP_{CS} mechanisms over D-MAC respectively. As shown, with increasing of beamwidth, OPP_{HOL} mechanism starts to behave as OPP_{CS} mechanism.

Figures 7.18 shows the fairness among the node connections. Similar to previous results, OPP_{CS} outperforms D-MAC while OPP_{HOL} suffers from low fairness. Figure 7.19 shows the average $ServTime$ for the different mechanisms. Figure 7.2 shows the average $CountNH$ and $StarvTime$ values. From these results, OPP_{HOL} starts to render the OPP_{CS} performance as the beamwidth becomes large.

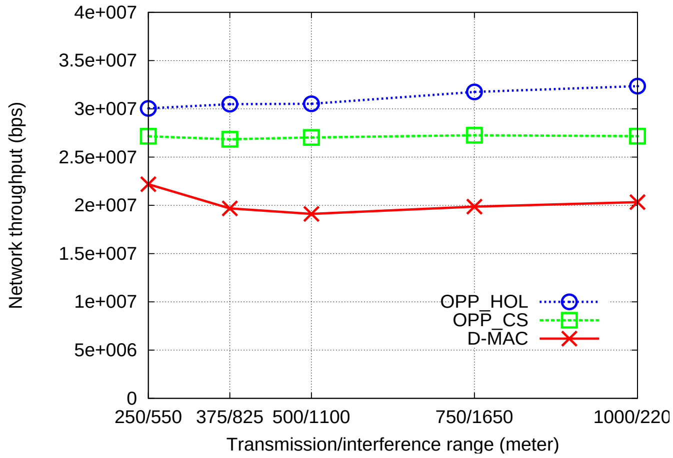

Figure 7.20: Network throughput versus transmission/carrier ranges

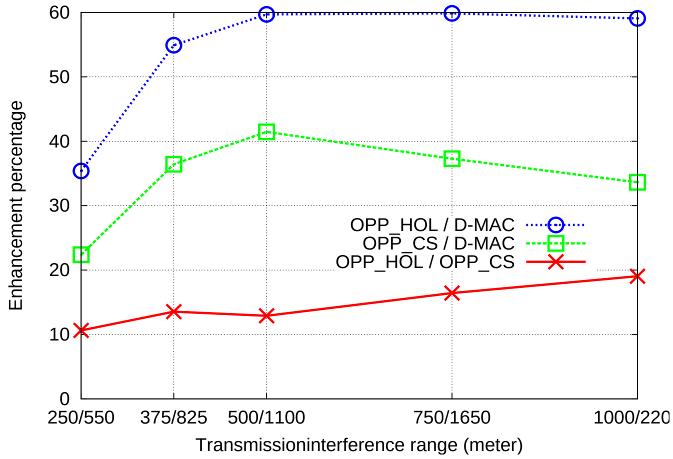

Figure 7.21: Throughput enhancement over D-MAC mechanism versus transmission/carrier sense ranges

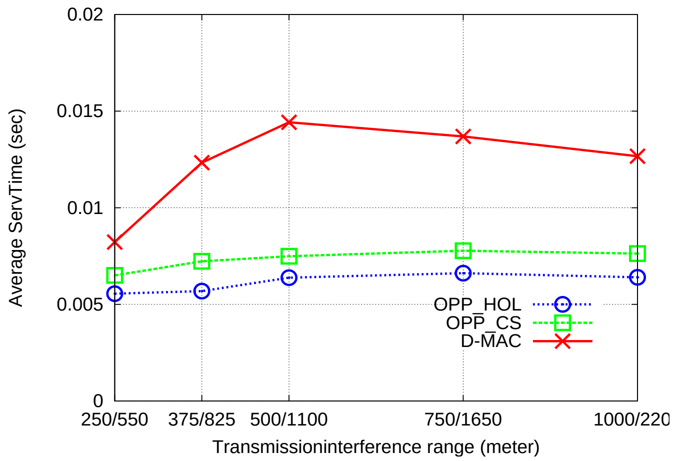

Figure 7.22: Average $ServTime$ versus transmission/carrier sense ranges

7.4.4 Impact of Transmission and Carrier Sense Range

Figures 7.20 and 7.21 show the network throughput and the relative enhancement of each mechanism over D-MAC respectively. Similar to OPP_{CS} performance, throughput of OPP_{HOL} mechanisms remains almost fixed as ranges increase. This indicates that the proposed opportunistic mechanisms scale with the transmission/carrier sense ranges. The average $ServTime$ for the different mechanisms in shown Figure 7.22.

7.5 Conclusion

We have introduced the second opportunistic enhancement to IEEE 802.11 networks using directional antennas. This mechanism is built on topmost of the OPP_{CS} mechanism introduced in the previous chapter. Our OPP_{HOL} enhancement alters the accessing way of IEEE 802.11 to its MAC queue to eliminate unnecessary blocking assessments of a node. Simulations show that our mechanism improves network throughput by up to 60%

over original directional 802.11.

Chapter 8

Conclusion and Future Works

Various properties of wireless networks, such as: limited resources (e.g., energy, bandwidth, and storage), limited radio range, no pre-existing infrastructure, mobility, vulnerable medium, and noisy channels, have made it a challenging task to design efficient networking protocols for wireless communications. As a result, network protocols and designs should be engineered by optimizing across the boundaries of traditional network layers in what is referred to as cross-layer design. Cross-layer designs yield significantly improved performance by exploiting the tight coupling between the layers in wireless systems.

In this dissertation, we studied several mechanisms to enhance network performance. Our mechanisms are based on cross-layer design methodology, where the physical layer knowledge of the wireless medium is shared with higher layers, resulting in a significant improvement in performance. Our results showed that, protocols built with cross-layer designs could make better use of network resources and significantly outperform the original mechanisms. *Although the focus of this dissertation is IEEE 802.11 networks, all the proposed mechanisms and schemes could be easily adapted for other wireless* *standards*. We summarize our contribution below:

- We introduced a novel route selection metric that considers the wireless link error rates and the fragmentation mechanism adopted by IEEE 802.11 networks. We presented Retransmission-Aware Routing (RA) protocol that utilizes this metric. Our results indicate that this protocol outperforms the standard shortest route protocol significantly (up to orders of magnitude) in terms of the reduction in the total energy consumption per packet. It is also results in higher throughputs.

- We developed an enhanced BEB mechanism for IEEE 802.11 network. This mechanism is capable of differentiating between different types of corruptions that cause unsuccessful transmissions; collision corruptions and noise corruptions. Our results showed that this mechanism enhances the network performance by order of magnitudes especially in noisy environments, and maintains the network fairness among nodes experiencing different environment conditions.

- We designed a novel contention-based distributed MAC scheme that assesses the channel condition more accurately and exploits the radio capture phenomena. Utilizing the underlying physical layer design that supports frame capture, our approach increases overall network data throughput by permitting more concurrent transmissions. Our analysis shows that up to 35% of the blocking decisions of an 802.11 node are unnecessary. Our simulations show that our mechanism can achieve up to 22% more throughput than the original 802.11.

- We developed two novel opportunistic mechanisms to exploit the medium spatial reuse of the directional antenna in IEEE 802.11 networks. The first mechanism is to augment the MAC protocol with additional information (location of the stations) while the second mechanism changes the access routines of the MAC data queue. We showed analytically that an 802.11 node with directional antenna is conservative in terms of assessing channel availability, with as much as 60% of unnecessary blocking assessments. By altering the way the 802.11 accesses its MAC data queue, we show that the unnecessary blocking assessments of a node could reach 90%. We presented the implementation details for integrating our mechanisms with the physical layer and the MAC layer of original IEEE 802.11. We also defined the needed interaction signals needed between the two layers. Our results showed that the first mechanism improves network throughput by up to 40% over original directional 802.11 and by up to 60% in case of using the second mechanism with better fairness at the same time.

The ideas and the results presented in this dissertation can be extended in several directions. One way is to extend the route selection metric for ad hoc routing protocols, introduced in Chapter 3, to include the bit transmission rate of the MAC layer. As shown in Equation 3.1, wireless links with lower bit transmission rates have higher transmission reliability. Hence, the computations of the Retransmission-Aware Routing (RA) protocol should utilize the new metric to construct paths that are more efficient. It would be interesting to study the performance of anycast/multicast paths in ad hoc networks using this metric.

An additional extension for routing layer is to augment the routing protocols by on-demand/low-overhead maintenance mechanism in which connections switch to better routes whenever they become available. On-demand means the mechanism should only work as long as a route is needed. This is to comply with the on-demand methodology for using low overhead, which is important in ad hoc networks.

Another direction, is to extend *LED* mechanism in Chapter 5. One way is to study the effect of radio management techniques such as dynamic transmission power control on network performance. Also, we may enhance the mechanism by altering the way the 802.11 accesses its MAC data queue, similar to what was described in Chapter 7. Another approach may be to study the interaction between LED mechanism in MAC layer and the routing computations in the routing layer.

It may be useful to investigate more the correlation between $StarvTime$ metric and the network fairness for OPP_{HOL} scheme described in Chapter 7, and, to develop a mechanism to calculate the value of this metric to balance the tradeoff between the network throughput and network fairness. We may also study the effect of combining our schemes for directional antenna presented in Chapter 6 and Chapter 7 with other opportunistic mechanisms such as sending multiple back-to-back date packets [111] whenever a direction become available. In addition, radio management techniques such as dynamic transmission power control may also be included to improve the performance of our mechanisms.

BIBLIOGRAPHY

[1] Mobile Ad-Hoc Networks (MANET) Charter IETF. *http://www.ietf.org/html.charters/manet-charter.html*.

[2] The Monarch Group at Rice University. http://www.monarch.cs.rice.edu/.

[3] The Network Simulator ns-2,
http://www.isi.edu/nsnam/ns/.

[4] IEEE 802.11b, Part ll: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer Extension in the 2.4GHz Band. *supplement to IEEE 802.11 Standard*, September 1999.

[5] IEEE Standard 802.11, Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. June 1999.

[6] A. Acharya, A. Misra, and S. Bansal. MACA-P: A MAC for Concurrent Transmissions in Multi-hop Wireless Networks. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom'03)*, Fort Worth, Texas, March 2003.

[7] H. Ahmadi, A. Krishna, and R.O. LaMaire. Design Issues in Wireless LANs. *Journal of High Speed Networks*, 5:87–104, 1996.

[8] M. Ahmadi, A. Krishna, and R. LaMaire. Design Issues in Wireless LANs. *J. High Speed Networks*, 5, 1996.

[9] ANSI/IEEE. 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 2000.

[10] P. Bahl and V. Padmanabhan. RADAR: An In-Building RF-based User Location and Tracking System. In *Proceedings of IEEE Infocom 2000*, Tel-Aviv, Israel, March 2000.

[11] S. Banerjee and A. Misra. Minimum Energy Paths for Reliable Communication in Multi-hop Wireless Networks. In *Proc. of Mobihoc*, June 2002.

[12] S. Basagni, I. Chlamtac, V. Syrotiuk, and B. Woodward. A Distance Routing Effect Algorithm for Mobility (DREAM). In *Proc. ACM/IEEE Mobicom*, 1998.

[13] B. Bellur, R. Ogier, and F. Templin. Topology Broadcast Based on Reverse-Path Forwarding (TBRPF). In *Internet Draft, draft-ietf-manet-tbrpf-01.txt, work in progress*, 2001.

[14] P. Bhagwat, P. Bhattacharya, A. Krishna, and S. Tripathi. Enhancing Throughput over Wireless LANs using Channel State Dependent Packet Scheduling. In *Proceedings of the IEEE INFOCOM'96*, San Franciso, CA, USA, March 1996.

[15] V. Bharghavan, A. J. Demers, S. Shenker, and L. Zhang. MACAW: A Media Access Protocol for Wireless LAN's. In *Proceedings of SIGCOMM*, 1994.

[16] Giuseppe Bianchi. Performance Anaylsis of the IEEE 802.11 Distributed Coordination Function. *IEEE Journal on selected areas in communications*, 18, March 2000.

[17] J. Boer and et. al. Wireless LAN With Enhanced Capture Provision, U.S. Patent 5987033. Technical report, 1999.

[18] J. Bray and C. Sturman. *Bluetooth: Connect without Cables*. Prentice Hall PTR, 2000. ISBN: 0130898406.

[19] F. Cali, M. Conti, and E. Gregori. Dynamic Tuning of the IEEE 802.11 Protocol to Achieve a Theoretical Throughput Limit. *IEEE/ACM Transactions on Networking*, 8(6), December 2000.

[20] M. Cesana, D. Maniezzo, P. Bergamo, and M. Gerla. Interference Aware (IA) MAC: An Enhancement to IEEE802.11b DCF. In *Proceedings of IEEE Vehicular Technology Conference*, Orlando, Florida, USA, 2003.

[21] J.-H. Chang and L. Tassiulas. Energy Conserving Routing in Wireless Ad-hoc Networks. In *Proc. of Infocom*, March 2000.

[22] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris. Span: An Energy-Efficient coordination Alogrithm for Topology Mainte nance in Ad Hoc Wireless Networks. *ACM Wireless Networks Journal*, 8(5), September 2002.

[23] K. Cheun and S. Kim. Joint Delay-Power Capture in Spread-Spectrum Packet Radio Networks. *IEEE Transaction on Communications*, 1998.

[24] H.S. Chhaya and S. Gupta. Performance modeling of asynchronous data transfer methods of IEEE 802.11 MAC protocol. *Wireless Networks*, 3, 1997.

[25] K. Chin, J. Judge, A. Williams, and K. Kermode. Implementation experience with MANET routing protocols. *ACM SIGCOMM Computer Communications Review*, 32(5), November 2002.

[26] D.-M. Chiu and R. Jain. Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks. *Computer Networks and ISDN Systems*, 17:1–14, 1989.

[27] R. Choudhury, X. Yang, R. Ramanathan, and N. Vaidya. Using Directional Antennas for Medium Access Control in Ad Hoc Networks. In *Proceedings of the ACM MOBICOM'02*, Atlanta, Georgia, USA, September 2002.

[28] M. Corson and A. Ephremides. Lightweight Mobile Routing protocol (LMR), A Distributed Routing Algorithm For Mobile Wireless Networks. *Wireless Networks*, 1995.

[29] Maniezzo D., Bergamo P., Cesana M., and Gerla M. How to Outperform IEEE802.11: Interference Aware (IA) MAC. In *Proceedings of MedHocNet*, Mahdia, Tunisia, 2003.

[30] B. Davies and T. Davies. The Application of Packet Switching Techniques to Combat Net Radio. *Proc. of the IEEE*, 75(1), January 1987.

[31] D. De Couto, D. Aguayo, J. Bicket, and R. Morris. A HighThroughput Path Metric for MultiHop Wireless Routing. In *Proc. of MobiCom 03*, September 2003.

[32] J. Doble. *Introduction to Radio Propagation for Fixed and Mobile Communications*. Artech House Publishers, October 1996. ISBN: 0890065292.

[33] R. Dube, C. Rais, K. Wang, and S. Tripathi. Signal Stability-Based Adaptive Routing (SSA) for Ad Hoc Mobile Networks. *IEEE Personal Communications*, February 1997.

[34] C. Eklund, R. Marks, K. Stanwood, and S. Wang. IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access. *IEEE Communications Magazine*, 2002.

[35] A. El Gamal, C. Nair, B. Prabhakar, E. Uysal-Biyikoglu, and S. Zahedi. Energy-efficient Scheduling of Packet Transmissions over Wireless Ne tworks. In *Proc. of IEEE Infocom*, June 2002.

[36] T. ElBatt, T. Anderson, and B. Ryu. Performance Evaluation of Multiple Access Protocols for Ad hoc Networks Using Directional Antennas. In *IEEE Wireless Communications and Networking Conference (WCNC)*, New Orleans, Louisiana, USA, March 2003.

[37] P. Enge and P. Misra. Special issue on GPS: The Global Positioning System. *Proceedings of The IEEE*, 87(1), January 1999.

[38] Sophia Antipolis Valbonne France. European Telecommunication Standards Institute, 650 Route des Lucioles. HIgh PErformance Radio Local Area Network Type 1: functional specification. *pr ets 300 652 edition*, May 1996.

[39] N. Fahmy, T. Todd, and V. Kezys. Ad Hoc Networks with Smart Antennas Using IEEE 802.11-Based Protocols. In *Proceedings of IEEE International Conference on Communications (ICC 2002)*, New York, NY, USA, April 2002.

[40] H. Friis. A Note on a Simple Transmission Formula. *Proceedings of the IRE*, 41, May 1946.

[41] H. Friis. Introduction to Radio and Radio Antennas. *IEEE Spectrum*, 1971.

[42] C. Fullmer and J.J. Garcia-Luna-Aceves. Floor Acquisition Multiple Access (FAMA) for Packet-Radio Networks. In *Proceedings of SIGCOMM*, Cambridge, MA, 1995.

[43] J.J. Garcia-Luna-Aveces and M. Spohn. Source Tree Adaptive Routing. In *Internet Draft, draft-ietf-manet-star-00.txt, work in progress*, 1999.

[44] J.H. Gass Jr., M.B. Pursley, H.B. Russell, and J.S. Wysocarski. An Adaptive-Transmission Protocol for Frequency-Hop Wireless Communication Networks. *Wireless Networks*, 7(5):487–495, September 2001.

[45] E. Geraniotis and M. Soroushnejad. Probability of Capture and Rejection of Primary Multiple Access Interference in Spread Spectrum Networks. *IEEE Transactions on Communications*, 39(6), 1991.

[46] M. Gerla, X. Hong, L. Ma, and G. Pei. Landmark Routing Protocol (LANMAR). In *Internet Draft, draft-ietf-manet-lanmar-01.txt, work in progress*, 2001.

[47] M. Gerla, G. Pei, X. Hong, and T. Chen. Fisheye State Routing Protocol (FSR) for Ad Hoc Networks. In *Internet Draft, draft-ietf-manet-fsr-00.txt, work in progress*, 2001.

[48] T. Goff, N. Abu-Ghazaleh, D. Phatak, and R. Kahvecioglu. Preemptive Routing in Ad Hoc Networks. In *Proc. of ACM/IEEE MobiCom*, 1999.

[49] J. Gomez-Castellanos, A. Campbell, M. Naghshineh, and C. Bisdikian. PARO: A Power-Aware Routing Optimization Scheme for Mobile Ad Hoc Networks, draft-gomez-paro-manet-00.txt, Work in Progress. *IETF*, March 2001.

[50] S. Guo and O. Yang. Performance of Backup Source Routing (BSR) in Mobile Ad Hoc Networks. In *Proc. IEEE Wireless Networking Conference*, 2002.

[51] Z. Haas, M. Pearlman, and P. Samar. The Bordercast Resolution Protocol (BRP). In *Internet Draft, draft-ietf-manet-zone-brp-02.txt, work in progress*, 2002.

[52] Z. Haas, M. Pearlman, and P. Samar. The Zone Routing Protocol (ZRP) for Ad Hoc Networks. In *IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt*, 2002.

[53] Z. Hadzi-Velkov and B. Spasenovski. Capture Effect in IEEE 802.11 Wireless LANs. In *Proceedings of IEEE ICWLHN 2001*, Singapore, December 2001.

[54] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient Communication Protocols for Wireless Microsensor Networks. In *Proc. of the Hawaiian International Conference on Systems Science*, January 2000.

[55] Y. Hu and D. Johnson. Design and Demonstration of Live Audio and Video over Multihop Wireless Ad Hoc Networks. In *Proc. of MILCOM*, 2002.

[56] Y-C. Hu, D. Johnson, and D. Maltz. Flow State in the Dynamic Source Routing Protocol. In *Internet Draft, draft-ietf-manet-dsrflow-00.txt, work in progress*, 2001.

[57] Z Huang, C-C. Shen, C. Srisathapornphat, and C. Jaikaeo. A Busy-Tone Based Directional MAC Protocol for Ad Hoc Networks. In *IEEE MILCOM*, Anaheim, CA, USA, October 2002.

[58] P. Jacquet, P. Muhlethaler, A. Qayyum, A. Laouiti, L. Viennot, and T. Clausen. Optimized Link State Routing Protocol. In *Internet Draft, draft-ietf-manet-olsr-04.txt, work in progress*, 2001.

[59] R Jain. *The Art of Computer Systems Performance Analysis*. John Wiley and Sons, 1991.

[60] Z. Ji, Y. Yang, J. Zhou, M. Takai, and R. Bagrodia. Exploiting Medium Access Diversity in Rate Adaptive Wireless LANs. In *Proceedings of MobiCom'04*, Philadelphia, Pennsylvania, USA, September 2004.

[61] M. Jiang, J. Li, and Y. Tay. Cluster Based Routing Protocol (CBRP) Functional Specification. In *Internet Draft, draft-ietf-manet-cbrp.txt, work in progress*, 1999.

[62] D. Johnson and D. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In *Mobile Computing*, pages 153–181, 1996.

[63] D. Johnson, D. Maltz, Y-C. Hu, and J. Jetcheva. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. In *Internet Draft, draft-ietf-manet-dsr-05.txt, work in progress*, 2001.

[64] P. Karn. MACA - A New Channel Access Method for Packet Radio. In *ARRL/CRRL Amateur Radio 9th Coputer Networking Conference*, September 1990.

[65] Y. Ko and N. Vaidya. Location-Aided Routing in Mobile Ad Hoc Networks. In *Proc. ACM/IEEE Mobicom*, 1998.

[66] Y-B. Ko, V. Shankarkumar, and N. Vaidya. Medium Access Control Protocols Using Directional Antennas in Ad Hoc Networks. In *Proceedings of IEEE INFOCOM '00*, Tel-Aviv, Israel, March 2000.

[67] A. Kochut, A. Vasan, A. Shankar, and A. Agrawala. Sniffing out the correct Physical Layer Capture model in 802.11b. In *Proceedings of IEEE International Conference on Network Protocols (ICNP)*, Berlin, Germany, October 2004.

[68] P. Krishnan, A.S. Krishnakumar, W.-H. Ju, C. Mallows, and S. Ganu. A System for LEASE: Location Estimation Assisted by Stationary Emitters for Indoor RF Wireless Networks. In *Proceedings of IEEE Infocom 2004,* Hong Kong, March 2004.

[69] S. Kubota, K. Mutsuura, O. Akizuki, and S. Ooshita. A Random Access Micro-Cellular System. *IEICE Trans. Fundamentals*, (7), 1997.

[70] S. Kubota, K. Mutsuura, O. Akizuki, and S. Ooshita. A Random Access Micro-Cellular System. *IEICE Trans. Fundamentals*, E80-A(7):1241–1248, July 1997.

[71] C.T. Lau and C. Leung. Capture Models for Mobile Packet Radio Networks. *IEEE Transactions on Communications*, COM-40:917–925, May 1992.

[72] W. Lee. *Mobile Communications Engineering*. McGraw-Hill, 1982. ISBN: 0-07-037039-7.

[73] J. Li, J. Janotti, D. De Coutu, D. Karger, and R. Morris. A Scalable Location Service for Geographic Ad Hoc Routing. In *Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000)*, 2000.

[74] X. Liu, E. Chong, and N. Shroff. Opportunistic Transmission Scheduling With Resource-Sharing Constraints in Wireless Networks. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, 19(10), 2001.

[75] Y. Liu and E. Knightly. Opportunistic Fair Scheduling over Multiple Wireless Channels. In *Proceedings of the IEEE INFOCOM'03*, San Franciso, CA, USA, April 2003.

[76] D. Lu and D. Rutledge. Investigation of indoor radio channels from 2.4 GHz to 24 GHz. In *Proceedings of the IEEE Antennas and Propagation Symposium (APS/URSI)*, June 2003.

[77] H. Lundgren, E. Nordstrom, and C. Tschudin. Coping with comunication gray zones in ieee 802.11b based ad hoc networks. In *5th ACM international workshop on Wireless mobile multimedia (WoWMoM)*, September 2002.

[78] J. Metzner. On Improving Utilization in ALOHA Networks. *IEEE Trans. Commun.*, 1976.

[79] J.J. Metzner. On Improving Utilization in ALOHA networks. *IEEE Transactions on Communications*, COM-24:447–448, 1976.

[80] A. Misra and S. Banerjee. MRPC: Maximizing Network Lifetime for Reliable Routing in Wireless Environments. In *Proc. of WCNC*, March 2002.

[81] S. Murthy and J.J. Garcia-Luna-Aveces. Distributed Bellman-Ford routing protocol (DBF): A Routing Protocol for Packet Radio Networks. In *Proc. ACM International Conference on Mobile Computing and Networking*, 1995.

[82] K. Mutsuura, H. Okada, K. Ohtsuki, and Y. Tezuka. A New Control Scheme with Capture Effect for Random Access Packet Communications. In *Proc. IEEE GLOBECOM*, 1989.

[83] K. Mutsuura, H. Okada, K. Ohtsuki, and Y. Tezuka. A New Control Scheme with Capture Effect for Random Access Packet Communications. In *Proceedings of IEEE GLOBECOM*, pages 938–944, 1989.

[84] T. Nadeem and A. Agrawala. IEEE 802.11 DCF Enhancements for Noisy Environments. In *Proceedings of The 15th IEEE International Symposium on*

Personal, Indoor, and Mobile Radio Communications (PIMRC 2004), Barcelona, Spain, September 2004.

[85] T. Nadeem and A. Agrawala. IEEE 802.11 Fragmentation-Aware Energy-Efficient Ad-Hoc Routing Protocols (runner up for Best Paper Award). In *Proceedings of IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, Fort Lauderdale, Florida, USA, October 2004.

[86] T. Nadeem and A. Agrawala. Performance of IEEE 802.11 based Wireless Sensor Networks in Noisy Environments. In *Proceedings of IEEE Workshop on Information Assurance in Wireless Sensor Networks (WSNIA'05) in conjunction with 24th IEEE International Performance Computing and Communications Conference (IPCCC'05)*, Phoenix, Arizona, USA, April 2005.

[87] T. Nadeem, S. Banerjee, A. Misra, and A. Agrawala. Energy-Efficient Reliable Paths for On-Demand Routing Protocols. In *Proceedings of Sixth IFIP IEEE International Conference on Mobile and Wireless Communication Networks*, Paris, France, October 2004.

[88] T. Nadeem, T. Elsharnouby, and A. Agrawala. Opportunistic Mechanisms for IEEE 802.11 Networks using Directional Antenna. Under Submission.

[89] T. Nadeem, L. Ji, A. Agrawala, and J. Agre. Location Aware IEEE 802.11 DCF for Spatial Reuse Enhancment. Under Submission.

[90] T. Nadeem, L. Ji, A. Agrawala, and J. Agre. Location Enhancement to IEEE 802.11 DCF. In *Proceedings of 24th IEEE INFOCOM 2005*, Miami, Florida, USA, March 2005.

[91] A. Nasipuri, K. Li, and U. Sappidi. Power Consumption and Throughput in Mobile Ad Hoc Networks using Directional Antennas. In *IEEE International Conference on Computer Communication and Networks (ICCCN)*, Miami, Florida, October 2002.

[92] A. Nasipuri, S. Ye, J. You, and R. Hiromoto. A MAC Protocol for Mobile Ad Hoc Networks using Directional Antennas. In *Proceedings of the IEEE WCNC*, Chicago, IL, USA, September 2000.

[93] J. Ng and I. Lu. A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks. In *IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks*, 1999.

[94] N. Nikaein and C. Bonnet. Hybrid Ad Hoc Routing Protocol - HARP. In *proceeding of IST 2001: International Symposium on Telecommunications*, 2001.

[95] N. Nikaein, H. Labiod, and C. Bonnet. Distributed Dynamic Routing Algorithm (DDR) for Mobile Ad Hoc Networks. In *proceedings of the MobiHOC 2000*, 2000.

[96] Bluetooth official website. http://www.Bluetooth.com.

[97] V. Park and S. Corson. Temporally-Ordered Routing Algorithm (TORA). In *Internet Draft, draft-ietf-manet-tora-spec-03.txt, work in progress*, 2001.

[98] V. Park and S. Corson. Temporally-Ordered Routing Algorithm (TORA) Version 1: Functional Specification, draft-ietf-manet-tora-spec-04.txt, Work in progress. *IETF*, July 2001.

[99] C. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In *In Proc. of the ACM SIGCOMM*, 1994.

[100] C. Perkins, E. Royer, and S. Das. Ad Hoc On-demand Distance Vector (AODV) Routing. In *Internet Draft, draft-ietf-manet-aodv-11.txt, work in progress*, 2002.

[101] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In *Proc. of the* 2^{nd} *IEEE Workshop on Mobile Computing Systems and Applications*, February 1999.

[102] Freescale Zigbee Reference Platform. http://www.freescale.com/.

[103] B. Prabhakar, E. Uysal-Biyikoglu, and A. El Gamal. Energy-efficient Transmission over a Wireless Link via Lazy Packet Scheduling. In *Proc. of IEEE Infocom*, April 2001.

[104] J.G. Proakis. Digital Communications. *Third Edition*, *McGraw-Hill*, *Inc.*, *New York*, 1995.

[105] J.G. Proakis. *Digital Communications*, 4^{th} *edition. Page 270.* New York, McGraw-Hill, 2000.

[106] Daji Qiao and Sunghyun Choi. Goodput enhancement of IEEE 802.11a wireless LAN via link adaptation. In *Proc. of IEEE International Conference on Communications*, 2001.

[107] Daji Qiao, Sunghyun Choi, and Kang G. Shin. Goodput Analysis and Link Adaptation for IEEE 802.11a Wireless LANs. *IEEE Transaction On Mobile Computing*, 1(4), 2002.

[108] R. Ramanathan. On the Performance of Ad Hoc Networks with Beamforming Antennas. In *Proceedings of the MobiHOC '01*, Long Beach, CA, USA, October 2001.

[109] R. Ramanathan and R. Rosales-Hain. Topology Control of Multihop Wireless Networks using Transmit Power Adjustment. In *Proc. of Infocom*, March 2000.

[110] T. Rappaport. *Wireless communications, principles and practice*. Prentice Hall, 1996.

[111] B. Sadeghi, V. Kanodia, A. Sabharwal, and E. Knightly. OAR: An Opportunistic MAC for Multirate Ad Hoc Networks. *ACM Journal of Mobile Networks and Applications (MONET)*, 2004.

[112] M. Sanchez, T. Giles, and J. Zander. Beam Forming Antennas in Multi-hop Packet Radio. In *Proceedings of the Swedish Workshop on Wireless Ad Hoc Networks*, March 2001.

[113] Santivanez and R. Ramanathan. Hazy Sighted Link State routing protocol (HSLS). Technical report, BBN Technical Memorandum No. 1301, 2001.

[114] K. Scott and N. Bambos. Routing and Channel Assignment for Low Power Transmission in PCS. In *Proc. of ICUPC*, October 1996.

[115] S. Singh and C.S. Raghavendra. PAMAS-Power Aware Multi-Access Protocol with Signaling for Ad Hoc Networks. In *ACM Comm. Review*, July 1998.

[116] M. Soroushnejad and E. Geraniotis. Probability of Capture and Rejection of Primary Multiple Access Interference in Spread Spectrum Networks. *IEEE Transactions on Communications*, 39(6), 1991.

[117] A. Spyropoulo and C. Raghavendra. Capacity Bounds For Ad-Hoc Networks Using Directional Antennas. In *Proceedings of IEEE International Conference on Communications (ICC'03)*, Anchorage, Alaska, USA, May 2003.

[118] C. Srisathapornphat and C-C. Shen. Energy Consumption Behavior and Performance of Directional Virtual Carrier Sensing Schemes. In *Proceedings of the IEEE WCNC*, New Orleans, Louisiana, USA, March 2003.

[119] M. Takai, J. Martin, A. Ren, and R. Bagrodia. Directional Virtual Carrier Sensing for Directional Antennas in Mobile Ad Hoc Networks. In *Proceedings of The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Lausanne, Switzerland, June 2002.

[120] Y.C. Tay and K.C. Chua. A Capacity analysis for the IEEE 802.11 MAC protocol. *Wireless Networks*, pages 159–171, January 2001.

[121] C.-K. TOH. Associativity-Based Routing for Ad-Hoc Mobile Networks. *Wireless Personal Communications Journal, Special Issue on Mobile Networking and Computing Systems*, 1997.

[122] C.K. Toh, H. Cobb, and D. Scott. Performance Evaluation of battery-Life-Aware Routing Schemes for Wireless Ad Hoc Networks. In *Proc. of ICC*, June 2001.

[123] A. Vasan, A. Kochut, and A. Shankar. Sniffing out the Correct Physical Layer Capture Model in 802.11b. Technical report, Technical report, UMIACS-TR-2004-26 and CS-TR-4583, Department of Computer Science, University of Maryland College Park, 2004.

[124] A. Vasan, R. Ramjee, and T. Woo. ECHOS: Enhanced Capacity 802.11 Hotspots. In *Proceedings of IEEE INFOCOM 2005*, Miami, Florida, March 2005.

[125] J. Wang, H. Zhai, and Y. Fang. Opportunistic Packet Scheduling and Media Access Control for Wireless LANs and Multi-hop Ad Hoc Networks. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'04)*, Atlanta, Georgia, USA, March 2004.

[126] Y. Wang and J.J. Garcia-Luna-Aceves. Collision Avoidance in Single-Channel Ad Hoc Networks Using Directional Antennas. In *Proceedings of the IEEE Intl. Conf. on Distributed Computing Systems (ICDCS '03)*, Providence, Rhode Island, USA, May 2003.

[127] C. Ware, J.F. Chicharo, and T. Wysocki. Modelling of Capture Behaviour in IEEE 802.11 Radio Modems. In *Proceedings of IEEE International Conference on Telecommunications*, June 2001.

[128] C. Ware, J. Judge, J. Chicharo, and E. Dutkiewicz. Unfairness and Capture Behaviour in 802.11 Ad-Hoc Networks. In *Proceedings of IEEE International Conference on Communications*, 2000.

[129] Zigbee wireless communication. http://www.zigbee.org/.

[130] H. Wu, Y. Peng, K. Long, S. Cheng, and J. Ma. Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysis and Enhancement. In *Proc. of IEEE INFOCOM*, Nevada, USA, June 2002.

[131] K. Xu, M. Gerla, and S. Bae. Effectiveness of RTS/CTS handshake in IEEE 802.11 based adhoc networks. *Ad Hoc Network Journal , Elsevier Science*, 1(1), 2003.

[132] Y. Xu, J. Heidemann, and D. Estrin. Geographically-informed Energy Conservation for Ad Hoc Routing. In *Proc. of ACM Mobicom*, July 2001.

[133] X. Yang and N. Vaidya. On the Physical Carrier Sense in Wireless Ad-hoc Networks. In *Proceedings of IEEE INFOCOM 2005*, Miami, Florida, March 2005.

[134] M. Yarvis, W. Conner, L. Krishnamurthy, J. Chhabra, B. Elliott, and A. Mainwaring. Real-World Experiences with an Interactive Ad Hoc Sensor Network. In *Proc. of the International Workshop on Ad Hoc Networking*, August 2002.

[135] F. Ye, S. Yi, and B. Sikdar. Improving Spatial Reuse of IEEE 802.11 Based Ad Hoc Networks. In *Proceedings of IEEE GLOBECOM*, San Francisco, California, December 2003.

[136] W. Ye, J. Heidemann, and D. Estrin. An Energy Efficient MAC Protocol for Wireless Sensor Networks. In *Proc. of Infocom*, June 2002.

[137] S. Yi, Y. Pei, and S. Kalyanaraman. On the Capacity Improvement of Ad Hoc Wireless Networks Using Directional Antennas. In *Proceedings of MobiHhoc '03*, Annapolis, Maryland, USA, June 2003.

[138] J. Yoon, M. Liu, and B. Noble. Random Waypoint Considered Harmful. In *Proc. of IEEE Infocom*, April 2003.

[139] J. Zhu, X. Guo, L. Yang, and W. Conner. Leveraging Spatial Reuse in 802.11 Mesh Networks with Enhanced Physical Carrier Sensing. In *Proceedings of IEEE International Conference on Communications (ICC04)*, Paris, France, June 2004.