I, HRISHIKESH GOSSAIN, hereby submit this work as part of the requirements for the degree of:

DOCTOR OF PHILOSOPHY

in:

COMPUTER SCIENCE

It is entitled:

POWER CONTROL AND SPATIAL REUSABILITY IN MOBILE AD-HOC NETWORKS

This work and its defense approved by:

Chair: DR. DHARMA P. AGRAWAL

DR. JAMES CAFFERY

DR. YIMING HU

DR. YIZONG CHENG

DR. JINTAI DING
Power Control and Spatial Reusability in Mobile Ad Hoc Networks

A dissertation submitted to
Division of Research and Advanced Studies
University of Cincinnati

In partial fulfillment of the requirements of degree of

DOCTORATE OF PHILOSOPHY (Ph.D.)
in the Department of Electrical and Computer Engineering and
Computer Science
College of Engineering

2005

by

Hrishikesh Gossain

B.E., Motilal Nehru R.E.C., India, 1998
M.S., University of Cincinnati, 2002

Thesis Advisor and Committee Chair: Dr. Dharma P. Agrawal
ABSTRACT

In this dissertation, we focus on the issue of power control and spatial reusability in Mobile Ad Hoc Networks (MANETs). We introduce a novel Spatial Reuse MAC (SRM) protocol based on IEEE 802.11 which accomplishes spatial reuse by employing a combination of power control and a distributed transmission sneaking mechanism. Our MAC scheme provides an improved power efficiency and enhanced throughput as compared to existing schemes. We also focus on the spatial reusability by using directional antennas. Existing MAC protocols which have been designed under the omni-directional antenna assumptions are inadequate to fully exploit the benefits of directional antennas. Hence, the design of an efficient MAC protocol for directional antennas is an important issue and needs further investigation. We introduce a new MAC protocol for Directional Antennas (MDA) which exploits the benefits offered by such an environment. Through simulation work we show that MDA outperforms all exiting directional MAC protocols. We have also addressed directional routing issues in MANETs and propose an on-demand Directional Routing Protocol (DRP) which assumes a cross layer interaction between the routing and the MAC layers. The main features of DRP include an efficient route discovery mechanism, establishment and maintenance of directional routing and directional neighbor tables and a novel directional route recovery mechanism. A detailed study of issues related to routing in directional antenna systems is done and the behavior of different IEEE 802.11 system parameters in a multihop directional environment is also provided undertaken.
To my beloved parents,
I express my sincere gratitude to my advisor Dr. Dharma P. Agrawal for his guidance, support and patience during my entire research work. His helpful suggestion and pointers laid the foundation of my Ph.D. dissertation work.

I would also like to thank my committee members Dr. James Caffrey, Dr. Yiming Hu, Dr. Yizong Cheng, and Dr. Jintai Ding for their extremely helpful suggestions and comments. I would like to thank Department of Electrical and Computer Engineering and Computer Science (ECECS) for giving me the opportunity to continue my Ph.D.

I would like to thank my friends Carlos, Deepankar, Navaneet, and Binay for their guidance and showing me the right path academic or otherwise. I would also like to thank Kumar, Dave, Tarun, Nagesh, Roy Ashok, Vivek with whom I had the opportunity to work with. I am also greatly thankful to my lab members who made my stay in Cincinnati entertaining and fun.

Finally, I would like to thank my parents and brothers for their patience and support during my entire stay in Cincinnati.
# Table of Contents

1. Introduction ..................................................................................................................... 7  
   1.1 Introduction............................................................................................................... 7  
   1.2 Dissertation Organization ....................................................................................... 10 
2. IEEE 802.11 Standards for WLAN .............................................................................. 12  
   2.1 Introduction............................................................................................................. 12  
   2.2 IEEE 802.11 Architecture ....................................................................................... 14  
   2.3 IEEE 802.11 Physical Layer ................................................................................... 15  
   2.4 IEEE 802.11 Medium Access Control (MAC) Sublayer........................................ 16  
      2.4.1 Point Coordination Function (PCF) ................................................................. 17  
      2.4.2 Distributed Coordination Function (DCF)....................................................... 18 
3. Power Control and Spatial Reusability in IEEE 802.11 ............................................... 22  
   3.1 Introduction............................................................................................................. 22  
   3.2 Related Work .......................................................................................................... 24  
   3.3 Preliminaries ........................................................................................................... 28  
      3.3.1. Impact of Transmission Power Level on Receiver Interference Range .......... 30  
      3.3.2. Node Behavior in the IEEE 802.11 C-Zone ................................................... 31 
4. Spatial Reuse MAC (SRM) Protocol............................................................................ 34  
   4.1 Introduction............................................................................................................. 34  
   4.2 SRM Description .................................................................................................... 34  
      4.2.1. Node Behavior within the C-Zone.................................................................. 40  
      4.2.1. Sneaking Procedure ...................................................................................... 41  
      4.2.1.1 Sneaking in DT’s C-Zone ......................................................................... 41  
      4.2.1.2 Sneaking in DT’s Transmission Range..................................................... 43 
   4.3 Simulation Environment and Results...................................................................... 46  
      4.3.1 Simulation Topology ....................................................................................... 47  
      4.3.2 Simulation Results .......................................................................................... 48 
5. Directional Antenna Systems........................................................................................ 56  
   5.1 Introduction............................................................................................................. 56  
   5.2 Antenna Concepts ................................................................................................... 57  
   5.3 Evolution of Smart Antenna System for MANETs ................................................ 59  
   5.4 The Antenna Model ................................................................................................ 62 
6. Spatial Reusability using Directional Antennas ........................................................... 65  
   6.1 Introduction............................................................................................................. 65  
   6.2 Related Work .......................................................................................................... 66  
   6.3 The DMAC and CRM Protocols............................................................................. 69  
      6.3.1 The DMAC Protocol........................................................................................ 70  
      6.3.2 Problems with DMAC ..................................................................................... 71  
   6.4 The CRM Protocol.................................................................................................. 73  
      6.4.1 Problems with CRM ........................................................................................ 74 
7. Proposed MAC Protocol for Directional Antennas (MDA)......................................... 76  
   7.1 Introduction............................................................................................................. 76  
   7.2 Determination of Neighbors’ Location .................................................................... 77  
   7.3 The Diametrically Opposite Directional RTS and CTS ........................................ 79  
   7.4 The Enhanced Directional NAV (EDNAV)............................................................ 85  
      7.4.1 The DNAV in MDA ........................................................................................ 86
9.5.4 Route Recovery Mechanisms ................................................................. 153
  9.5.4.1 Location Tracking Mechanism ......................................................... 153
  9.5.4.2 Local route recovery ......................................................................... 154
  9.5.4.3 Zonal Route Recovery ................................................................. 157
9.6. Mobile Random Scenario ........................................................................ 158
10. Conclusion and Future Research Direction ............................................... 161
Bibliography ................................................................................................. 163
List of Figures

Figure 2.1 – Protocol stack in a wireless node ...................................................................... 13
Figure 2.2 – IEEE 802.11 modes of operation .................................................................... 15
Figure 2.3 – Access mechanisms in 802.11 ....................................................................... 17
Figure 2.4 – Contention Free Period Repetition interval in 802.11 ...................................... 17
Figure 2.5 – Hidden and Exposed Terminal Problem .......................................................... 19
Figure 2.6 – Virtual Carrier Sensing in 802.11 ................................................................ 20
Figure 3.1 – Channel spatial reusability in the SRM protocol .............................................. 30
Figure 3.2 – Node behavior in the transmission range and carrier sensing range ............... 32
Figure 4.1 - Channel spatial reusability in the SRM protocol .............................................. 36
Figure 4.2 – Channel spatial reusability in the SRM protocol (nodes within C-zone use SRM_EIFS for their NAVs) ......................................................... 43
Figure 4.3 – Flow Chart for SRM DT and ST Packet Transmission ......................................... 45
Figure 4.4 – Aggregate throughput and total data delivered per Joule for varying combination of packet sizes for chain topology (15 flows) ........................................ 50
Figure 4.5 – Aggregate throughput and total data delivered per Joule for varying node distances for chain topology (15 flows) .............................................................. 52
Figure 4.6 – Aggregate throughput for varying network load for chain topology (15 flows) .......................................................................................................................... 53
Figure 4.7 – Total data delivered per Joule for varying network load for chain topology (15 flows) .................................................................................................................. 53
Figure 4.8 – Aggregate throughput and total data delivered per Joule with increasing load (random topology) .................................................................................................. 55
Figure 4.9 – Aggregate throughput and total data delivered per Joule for different scenarios (random topology) ................................................................. 55
Figure 4.10 – Aggregate throughput and total data delivered per Joule for different packet sizes (random topology) ................................................................. 55
Figure 5.1 – Coverage range comparison of omni-directional and directional transmissions .......................................................................................................................... 58
Figure 5.2 – The antenna model .......................................................................................... 63
Figure 6.1 – Directional communication example .................................................................. 70
Figure 6.2 – Problems with CRM ..................................................................................... 75
Figure 7.1 – Coverage Range in DMAC, CRM and MDA, and RTS/CTS/DATA/ACK exchange in MDA ........................................................................................................ 80
Figure 7.2 – Algorithm to calculate the D and K values ....................................................... 83
Figure 7.3 – DNAV update procedure in MDA .................................................................. 86
Figure 7.4 – DNAV limitations and the DT table ................................................................. 89
Figure 7.5 – Linear topology evaluation .............................................................................. 95
Figure 7.6 – Absence of deafness ....................................................................................... 99
Figure 7.7 – Impact of persistent hearing of DATA ............................................................... 100
Figure 7.8 – Impact of deafness ......................................................................................... 101
Figure 7.9 – Spatial reuse gain in random topology ............................................................. 104
Figure 7.10 – Average end to end packet delay ................................................................. 104
Figure 7.11 – Energy consumption of overall system .......................................................... 109
List of Tables

Table 4.1 – Number of flows for various distances and scenarios ........................................ 48
Table 9.1 - Antenna Beams to be scanned for local route recovery .................................. 146
Table 9.2 - Efficiency of Direction Estimation..................................................................... 149
1. Introduction

1.1 Introduction

Recent years have seen a tremendous growth in the demand of wireless technologies. The driving force for such a growth is the anytime, anywhere service, possible only with wireless. The advances in VLSI has now made possible to build a high-speed wireless system which are not only cheap but also very easy to install and operate.

However, unlike their wired counterpart, wireless is a broadcast medium and multiple devices can access the medium at the same time. If multiple transmissions are done at the same time, it may result into garbled data (called collision) at a receiving node, making communication impossible for any of the participating nodes. To prevent this from happening, a Medium Access Control (MAC) moderates the wireless access of channel [1,2]. The primary function of MAC is to define a set of rules; which allows devices to communicate in an orderly and efficient manner. Hence MAC protocols play a crucial role in efficient and fair access of wireless medium for different users.

Traditionally wireless networking has being used for cellular telephony [3, 4]. Internet connectivity through radio modems has also being an important application. These systems either provides single hop connectivity to a fixed wired base station or to a wireless device, which is connected to Internet through wired link. However there is a
recent interest towards a more decentralized method of wireless channel access. Such an example is the IEEE 802.11 medium access control (MAC) [1] protocol. It supports a peer to peer interaction between the nodes, and a network can be formed on demand without the assistance of any central authority. These networks are known as a Mobile Ad-Hoc Networks (MANETs) [4]. They offer many benefits compared to traditional centralized system; battlefield applications, disaster recovery are among few. These networks do not need installation of expensive base station and nodes can communicate directly with their neighbors without going through a base station, saving energy and improving throughput [9, 10, 11]. Hence there is a recent trend towards integrating MANETs to cellular systems to increase the coverage and capacity of a cell.

However, in MANETs, nodes are generally powered by batteries, which have limited lifetime. It makes the power consumption of the system a major issue. Also due to dynamic and decentralized access of the wireless medium, the available bandwidth to the end users is far below than what a channel can support. For example, existing IEEE 802.11 based standard can support up to 54Mbps (802.11g) of data traffic, although actual available bandwidth is far below than that. This is mainly because of the overhead involved in control packets, and increased chances of collision in wireless medium. One way to increase the throughput of the channel is to use some kind of spatial reusability concept, wherein more than one transmission is possible within a transmission zone. In this first part of our thesis work, we will show that power control and spatial reusability in a MANET are closely related and it is possible to improve on them by designing an intelligent MAC scheme. We introduce a novel Spatial Reuse MAC (SRM) based on IEEE 802.11 which accomplishes spatial reuse by employing a combination of power
control and a distributed transmission sneaking mechanism. Our MAC scheme provides an improved power efficiency and throughput than any of the existing approaches. This part of our thesis is designed assuming omni-directional nature of transmission among the nodes.

In the second part of our thesis work, we will focus on the spatial reusability by using directional antennas [5]. The chief contributor to the capacity limitation in IEEE 802.11 based system is the omni-directional nature of the transmission. For example, the distribution of energy in all directions other than the direction of recipient not only generates unnecessary interference to other nodes, but also decreases the range of their transmissions. With directional communications, on the other hand, both range and spatial reuse can be substantially enhanced, by having nodes concentrate transmitted energy only towards their destinations’ direction. On the receiving side, directional antennas enable a node to selectively receive signals only from certain desired direction, thereby increasing the signal to interference and noise ratio (SINR).

Traditional MAC protocols which have been designed under the omni-directional assumption [1, 6] are no longer suitable to use over directional antennas, since they can no longer exploit the benefits offered by directional antennas. Hence, the design of an efficient MAC protocol for directional antennas is a crucial issue and needs further investigation. We introduce a new MAC protocol for Directional Antennas (MDA) which very efficiently exploits the benefit offered by directional antenna. Through simulation work we show that MDA outperforms all exiting directional MAC protocols in the majority of scenarios. In addition, we show that MDA effectively addresses the various issues raised by the use of directional antennas over ad hoc networks.
Next, we address directional routing issues in MANETs. Although there is plethora of literature for designing efficient directional MAC schemes, a complete design of a routing protocol tuned to the underlying directional environment has mostly remained unexplored. Existing directional routing schemes either assume a complete network topology beforehand or simply use omnidirectional routing protocols to forward packets in underlying directional environment. Here we argue that a routing protocol specifically tuned to the underlying MAC layer can reap interesting performance benefits. For example, in a directional routing protocol, a source node can exploit the antenna beam information towards its destination for an efficient route recovery. Hence we propose a Directional Routing Protocol (DRP) for MANETs. DRP is an on-demand directional routing protocol which assumes a cross layer interaction between routing and MAC layer and is inspired by Dynamic Source Routing (DSR) protocol. The main features of DRP include an efficient route discovery mechanism, establishment and maintenance of directional routing and directional neighbor tables (DRT and DNT respectively) and novel directional route recovery mechanisms. A detailed study of issues related to routing in directional antenna systems. We also outline the behavior of different IEEE 802.11 system parameters in a multihop directional environment.

1.2 Dissertation Organization

This dissertation is organized as follows. We will start with giving an overview of IEEE 802.11 Medium Access Control (MAC) mechanism in Chapter 2. We will elaborate on the different issues existing in IEEE 802.11 MAC and also outline some of the ongoing work in IEEE 802.11 working group. In Chapter 3, we will address the issue of power
control and spatial reusability in 802.11. We start with first giving a background on power control over IEEE 802.11 and then give a detailed description of the issues relevant to power control, describe the related work in this area and their limitations. Chapter 4 describes our proposed SRM protocol and provides a detailed simulation result to show benefits of SRM over existing MAC schemes. In the next part of our proposal we focus on the issues of spatial reusability using directional antennas. We start with first giving a background on present antenna systems for wireless networks in Chapter 5. In Chapter 6 we describe the existing work in the area of designing a MAC protocol for directional antennas. In this chapter we will also outline the antenna model used in our directional MAC scheme. Then in Chapter 7, we introduce MDA protocol and through extensive simulation work show how MDA outperforms existing schemes. In Chapter 8 we describe methods to handle deafness in directional antennas and handling “self induced blocking problem” (described in later section). Chapter 9 describes our Directional Routing Protocol (DRP) and provides a comparison of DRP with DSR running over omni and directional antenna systems. We conclude this dissertation in Chapter 10 outlining some of the future research directions in power control and directional antennas systems.
2. **IEEE 802.11 Standards for WLAN**

### 2.1 Introduction

Wireless local area network (WLAN) [1, 7, 8, 10, 11] constitutes a fast growing area introducing the flexibility of wireless access into office, home and production environments [7]. The main goal of WLANs is to replace cabling in office environments and introduce a higher flexibility for ad hoc communications. The IEEE standard 802.11 specifies the family of WLANs in which many products are already in the market. As the number in the standard indicates, the standards belong to the family of 802.x LAN standards, e.g. 802.3 Ethernet or 802.5 Token Ring.

However WLANs have fundamental characteristics that make them different than traditional wired LANs. For example, in a wired LAN, an address is equivalent to a physical location whereas in WLAN an address is a message destination, and because of mobility of the nodes, it may not be a fixed location. Wireless medium is a broadcast and much more error prone than a guided wired cable, hence proper arbitration of the wireless channel is needed. A WLAN Medium Access Control (MAC) layer is designed considering above characteristics of wireless medium. The MAC layer should be able to operate with multiple physical layers, each of which can exhibit different transmission characteristics; also it should be able to provide a unified interface to higher layers.
A pictorial view of the mobile ad hoc nodes’ MAC layer in TCP/IP protocol stack is shown in Figure 2.1. A closer look at the TCP/IP stack reveals that Data Link Layer in a wireless node is now divided into two sublayers: MAC and Logical Link Control (LLC). MAC layer lies below the Logical Link Control (LLC) to arbitrate the wireless medium. It should be noted that we still need a LLC to provide an error-free packet to higher layer and physical layer to provide a bit pipe.

While discussing the arbitration of multi-access wireless link by MAC layer, there are two extreme strategies which can be developed [2]. First is termed as “free-for-all”, in which nodes normally send new packets immediately, hoping for no interference from other nodes. Still a designer has to develop the methods of retransmission in case collision occurs. The other extreme is the “perfectly scheduled” approach in which there is some order (e.g. round robin), in which nodes can access the channel. However this kind of scheme needs a central controller to decide the scheduling strategy, duration of interval and how the nodes are informed about their turns.

To handle the issue of multi-access communication in wireless local area networks, IEEE formed the working group (WG) 802.11 in 1990s. By the end of 1997, the WG finalized the initial draft of the standard for wireless LANs. The draft covers the lower two layers
of TCP/IP protocol stack [1, 10, 11]: physical layer and MAC sublayer. Initial draft specified a 2.4 GHz operating frequency with data rates of 1 and 2Mbps. With popularity of 802.11 based WLANs, WG decided to enhance the basic standard to support different services and accordingly they form separate working group within 802.11 umbrella to handle each of such issues.

2.2 IEEE 802.11 Architecture

IEEE 802.11 networks can exhibit two different basic system architectures as shown in Figure 2.2, namely infrastructure-based mode and ad hoc mode. Figure 2.2(a) and Figure 2.2(b) shows the different components in an infrastructure-based and ad hoc mode of IEEE 802.11 architecture. Nodes are generally termed as stations (STA) and nodes within the radio range of each other forms a Basic Service Set (BSS). If the BSS does not contain any Access Point (AP) and there is a peer to peer interaction among the nodes, the ad hoc mode is formed and is shown in Figure 2.2(a). On the other hand if BSS do have an AP it is termed as infrastructure-mode. Multiple BSSs may be connected to backbone through wired link forming an Extended Service Set (ESS), as shown in Figure 2.2(b). An IEEE 802.11 node can work in any of these modes.
Given this basic overview of the basic architecture of IEEE 802.11 network, in the following section we will elaborate on the physical and MAC layer specification in 802.11.

2.3 IEEE 802.11 Physical Layer

The initial draft of IEEE 802.11 [1, 10], defined three different physical layers supported by MAC: infrared (IR), frequency hoping spread spectrum (FHSS), and direct sequence spread spectrum (DSSS).

The FHSS utilizes the 2.4 GHz industrial, scientific, and medical (ISM) band (i.e., 2.4000 – 2.4835 GHz). In United States, it can support up to 79 channels, where the first channel has a center frequency of 2.402 GHz, and all subsequent channels are placed 1 MHz apart which is mandated by Federal Communications Commission (FCC) for ISM band. Three different hoping sequences are established with 26 hoping sequence per set. This enables
different BSS to coexist in the same geographical area, and alleviates congestion and maximizes throughput. The maximum hoping rate permitted was 2.5 hops/s.

The DSSS also uses the 2.4 GHz ISM frequency band, where the basic rate of 1 Mbps is encoded with Differential Binary Phase Shift Keying (DBPSK), and a 2 Mbps enhanced rate uses differential Quadrature Phase Shift Keying (DQPSK). The spreading is done by dividing the available bandwidth into 11 channels, each 11 MHz wide, and using an 11-chip Barker sequence to spread each data symbol.

The IR specification identifies a wavelength range from 850 to 950 nm. The IR band is designed for indoor use only, and enables stations to receive line-of-site transmission.

2.4 IEEE 802.11 Medium Access Control (MAC) Sublayer

The responsibility of a MAC protocol is the arbitration of accesses to a shared medium among several end systems. In IEEE 802.11 this is carried out via an Ethernet-like [12] stochastic and distributed mechanism: Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) [13]. The medium can alternate between a contention period (CP), which requires all nodes to contend to access the channel, and a contention free period (CFP), which uses a controlled or mediated channel access by Access Point (AP), thereby eliminating the need for nodes to contend for channel access (Figure 2.3). IEEE 802.11 specifies two medium access control protocols, Point Coordination Function (PCF) and Distributed Coordination Function (DCF).
PCF is based on polling controlled by an AP. DCF on the other hand, supports best effort packet delivery. DCF is designed for asynchronous data transport, where users with data to transmit have an equally fair chance of accessing the channel.

**2.4.1 Point Coordination Function (PCF)**

PCF is an optional capability, which provides a contention free, connection-oriented frame transfer. It relies on a PC to perform polling. Generally the function of PC is
performed by an AP within each BSS. Nodes within the BSS which are capable of operating in CFP are termed as CF-aware nodes.

PCF is required to co-exist with the DCF and logically sits on top of the DCF (Figure 2.3). CFP repetition interval is used to determine the frequency with which the PCF interval occurs. Within a repetition interval, a portion of the time is allocated to contention-based traffic and the remainder for contention free traffic as shown in Figure 2.4. While DCF is studied for several researchers, the combined performance of DCF and PCF operating in a common repetition interval is much less understood. Generally 802.11 based ad hoc networks uses DCF as a channel access mechanism. In the following subsection we will elaborate more on DCF.

### 2.4.2 Distributed Coordination Function (DCF)

The DCF is based on carrier sense multiple access with collision avoidance (CSMA/CA). Since a node will not be able to listen to the channel while transmitting, CSMA/CD (collision detection) as in Ethernet is not used. IEEE 802.11 based network suffer from hidden terminal problem. To illustrate, if node X wants to send packet to node Y, and node Z also has a packet to be sent to Y, if the duration of X’s and Z’s data transmission time overlap, it will result into a collision at Y. To prevent it from happening, IEEE 802.11 suggests a mechanism of Request to Send (RTS) and Clear to Send (CTS) handshake. RTS/CTS packets include the duration information of an ongoing transmission and both sender (by RTS) and receiver (by CTS) reserve the channel before actual DATA transmission. It prevents any other node to transmit their packet for the entire duration of the ongoing transmission in their neighborhood. This is also termed as
a virtual carrier sensing. All adjacent nodes maintain a data structure Network Allocation Vector (NAV) to store this duration information. It is in addition to the physical layer carrier sensing done at the lower layer.

![Diagram of RTS/CTS Transmission](image)

Figure 2.5 – Hidden and Exposed Terminal Problem

The importance of RTS/CTS can be better explained by Figure 2.5, where node S wants to send packet to node R, where as node B has a packet to send R. Without RTS/CTS, if the duration of S’s and B’s data transmission time overlaps, it will result into a collision at R. To avoid this from happening, nodes first reserve the channel through RTS/CTS handshake as shown in Figure 2.5. This prevents node B from sending its DATA for the entire duration of R’s transmission. It should be noted that although RTS/CTS solves the problem of hidden terminal problem, it does not solves the problem of exposed terminal. For example, if we assume an ongoing transmission form S to A, and assuming that node R, has already set its NAV based on RTS received from S, if it received an RTS from node B, it is not going to reply back with a CTS, since its NAV is set, even though its CTS may not collide with data reception at A.

Figure 2.6 gives an example on how nodes within the transmission range set their NAVs during RTS-CTS-DATA-ACK transmission. SIFS, DIFS, and EIFS are interframe spaces
(IFSs) specified by IEEE 802.11. IEEE 802.11 defines four IFSs, namely, SIFS (short interframe space), PIFS (PCF interframe space), DIFS (DCF interframe space), and EIFS (extended interframe space). Basically, IFSs provide priority levels for channel access. The SIFS is the shortest of the interframe spaces and is used after RTS, CTS, and DATA frames to give the highest priority to CTS, DATA and ACK, respectively. In DCF, a node waits for the DIFS duration before transmitting any packet whenever the channel is found idle.

The IEEE 802.11 MAC protocol uses a backoff mechanism to resolve channel contention. Before initiating a transmission, a node S does both virtual (NAV) and physical carrier sensing. If NAV is not set, and the channel is sensed idle, the node defers for DIFS period before sending its packet. If the channel is found busy (by carrier sensing), the node S chooses a random backoff interval from \([0, \text{CW}]\), where \(\text{CW}\) is called contention window. After every idle “slot time”, node S decrements the backoff counter by one. When it reaches zero, node S can transmit the packet. In case collision occurs with some other transmission, S doubles its CW, chooses a new backoff interval and tries retransmission again once the backoff timer expires. If during the backoff stage the medium is sensed busy, the node freezes its backoff and resumes it once the medium

**Figure 2.6 – Virtual Carrier Sensing in 802.11**
has become idle for a duration called DIFS. The backoff procedure is only invoked when the medium has been sensed idle for DIFS duration.
3. Power Control and Spatial Reusability in IEEE 802.11

3.1 Introduction

Power control is a determinant technique for energy conservation and thus is of fundamental importance to wireless ad hoc stations which primarily rely on limited battery power. Besides energy saving, power control can also increase the capacity of the network by enhancing spatial reuse of the wireless channel. Current research on power control by appropriate medium access control (MAC) focus on suitably varying transmit power in order to reduce energy consumption [14, 15, 16, 17, 18, 19, 20], while there are no specific mechanisms to make an efficient and coordinated reuse of additional channel capacity. Existing solutions either block the entire station’s radio range [20], similar to the IEEE standard 802.11 [1], so as to prevent collisions, or simply do not address the spatial reuse capability, thus resulting in a relatively high number of collisions, degraded network performance, and quite often higher energy consumption than IEEE 802.11 without power control [14, 17, 20, 21, 22].

Various strategies for achieving power control can be classified based upon the presence of symmetric or asymmetric links between nodes. In the context of IEEE 802.11 networks, link symmetry is assumed in its design while communication in asymmetric
networks has been shown to be a relatively hard task [23, 24]. A simple protocol for power control over IEEE 802.11 has been suggested that is based on the RTS-CTS exchange [14, 17, 21, 22]. To alleviate the problem of link asymmetry, RTS and CTS are transmitted at the highest power level whereas DATA and ACK use the minimum power level needed for communication between the nodes and is referred to as the BASIC scheme [20]. It has been shown that the BASIC scheme has many underlying deficiencies, and an improved protocol called Power Control MAC (PCM) has been introduced [20]. PCM periodically [20] increases the transmit power during DATA transmission so as to overcome major limitations such as increased number of collisions and retransmissions, higher energy consumption, and throughput degradation. However, all of these schemes fail to explore spatial channel reuse to its maximum possible potential as either the entire radio range as in PCM is blocked, or stations access the shared medium without any coordination and thus increasing the number of collisions and energy consumption.

In this chapter we introduce a novel Spatial Reuse MAC (SRM) based on IEEE 802.11 which explores spatial reuse by employing a combination of power control and a distributed transmission sneaking mechanism. SRM follows the approach of the BASIC scheme for RTS-CTS and DATA-ACK exchanges while suitably managing the IEEE 802.11 network allocation vector (NAV) so as to overcome deficiencies of the BASIC protocol. In order to accomplish wireless channel spatial reuse, we introduce a technique of transmission sneaking whereby a pair of nodes in the neighborhood of an ongoing transmission can communicate if they have the knowledge that their transmission is not going to collide with any of the ongoing transmissions. SRM is observed to improve
throughput as compared to PCM and IEEE 802.11 while significantly increasing the energy saving.

In the next section we are going to describe the existing IEEE 802.11-based power control schemes and their shortcomings. In next chapter we will presents our proposed SRM protocol in detail.

### 3.2 Related Work

A scheme with power control has been introduced in [21, 22] and is based on the RTS-CTS handshake implementation of the IEEE 802.11 MAC protocol. Basically, the technique in [22] mandates the transmitted RTS to contain the current power level employed by the sender in its transmission and allows the receiver to include its desired transmit power level in the corresponding CTS back to the sender. This enables the transmitter and receiver nodes to assist each other in selecting transmit power and conduct DATA-ACK transmission with minimum necessary power levels. A variation of this scheme is to transmit RTS and CTS at the maximum power level, while DATA and ACK packets could be transmitted at a lower power level [17]. As mentioned earlier, this is referred to as BASIC scheme and has been shown to have significant shortcomings [20]. More specifically, this scheme incurs an increased number of collisions and retransmissions, and frequently consumes more energy than the regular IEEE 802.11 without power control.

To address the shortcomings of the BASIC scheme, a power control MAC (PCM) is proposed in [20]. Similar to the BASIC scheme, PCM transmits the RTS and CTS at the maximum power level. However, the transmitter in PCM periodically increases the
transmit power during DATA-ACK transmission so as to indicate all nodes in the sender stations’ radio range that the channel still remains busy. This prevents collisions with the ongoing transmission while accomplishing energy saving. The PCM protocol is shown to achieve throughput comparable to IEEE 802.11 while improving on energy consumption. However, PCM block entire transmission range and hence does not provide any improved on spatial reusability.

Power-aware routing optimization (PARO) [17] employs the BASIC scheme as a power control MAC protocol by finding routes that consumes low energy. Many other routing metrics have also been proposed [25, 26]. Another power control proposal similar to the BASIC scheme can be found in [14]. A node in this scheme builds a table with the minimum transmit power level required to communicate with its neighbor, which can be changed dynamically. But different power levels amongst nodes results in asymmetric links and, thus, raises the number of collisions.

A mechanism to determine the transmit power according to the packet size has been proposed in [15, 16]. The rationale being any reduction in transmission power may result in energy saving, but it could also add to errors. Therefore, this protocol selects a suitable power level based on the packet size. The higher is the bit error rate, larger is the number of retransmissions required, hence increasing overall energy consumption. Additionally, an adaptive scheme to choose the MAC frame size based on channel conditions is given in [27]. Fairness issues in IEEE 802.11 are also of paramount importance [28, 29] as nodes which use lower transmission power than their neighbors may have difficulty in accessing the medium. A scheme to improve fairness is presented in [30].
To ensure the presence of symmetric links, COMPOW (Common Power) [24] selects a common power level for all nodes in the network. The power level to be used is the smallest power level which achieves the same level of network connectivity as the highest power level. MACA-P [31] proposed a set of enhancements to the 802.11 DCF that allows parallel transmissions in many situations when two neighboring nodes are either both receivers or both transmitters, but a receiver and a transmitter are not neighbors. Like 802.11, MACA-P contains a contention-based reservation phase prior to data transmission. However, the data transmission is delayed by a control phase interval, which allows multiple sender-receiver pairs to synchronize their data transfers, thereby avoiding collisions and improving system throughput.

One control channel and multiple data channels are employed in the power control protocol proposed in [32], where the control channel is used to assign data channels to nodes. Regular RTS, CTS, a special RES packet, and broadcast packets are transmitted with the highest transmit power through the control channel. Source and destination nodes use RTS-CTS exchange to decide which channel and what power level to use for data transmissions. Upon the reception of the CTS, the RES packet is sent by the source to the destination node in order to reserve a data channel for communication. DATA and ACK transmissions take place in the reserved data channel with the power level negotiated by the RTS-CTS exchange.

The power controlled multiple access (PCMA) protocol [33] enables different nodes to possess different transmission power levels, where the transmit power can be changed on a per-packet basis. Altogether PCMA employs two channels, one for busy tones and the other for all other packets. Busy tones are used instead of the RTS-CTS packets to
overcome the hidden terminal problem. During the time a node is receiving DATA, it periodically sends a busy tone. The signal strength of busy tones received by a node is used to determine the highest power level at which this node may transmit without interfering with other ongoing transmissions. Therefore, a separate channel is needed. The concept of busy tones with two distinct channels is also utilized in [25, 34, 35, 36]. Power control is also used for the purpose of topology control in [37, 38, 39, 40], and has also been investigated as a means to establish energy efficient spanning trees for multicasting and broadcasting [18, 19].

Finally, the issue of spatial reusability in IEEE 802.11 has been considered in [41], where a protocol named as Interference Aware MAC (IA-MAC) has been proposed. IA-MAC modifies the CTS packet header so as to include information on the signal to interference and noise ratio (SINR) and on the power level at which a RTS is received, so that neighboring nodes overhearing the RTS/CTS handshake can eventually attempt a concurrent transmission. However, there are a few drawbacks with this approach. Firstly, it does not take power control into consideration which limits the gains of the protocol and also does not improve on energy efficiency. Secondly, by modifying the CTS packet header makes IA-MAC incompatible with the standard IEEE 802.11 MAC. Thirdly, IA-MAC only handles the case when nodes can successfully understand (i.e., decode) the RTS/CTS packets, while those nodes which can sense the packet but can not decode (see next section) have not been taken into account.
3.3 Preliminaries

In this work, we consider the IEEE 802.11 DCF access method. We define the terms transmission range, carrier sensing range, interfering range, carrier-sensing zone (C-Zone) and sneaking zone (S-Zone) which are used extensively throughout this paper. In the following description we assume A as the source and B as the recipient of an ongoing transmission.

**Transmission range:** This represents the range within which a packet can be successfully received, provided there is no interference from other nodes.

**Carrier-sensing range:** The range within which a transmission can be detected is termed as carrier-sensing range. This is always larger than the transmission range, and may be more than two times the size of the transmission range [28, 29, 30]. In our simulations we set the transmission range and carrier sensing range as 250 meters and 550 meters respectively when utilizing the highest power level. It is to be noted that different power levels result in different sizes for the transmission and carrier-sensing ranges. In addition, we define the *Carrier-sensing Zone (C-Zone)* [7] as the area where a signal can be detected, but cannot be decoded.

**Interfering range:** This represents the range within which a node in receiving mode can be interfered by another transmission. Interfering range may vary depending upon the distance between A and B, the power at which the packet is transmitted, and the number of transmission going on in the neighborhood.

**Sneaking Zone (S-Zone):** Assuming that nodes A and B transmit RTS-CTS at full power ($p_{\text{max}}$) and DATA-ACK at $p_{\text{desired}}$ ($p_{\text{desired}}$ is defined as the minimum power needed for a
successful communication between two nodes), we define the S-Zone as the area within the carrier sensing range of RTS-CTS, where a transmission (called sneaking transmissions or STs) is possible without interfering with A-B’s transmission. It should be noted that this area is generally blocked in IEEE 802.11 because all the packets are transmitted at full power. In SRM, transmissions starting with RTS-CTS handshake (e.g., between A and B), are termed as dominating transmissions (DTs). The ST is done without RTS-CTS handshake. However in both the case DATA and ACK are sent at $p_{desired}$. Nodes involved in DT and ST are termed as Dominating Nodes (DNs) and Sneaking Nodes (SNs) respectively.

Figure 3.1 illustrates the C-Zone and S-Zone for A’s RTS and DATA transmissions. It should be noted that the size of S-zone may be larger than C-Zone as it may also include a part of RTS-CTS transmission range, which becomes free because of the low power DATA-ACK transmission (which reduces the size of carrier sensing range).
3.3.1. Impact of Transmission Power Level on Receiver Interference Range

It is necessary to understand the relationship between transmission power and corresponding interfering range at a receiver. For a given transmission power, ignoring the multipath fading and shadowing (assuming they are minor factors in open space environment), the receiving power is mostly decided by the distance between the transmitter and receiver. There are different propagation model available to model this
loss, which largely depends on the distance $d$ between the transmitter and receiver. Let us assume a communication between two nodes A and B, where B is the receiving node at a distance $d_{AB}$ of the transmitter node A and there is an interfering node C at a distance $d_{CB}$ from B. Assuming that interference is contributed by C only, the signal to interference and noise ratio (SINR) equation at B can be simplified as [90]:

$$\text{SINR}_B = \frac{P_{t-AB}}{P_{t-CB}} \left( \frac{d_{CB}}{d_{AB}} \right)^4 \geq \text{SINR } _{\text{THRESHOLD}} \quad (1)$$

where $P_{t-AB}$ and $P_{t-CB}$ are the transmission power of node A and C respectively. Initially, let us fix the value of $P_{t-CB}$ and analyze the effect of change of $P_{t-AB}$ (the case when $P_{t-AB}$ is same as $P_{t-CB}$ has been studied in [92]). When node A starts its DATA transmission at $P_{t-AB} = p_{\text{desired}}$ to node B, node C, which is now out of C-Zone (Figure 3.1) of node A’s DATA transmission, after waiting for EIFS (defined in next section) period, initiates a RTS transmission which, as we know, is transmitted at full power (i.e., $p_{\text{max}}$). As a result, this RTS transmission from C will increase the overall interference level, decrease the SINR at B, and hence may compromise its packet reception. Thus, nodes in the neighborhood of A-B should refrain from transmitting the RTS-CTS at full power (as done in the BASIC scheme). Rather, they should select $P_{t-CB}$ so that its effect on the SINR at node B is minimal. Given all this, in SRM the sneaking transmission is not preceded by RTS/CTS.

### 3.3.2. Node Behavior in the IEEE 802.11 C-Zone

The DCF in IEEE 802.11 performs two forms of carrier sensing: physical (by listening to the wireless shared medium) and virtual. Virtual carrier sensing employs the duration
field which is included in the MAC frames. Using the duration information, nodes update their Network Allocation Vector (NAV) whenever they receive a packet. The channel is considered to be busy if either physical or virtual carrier sensing (by the NAV) so indicates.

Figure 3.2 gives an example on how nodes within the transmission range and C-Zone adjust their NAVs during RTS-CTS-DATA-ACK transmission. IEEE 802.11 defines four IFSs, namely, SIFS (short interframe space), PIFS (PCF inter frame space), DIFS (DCF interframe space), and EIFS (extended interframe space). Basically, IFSs provide priority levels for channel access.

![Diagram](image)

**Figure 3.2 – Node behavior in the transmission range and carrier sensing range**

In Figure 3.2, nodes in transmission range correctly set their NAVs when receiving RTS or CTS. However, since nodes in the C-Zone cannot decode the packet, they do not know the duration of the packet transmission. To prevent a collision with the ACK reception at the source node, nodes within the C-Zone set their NAVs for the EIFS duration. The
The main purpose of the EIFS is to provide enough time for a source node to receive the ACK frame, so the duration of EIFS is longer than that of an ACK transmission. As per IEEE 802.11, the EIFS is obtained using the SIFS, the DIFS, and the length of time to transmit an ACK frame at the physical layer’s lowest mandatory rate, and is given by [1]:

$$\text{EIFS} = \text{SIFS} + \text{DIFS} + \left(8 \times \text{ACKsize}\right) + \text{PreambleLength} + \text{PLCPHeaderLength}/\text{BitRate},$$

where ACKsize is the length (in bytes) of an ACK frame, BitRate is the physical layer’s lowest mandatory rate, PreambleLength is 144 bits, and PLCPHeaderLength is 48 bits.
4. Spatial Reuse MAC (SRM) Protocol

4.1 Introduction

Our proposed Spatial Reuse MAC (SRM) protocol is similar to the BASIC scheme in that it transmits RTS and CTS at $p_{\text{max}}$, and DATA and ACK at $p_{\text{desired}}$. However, contrary to the BASIC scheme that does not have any mechanism to coordinate spatial reuse of the channel capacity during the low power DATA-ACK transmission, SRM implements a fully distributed transmission sneaking technique so as to enable channel spatial reuse, which is accomplished without the need for a separate channel. SRM appropriately adjusts the EIFS period of those stations within the I-zone to overcome the drawbacks of the BASIC scheme, and at the same time prevent blocking of the entire interfering range as in PCM.

4.2 SRM Description

To illustrate the overall idea of SRM, let us consider Figure 4.1 where node A transmits a RTS to node B which, in turn, sends a CTS back to A. These transmissions are carried out at $p_{\text{max}}$, while the DATA-ACK are transmitted at $p_{\text{desired}}$. Figure 4.1 depicts the various ranges and zones of the RTS-CTS and DATA-ACK transmission between nodes.
A and B. At this point, let us define what are Dominating Transmission and Sneaking Transmission.

- **Dominating Transmission (DT):** Whenever a pair of nodes successfully completes the RTS-CTS handshake before a DATA-ACK transmission, we refer to this as the Dominating Transmission (DT). For example, nodes A and B in Figure 4.1 have successfully completed RTS-CTS handshake and together with the oncoming DATA-ACK transmission, it is called as the Dominating Transmission as it reserved the channel through a RTS-CTS handshake. Nodes A and B are called Dominating Nodes (DNs) of DT.

- **Sneaking Transmission (ST):** From Figure 4.1, we see that the pair of nodes C, D and E, F could eventually communicate with each other if they had the knowledge of the minimum power level required to communicate. In this case, however, these pair of nodes cannot use RTS-CTS at $p_{\text{max}}$ as they would collide with the current dominating transmission between A and B. The IEEE 802.11 standard allows nodes to communicate without using RTS-CTS [1] when the amount of data to be sent is less than the threshold $RTSThresh$. SRM utilizes this ability to directly transmit DATA without RTS-CTS in order to allow nodes C and D, E and F to communicate at low power despite the ongoing DT between nodes A and B. We define this transmission as Sneaking Transmission (ST), and the nodes involved as Sneaking Transmitter and Sneaking Receiver. As explained next, SRM permits nodes to sneak the medium provided the ST does not collide with the DT.
In SRM, we assume that every node has access to a table with the minimum power level required to communicate with each of its neighbors [14]. There are several ways this can be achieved. One possible solution is to exchange hello packets between neighboring nodes either at the MAC or at the network layer. Since protocol efficiency is of a paramount importance in wireless networks and given that many routing protocols for ad hoc networks already employ a form of hello packets to maintain network connectivity [45, 46, 47, 48], we follow a cross-layer design in SRM with the network layer assisting the MAC layer in the determination of the various $p_{desired}$ amongst neighbor nodes (cross-layer solutions for wireless ad hoc networks are receiving great attention in several layers of the protocol stack [28]). Network layer hello packets are always transmitted as MAC layer broadcast, therefore always sent at $p_{max}$. Thus, whenever a node receives a broadcast packet, it calculates $p_{desired}$ based on the received power level, $p_r$, and the transmitted
power level, $p_{\text{max}}$, as: 

$$p_{\text{desired}} = \frac{p_{\text{max}}}{p_r} \times R_{\text{thresh}} \times c,$$

where $R_{\text{thresh}}$ is the minimum necessary received signal strength and $c$ is a constant [33] usually equal to 1. Note that by using this model we assume that signal attenuation between neighboring nodes is the same in both the directions, and is considered fairly reliable with a high probability [20]. Additionally, SRM builds on this assumption and employs the Received Signal Strength Indicator (RSSI) model to estimate the distance between the transmitter node A and the receiver B based on the power transmitted ($p_{\text{max}}$) and the power received ($p_r$) at B as:

$$d_{\text{estimated}}(p_{\text{max}}, p_r) = \begin{cases} 
\sqrt{\frac{p_{\text{max}} \times G_t \times G_r \times \left(\frac{3\times10^8}{4\pi f}\right)^2}{L \times p_r}} & \text{if } p_{\text{max}} \times G_t \times G_r \times \left(\frac{3\times10^8}{4\pi f}\right) \leq \left(\frac{4\pi f \times H_t \times H_r}{3\times10^8}\right) \\
\sqrt{\frac{p_{\text{max}} \times G_t \times G_r \times H_t^2 \times H_r^2}{L \times p_r}} & \text{otherwise}
\end{cases}$$

(1)

where $G_t$ and $G_r$ are the transmitter and receiver antenna gains, respectively, $f$ is the operating frequency band, $L$ is the system loss, and $H_t$ and $H_r$ are the transmitter and receiver antenna heights, respectively. This model can approximately determine the distance between two nodes [49]. In our simulations, we have used typical values of wireless nodes for these parameters [49], namely, $G_t = G_r = L = 1$, $H_t = H_r = 1.5$ meter, and $f$ being equal to the operating frequency of IEEE 802.11 (e.g., $f = 915$ MHz). Note that more accurate models than RSSI [50] could be used to estimate distance without any modification to SRM protocol. With equation (1), whenever a node receives either a broadcast or a RTS-CTS, it can determine its distance from the transmitter in question.
We now discuss the steps taken for a DT in SRM. Before sending a RTS packet, a sender node A calculates the minimum power level, say $p_{\text{recv-A}}$, it needs to correctly receive a packet. This is done based on node A’s current interference profile (generally, this power level is higher than the power level needed when there is no surrounding interference). Next, node A includes both $p_{\text{recv-A}}$ and the SINR at A in its RTS packet before transmission. Essentially, the value of $p_{\text{recv-A}}$ is calculated as follows:

$$P_{\text{recv-A}} = \text{SINR}_A \cdot P^A_i$$  \hspace{1cm} (2)

In equation (2), SINR$_A$ is the SINR at node A and $P_i$ is the corresponding interference. Upon receiving the RTS packet coming from node A, with help of NDT, node B first calculates $p_{\text{desired}}$ (the power level needed to send back the ACK packet to A). Next, node B calculates its own $p_{\text{recv-B}}$ (the minimum power needed at B to correctly receive a packet) and includes it together with the SINR at B in its CTS back to A. When node A received the CTS back from node B, it is important to node that its original estimate of $p_{\text{desired}}$ may now change given the SINR at node B. Basically, node A may have to increase its power level so as to achieve the desired signal quality at node B.

Once the DT is in place, we now turn the attention as to how the ST is performed in SRM. As outlined in Section 4.2, ST is performed by the nodes which are not able to capture the channel as a DT and are within the carrier sensing range of the DT. In SRM, nodes can only sneak the ongoing DT if they ensure that their ST will not collide at the DNs. For that, a potential sneaking node needs to determine the amplitude of its ST. In other words, nodes in the C-Zone need to estimate both the transmission range and carrier sensing range of their potential SN and make sure that the DNs are outside of this range. Here, we assume that if a node X is outside the carrier sensing range of a transmitter Y, it
is not going to be affected by any packet transmission from Y. Mathematically node D, in Figure 4.1, can sneak a packet at $p_{\text{desired}}$ to node C during the DT between nodes A and B iff:

\begin{enumerate}
\item $\text{distance}(p_{\text{desired}}, CThresh) < \text{distance}_{D,A}$ ; and
\item $\text{distance}(p_{\text{desired}}, CThresh) < \text{distance}_{D,B}$
\end{enumerate}

where $\text{distance}_{D,A}$, and $\text{distance}_{D,B}$ are the distances (in meters) between nodes D and A, D and B, respectively, and $CThresh$ is the minimum power level below which a signal cannot interfere with any potential ongoing reception, and is defined in the IEEE 802.11 specifications [1]. In other words, $CThresh$ can be used to determine the boundary of the carrier sensing range, the same way $RxThresh$ can be employed to determine the transmission range boundary. Therefore, if relations (i) and (ii) are satisfied, we can guarantee that a possible ST from D will not collide either with the receiver or with the transmitter of the DT. Node C also does a similar check before sending its ACK packet. Similarly from Figure 1, we can see that nodes H cannot communicate with G at a low power level as their transmission would collide at B. If we assume that the chances of ACK collision is negligible (since its’ a small packet), we can safely omit check (i).

Note that node D in Figure 4.1 is not a neighbor of either node A or node B given that it is located within the C-Zone with respect to these nodes. Therefore, an important issue is how a node (e.g., node D in Figure 4.1), in the C-Zone set their NAV so that they will not transmit RTS-CTS and collide with the ongoing low power DT (as in the BASIC scheme). In the next subsection we elaborate on the node behavior within the C-Zone for SRM.
4.2.1. Node Behavior within the C-Zone

Nodes located in the C-Zone of both node A and B will only be able to sense a transmission, but cannot decode it. The reason why it is crucial for SRM to determine whether a given transmission is due to an RTS or CTS is that this is the only way a node can infer when the actual DATA transmission of this ongoing DT will start. Therefore, packet type determination for nodes in the C-Zone is crucial, while the distance is not an issue and can still be obtained through equation (2). To overcome this, we implement a scheme in SRM in which a node can determine with high probability the type of packet (if RTS, CTS, or neither) is currently being transmitted over the wireless medium based on the duration of the transmission. In SRM, the size of the RTS packet is 22 bytes and of the CTS is 16 bytes (here, we use 1 byte to encode $p_{\text{desired}}$ and 1 byte to encode the SINR level) as these packets include the $p_{\text{desired}}$ and the SINR information. Hence it is possible to deduce with high probability whether the transmission was due to a RTS or CTS.

In case node receives RTSs and CTSs from different transmitters consecutively, it always keeps track of the DT which is closest, in terms of distance as given by equation (2), to itself. In other words, nodes always consider the worst case scenario. Moreover, an important issue in SRM is how nodes in the C-Zone set their NAVs. In SRM we rename the EIFS as SRM_EIFS and redefine its duration for nodes in the C-Zone as:

$$SRM\_EIFS = SIFS + DIFS + [(8\times \text{AverageDATAsize})/ \text{DataRate}] + [(8\times \text{ACKsize}) + \text{PreambleLength} + \text{PLCPHeaderLength}] / \text{BitRate},$$

(3)
where $AverageDATAsize$ is the average size (in bytes) of a DATA transmission, $DataRate$ is the rate at which DATA packets are sent (here, assumed to be the same at all stations). To estimate the value of $AverageDATAsize$, we have run several simulations (discussed next) by varying the $AverageDATAsize$, each of which gives a different value for $SRM_EIFS$. We then evaluate the effect of this parameter on the total data delivered per Joule, and estimate the most suitable $AverageDATAsize$ (we have simulations for different packet sizes too).

### 4.2.1. Sneaking Procedure

We now describe a fully distributed sneaking procedure in SRM. Sneaking in SRM can be divided into two phases: sneaking in DT’s C-Zone and sneaking at DT’s transmission range.

#### 4.2.1.1 Sneaking in DT’s C-Zone

Let us first focus on the sneaking procedure in the C-Zone of the DT’s RTS/CTS. In SRM, whenever a node has DATA to send and its NAV is set (meaning there is an ongoing DT), it may transmit the DATA directly if constraints (i) and (ii) defined earlier are satisfied. However, to guarantee that the sneaking DATA will not collide with the ongoing DT’s RTS or CTS at $p_{max}$, the sneaking node can only start its sneaking DATA transmission once the low power DT’s DATA transmission has started (see Figure 4.1). Furthermore, as we can see from Figure 4.2, the length of the DATA packet a sneaking source can transmit (i.e., the Sneaking DATA) has to be proportional to the sneaking
source’s NAV (which is, in turn, set for the duration of SRM_EIFS if the node is within the DT’s C-Zone, or is set for the duration field contained in the RTS-CTS header if the node sits in the transmission range of the DT’s source, destination, or both), since the NAV of a node indicates the remaining duration for which the medium will be busy. That is, the length of DATA part of a node’s sneaking transmission is essentially decided based on its current NAV length and the data transmission speed. Thus, a sneaking source can determine how big the DATA packet can be. In this calculation, the sneaking source also accounts for the time taken by the sneaking ACK to arrive back at the source. In our existing implementation of SRM, sneaking may result in fragmentation and reassembly of the packet at the MAC layer. However, since fragmentation has been extensively employed in the context of IEEE 802.11 with little overhead [1, 91], we believe this is not a major roadblock. A more efficient solution could be to have a separate queue for small size packets. This way, fragmentation and reassembly would not be needed.

Finally, note in Figure 4.2 that at the sneaking source we employ a backoff mechanism called sneaking backoff. Before any sneaking node tries to sneak the medium, it has to backoff for a random duration between $\left[20, 20 \times N\right] \text{µs}$, where $N$ is an estimate of the average number of neighbors a node has, and is dynamically obtained through the routing protocol in our simulations. The reason why the sneaking backoff is a multiple of 20 µs is because this is the time required for a node to sense medium activity [1]. This is implemented in SRM to provide for the case where multiple nearby nodes try to sneak the medium simultaneously, hence causing collisions. This way, a node can interrupt its sneaking transmission if it detects the medium has become busy during the sneaking backoff period. When sneaking is interrupted, the node returns to regular IEEE 802.11
algorithm (with RTS-CTS) as if transmission sneaking had never been attempted. Sneaking may be tried again in the next DT only.

![Diagram of channel spatial reusability in the SRM protocol](image)

Figure 4.2 – Channel spatial reusability in the SRM protocol (nodes within C-zone use SRM_EIFS for their NAVs)

### 4.2.1.2 Sneaking in DT’s Transmission Range

Let us now focus on the sneaking procedure for the nodes which have correctly received any of the DT’s RTS-CTS. As explained before, if the $p_{\text{desired}}$ used by DNs is below certain levels it is also possible to obtain a sneaking opportunity within the transmission range of the DT. First let us assume that a given node X has correctly received both RTS and CTS packets from the DNs. In this case, node X becomes aware of SINR at both S and R and also of the expected DATA-ACK receiving power (based on the exchanged $p_{\text{recv-S}}$ and $p_{\text{recv-R}}$). Thus, rather than estimating its carrier sensing zone (as done in the previous subsection), node X can precisely determine if its transmission at $p_{\text{desired}}$ is going...
to cause any collision at either S or R. Mathematically, node X can transmit its packet at p_{desired} iff:

(iii) $SINR_s = \frac{P_{S_{\text{recv-S}}}}{P_{i-S} + P_{\text{DATA}_{\text{recv-X}}}} \geq SINR_{\text{THRESHOLD}}$

(iv) $SINR_R = \frac{P_{R_{\text{recv-R}}}}{P_{i-R} + P_{\text{DATA}_{\text{recv-X}}}} \geq SINR_{\text{THRESHOLD}}$

where $P_{i-S} = \frac{P_{\text{ACK}_{\text{recv-S}}}}{SINR_S}$ and $P_{i-R} = \frac{P_{\text{DATA}_{\text{recv-R}}}}{SINR_R}$ represent the interfering powers at S and R respectively and is calculated based on received RTS and CTS packets.

However, if node X receives only one of RTS or CTS, it will not be able to determine the SINR profile at one of the DNs. In other words, node X is in the transmission range of only one of the DNs. Therefore, for the other DN (i.e., node S or R in our example) that node X is not able to decode the packet, it employs a similar scheme as described previously in subsection B.1 (estimating the carrier sensing range) before starting its sneaking transmission. A flow chart describing SRM sneaking procedure is shown in Figure 4.3.
Figure 4.3 – Flow Chart for SRM DT and ST Packet Transmission
4.3 Simulation Environment and Results

We have implemented and simulated PCM, SRM and IEEE 802.11, which is the only protocol which does not employ power control. Since the BASIC scheme has been studied and compared with PCM in [8] and PCM has been shown to be superior to BASIC in all scenarios, we do not consider the BASIC scheme in our study. We have used the following metrics to assess the performance of our considered MAC protocols:

- Aggregate throughput over all flows in the network.

- Total data delivered per unit of transmit energy consumption (or, Mbits delivered per Joule). This is calculated as the total data delivered by all the flows divided by the total amount of transmit energy consumption over all nodes (Mbits/Joule). The energy consumed in packet reception is not taken into consideration in this metric.

For our simulations, we use NS-2 (ns-2.26) with the CMU wireless extension [49]. We use 1 Mbps for the channel bit rate. Similar to [20], the application packet size is of 512 bytes unless otherwise specified, and each flow in the network transmits CBR traffic. We have also carried out simulations for different packet sizes and various network loads. We do not consider mobility in our simulations. For the radio propagation model, a two-ray path loss model is used [49]. We do not consider fading in our simulations. As for the routing protocol, we have employed DSR (Dynamic Source Routing) [51] and the various $p_{desired}$ among the nodes are evaluated during route discovery phase, thus incurring no extra overhead to SRM.

We consider that interfering range is about two times larger than the transmission range as it is mostly the case in IEEE 802.11 stations [28]. More specifically, in our simulation
we consider the transmission range to be 250 m and the interfering range to be 550 m, at the highest transmit power level ($p_{\text{max}}$). All simulation results are the average of 30 runs, and each simulation runs for 70 seconds of simulation time.

### 4.3.1 Simulation Topology

We use both a simple chain and random topologies. For the chain topology, we consider 7 transmit power levels, 1.35 mW, 3.05 mW, 7.25 mW, 18 mW, 36.6 mW, 75.8 mW, and 281.8 mW, which roughly correspond to the transmission ranges of 50 m, 75 m, 100 m, 125 m, 150 m, 180 m, and 250 m, respectively. As for the random topology, we consider 4 power levels, namely, 1.35 mW, 7.25 mW, 36.6 mW, and 116 mW, which approximately correspond to the transmission ranges of 50 m, 100 m, 150 m, and 200 m. The transmission range at power level $p_{\text{max}}$ is 250 m in our simulations for both topologies.

- **Chain Topology:** Our chain topology consists of 30 nodes with 15 single hop flows. The distance between adjacent node pairs is uniform. In our simulations, we vary the distance from 50 m to 250 m.

- **Random Topology:** For the random topology, we place 50 nodes randomly within a 1500x1500 m$^2$ flat area. One flow originates at 25 of these nodes with the nearest node as its destination. We simulated 10 different random topologies (scenarios). Table 4.1 shows the number of flows using different distances for each of the scenarios. For example, scenario 1 indicates that there are 16 transmitters whose recipient is at distance 50 m, 6 transmitters whose recipient is at 100 m, and 3 transmitters have recipient at 150 m. This particular scenario does have any flow at 200 m.
4.3.2 Simulation Results

In this subsection, we discuss our simulation results. Results for the chain topology are presented first, followed by the results of the random topology.

Table 4.1 – Number of flows for various distances and scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 m</td>
<td>16</td>
<td>15</td>
<td>15</td>
<td>9</td>
<td>9</td>
<td>8</td>
<td>15</td>
<td>10</td>
<td>13</td>
<td>9</td>
</tr>
<tr>
<td>100 m</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>4</td>
<td>9</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>150 m</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>200 m</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

B.1 Chain topology: varying combination of application packet size and SRM_EIFS average data size

Figure 4.4 shows the simulation results for 30 nodes with 15 flows in a chain topology. Each flow generates traffic at the rate of 200 Kbps. In this figure, the x-axis represents the packet size generated by the application (i.e., CBR) whereas each curve in the graph represents a different value for AverageDATAsize as given in equation (2). We have considered packets of size 64, 128, 256, and 512 bytes. This study is of paramount importance as the analysis allows the nodes within the I-zone to select different values of AverageDATAsize than the actual application data size employed by the ongoing DT.

As we can see from both Figures 4.4(a) and 4.4(b) that all curves for AverageDATAsize of 512 bytes is observed to give the best results. When AverageDATAsize is smaller than the application packet size, the net result is that SRM will sneak the DT for a reduced amount of time while its performance is still superior to the other protocols under study.
(see the next subsections). However, when AverageDATAsize is greater than the application packet size, there is a small chance (inferior to SRM_EIFS) that collisions with the ST may take place. In our simulations, we observed that during the period of time the DT is over and the ST is going on, nodes in the interfering range of the sneaking source and/or receiver (but who cannot detect the low power ST) are either backing off or waiting for DIFS so as to access the medium. Therefore, collisions may still occur occasionally. In spite of this fact, we observe (see next subsections) that the benefits resulted from sneaking in SRM surpass the drawbacks of the increased number of collisions. As a consequence of this analysis, otherwise noted the application packet size is considered to consist of 512 bytes. For this packet size, the value of SRM_EIFS is equal to 4450 µs. As discussed before, the size of ACK packets is set to 12 octets and the duration of the IEEE 802.11 EIFS field is set to 364 µs.

**B.2 Chain topology: varying node distance**

Similar to the previous study, Figure 4.5 shows the simulation results for 30 nodes with 15 flows in a chain topology. Each flow generates a traffic at the rate of 200 Kbps. As the distance between two neighbors increases in Figure 4.5(a), the aggregate throughput increases in all schemes. This is because when nodes are far apart, a larger number of nodes can transmit simultaneously. As expected, PCM and IEEE 802.11 achieve comparable throughput (their curves overlap) given that PCM does not utilize spatial reuse. SRM, on the other hand, outperforms both PCM and IEEE 802.11 for all node distances because of its transmission sneaking, while improvement is noticeable starting
from 125 meters separation between nodes as a larger number of nodes can carry out sneaking.

![Graphs showing aggregate throughput and total data delivered per Joule](image)

(a) – Aggregate Throughput  
(b) Total data delivered per Joule

Figure 4.4 – Aggregate throughput and total data delivered per Joule for varying combination of packet sizes for chain topology (15 flows)

The total data delivered per Joule in SRM has considerable improvement over the two other protocols. This is due to improved throughput possible by the SRM, coupled with its modified SRM_EIFS for nodes lying within the I-zone. PCM is observed to be more energy efficient than IEEE 802.11, but it is less efficient than SRM, given it requires periodic increments in power level. When the adjacent nodes are 250 meters apart, PCM performs nearly the same as the IEEE 802.11 since it cannot reduce the transmit power level and has to use $p_{\text{max}}$. A similar situation is also observed in SRM as it now has to transmit at $p_{\text{max}}$. With this separation, SRM improvement is negligible in terms of throughput and energy saving is negligible as there is hardly any opportunity for transmission sneaking.
Finally, note that the absence of sneaking would make SRM throughput comparable to the IEEE 802.11 and the PCM, but its energy efficiency would still be superior to the PCM as the SRM does not employ any changes in periodic power level.

**B.3 Chain topology: varying network load**

Figures 4.6 and 4.7 show simulation results for 3 different node distances (50 m, 100 m, and 150 m) in the chain topology, with a varying data rate (load) per flow. In all the scenarios, when the network is lightly loaded, the aggregate throughput is almost identical for all three protocols (Figure 4.6). This is specially the case as nodes are farther apart (Figures 4.6(b) and 4.6(c)) as transmission sneaking in SRM becomes less effective. However, with increment in network load the SRM throughput shows considerable improvement, as the number of transmission sneaking opportunities is improved.

Figure 4.7 compares the data delivered per Joule in SRM, PCM, and IEEE 802.11 with increasing network load. It is important to note that the total data delivered per Joule in SRM is higher than PCM and IEEE 802.11 even when the aggregate throughput for all protocols are the same as shown in Figure 4.6. This is due to the fact that SRM does not change the power level periodically as done in PCM, and hence its energy saving is higher. Needless to mention that the IEEE 802.11 which always transmits at $p_{\text{max}}$. Additionally we can also see that as the node distance increases, the total data delivered per Joule of SRM and PCM protocols decreases as $p_{\text{desired}}$ starts approaching $p_{\text{max}}$. Nevertheless, SRM is observed to deliver more data per Joule as compared to PCM and IEEE 802.11 in all scenarios.
Figure 4.5 – Aggregate throughput and total data delivered per Joule for varying node distances for chain topology (15 flows)

B.4 Random topology: varying network load

Figure 4.8(a) shows the simulation result for one particular scenario in the random topology for varying the data rate. In this case, simulation results are also similar to those for the case of chain topology. The aggregate throughput of SRM outperforms both IEEE 802.11 and PCM (IEEE 802.11 and PCM curves overlap).

Results for the data delivered per Joule are given in Figure 4.8(b). Both PCM and SRM show considerably improved performance over IEEE 802.11, with SRM providing the highest amount of data delivered per Joule.
Figure 4.6 – Aggregate throughput for varying network load for chain topology (15 flows)

Figure 4.7 – Total data delivered per Joule for varying network load for chain topology (15 flows)
B.5 Random topology: 10 different topologies

Figure 4.9(a) presents the simulation results for a random topology with 25 flows. Each flow generates data at the rate of 30 Kbps. The number in the horizontal axis indicates the 10 different scenarios simulated (see Table 4.1). As shown in the Figure 4.9, the aggregate throughput of SRM surpasses that of PCM and IEEE 802.11.

B.6 Random topology: varying packet size

Results for varying packet size in a random topology are given in Figure 4.10. We have simulated packet sizes of 64, 128, 256, and 512, where SRM_EIFS is modified to reflect each packet size. Each flow generates traffic at the rate of 30 Kbps. Figure 4.10(a) indicates that the aggregate throughput of all the schemes increases with an increase in the packet size. However, the performance of SRM is constantly superior to the PCM and IEEE 802.11. As shown in Figure 4.10(b), the total data delivered per Joule for SRM surpasses PCM and IEEE 802.11. Larger packet size means that nodes can sneak more data. Therefore, the gap between SRM and both PCM and IEEE 802.11 widens with increasing packet size.
Figure 4.8 – Aggregate throughput and total data delivered per Joule with increasing load (random topology)

Figure 4.9 – Aggregate throughput and total data delivered per Joule for different scenarios (random topology)

Figure 4.10 – Aggregate throughput and total data delivered per Joule for different packet sizes (random topology)
5. Directional Antenna Systems

5.1 Introduction

Researchers have tried to increase the capacity of ad hoc networks through a variety of innovative techniques. One of the main technological restrictions to the capacity limitations is the omni-directional nature of transmission. Distribution of energy in all directions other than the intended direction not only generates unnecessary interference to other nodes, but also decreases the potential range of transmissions [4, 5]. Existing MAC protocols as in IEEE 802.11 is designed assuming this omni-directional nature of transmission. This has put a fundamental limit on how high one can push the capacity of the system. A thorough study of the capacity of the ad hoc system is done in [53, 54], and it has been shown that the throughput obtainable by each node is

\[ \Theta(\frac{w}{\sqrt{n \log n}}) \]

where \( w \) is the data rate, and \( n \) is the number of nodes. This limitation on capacity exists irrespective of underlying routing protocol or channel access mechanism. It has been also shown [54] that splitting the channel into sub channels do not have any impact on this result.

One way to increase the capacity of the system is by using directional communications. In a simpler way, directional communication can be viewed as dividing the 360° omni region into M different directional regions, each covered by an antenna beam. By using directional communication using the same channel both range and spatial reuse can be
substantially enhanced, since nodes can concentrate transmitted energy only towards a given direction. On the receiving side, directional antennas enable a node to selectively receive signals only from a certain desired direction [5].

5.2 Antenna Concepts

The primary function of radio antennas is to couple electromagnetic energy from one medium (space) to another (wire, coaxial, waveguide etc.). The manner in which energy is distributed into and collected from the space has a profound effect on the use of wireless spectrum. One of the earliest used antenna configuration is a simple dipole antenna whose length depends on the wavelength $\lambda$. These antennas are the close approximation of omni-directional antennas whose radiation pattern is supposed to be symmetric in all directions (Figure 5.1).

In general, directional antenna transmits or receives more energy in one direction. This directionality is generally quantified by a term called gain and measures how much of the input power is concentrated in one particular direction. For a given direction $\vec{d} = (\theta, \phi)$, the gain of the direction antenna is given [5, 53] by

$$G(\vec{d}) = \frac{U(\vec{d})}{U_{avg}}$$

where $U(\vec{d})$ gives the power density in direction $\vec{d}$, $U_{avg}$ is the average power density over all directions, and $\eta$ is the efficiency of the antenna which accounts for loses. The gain gives the relative power in one direction as compared to an omni-directional antenna, and higher gain means a higher directionality. Gain is generally measured of decibels (dBi), where $G_{\text{dBi}} = 10\log_{10} (G_{\text{abs}})$. 
Antenna Pattern is used to specify the gain values in each direction in space. It generally has a main lobe of peak gain and side lobes (smaller gain). Peak gain is the maximum gain taken over all directions. Beam is also used as a synonym for “lobe”. A related concept in the antenna system is beam width. A “half power beam width” refers to the angular separation between the half power points on the antenna radiation pattern, where the gain is one half the peak gain. It is also be defined as “3 dB beam width”, which refers to the angle subtended by the two directions on either side of the direction of the peak gain that are 3 dB down in gain. Typically a more directional antenna has higher gain and lower beam width.

Figure 5.1 – Coverage range comparison of omni-directional and directional transmissions

Given this background in basic antenna concepts, we now give a brief description of different existing directional antenna systems. The growth of directional antenna can be studied at different stages, starting from basic sectorized and diversity antenna systems to more advanced smart antenna systems. The discussion presented here is not intended to cover all aspects of the technology; rather we will give the basics in an informal and intuitive fashion. Readers wishing to explore more in this field can refer to [5]. In a later section of this chapter we elaborate more on a member in the family of smart antenna
systems known as single *switched beam* antenna system, which is the topic of our research work.

### 5.3 Evolution of Smart Antenna System for MANETs

Independent of smart antenna type, almost all smart antenna systems are created by combining a set of independent antenna elements. These antenna elements are placed together and the separation between them is a function of the wavelength. This separation creates a phase difference between different antenna elements which can be adjusted to transmit/receive more energy in one particular direction. The type of smart antenna system is determined by the transceiver complexity and how the transceivers use these antenna elements to transmit or receive electromagnetic waves. In this section we will first study how these independent antenna elements can be used to form directional antennas.

The concept of smart antenna systems existed for some time now, but until recent years, cost barriers have prevented their use in commercial products. The technology development and advent of powerful low-cost digital signal processors (DSP), ASIC design, and development of software-based signal processing techniques and algorithms, have made these systems practical for not only cellular environment, but also for MANETs and there is a plethora of work going on in this area. Although there are different classifications of smart antennas available in the literature, we are first going to explain the two most cited types of smart antenna systems: switched beam and adaptive array antenna systems. Later we will focus on MIMO system which is created by using adaptive array antennas.
Switched beam antenna systems: Switched beam antennas are the simplest ones in terms of hardware design complexity and the various algorithms involved in direction of arrival estimation and beam forming. They employ linear RF beam forming network (BFN) comprising of multiple element arrays (MEAs) at both ends of the link. BFN combines \( n \) antenna elements to form up to \( n \) directional beams. The signal applied to each antenna element is weighted with pre-defined set of weights resulting in antenna patterns with beams pointing in small number of specified directions. This class of smart antenna system is similar to what present cellular system employs. A variant of switched beam antenna system called steerable antenna systems can also steer beam to continuously track a transmitter or receiver.

Switched beam antenna systems facilitate spatial reuse, since the energy is concentrated only in a particular direction. When a switched beam antenna directs its main lobe with enhanced gain in the direction of the user, it forms lobes, nulls and areas of medium and minimal gain in directions away from the main lobe. However since beam is not adaptive, presence of interferer in the beam can affect the performance of the system. Because fixed and predefined weights, present switched beam antenna system does not provide null suppression; this is facilitated by adaptive array antennas discussed next.

Adaptive array antennas: It provides highest degree of accuracy and flexibility in configuring the beam patterns and interference suppression. They have infinite
number of radiation pattern which can be adjusted in real time; and by using a variety of signal-processing algorithms, they can effectively locate and track signals to minimize interference and maximize signal reception quality. Unlike switched beam antennas, adaptive array antennas can deal with multipath by adaptively changing their radiation pattern to accommodate the scattering resulting from multipath. Infact, they exploits multipath to get spatial multiplexing gain. However this requires some feedback resulting in increased signal processing complexity. An \( n \) element antenna having \( n \) degrees of freedom (DOFs) can adaptively null \( n-1 \) interferences completely even when they are uncorrelated with each other and with the desired signal. This approach continuously updates its transmission strategy based on changes in both its desired and interference signal locations. Its ability to track users smoothly with main lobes and possible interferers by nulls ensures that the link budget is constantly maximized.

- **Multiple Input Multiple Output (MIMO) Systems:** The use of adaptive array antennas at both ends of a communication link provides a significant improvement in link reliability, spectral efficiency, and resulting into a technology known as multiple-input multiple output (MIMO) systems. By using multiple antennas at both ends of a link, it is now possible to multiplex the data stream, and open up multiple data pipes within the same frequency spectrum to yield a linear bandwidth of the system, with no extra power consumption. A transmitter/receiver can transmit/receive multiple signals simultaneously by
forming beams in desired directions while nullifying the interferers. Signals can be dependent or independent. While dependent signals received at the receiver leads to diversity gain, independent signals arrive at receiver with different “spatial signatures” which are exploited by the receiver to separate them and thereby yielding spatial multiplexing gain. The main bottleneck towards commercialization of adaptive array system is the cost. Since each of the independent antenna beams now requires independent DSP controllers, it considerably increases the cost of the overall system.

5.4 The Antenna Model

The primarily limitation in the use of directional antennas for ad hoc networks is the cost. Hence in this work, we assume a single switched beam directional antenna model, mainly because of its simplicity and cheaper cost.

We have implemented a complete and flexible directional antenna module at the Network Simulation (NS – version 2.26) [49]. This model possesses two separate modes: Omni and Directional. This may be seen as two separate antennas: an omni-directional and a single switched beam antenna which can point towards any fixed specified direction [65]. In principle, both the Omni and Directional modes may be used to transmit or receive signals. However, in our proposed MDA protocol, the Omni mode is used only to receive signals, while the Directional mode is used for transmission as well as reception. This way, both transmitter and receiver take advantage of the increased coverage range provided by beamforming. This feature is included in our protocol and evaluated in our implementation.
In *Omni* mode, a node is capable of receiving signals from all directions with a gain of $G^O$. While idle (i.e., neither transmitting nor receiving), a node stays in *Omni* mode when using our proposed protocol. By employing selection diversity, as soon as a signal is sensed a node can detect the antenna through which the signal is strongest and goes into the *Directional* mode in this particular antenna.

![Figure 5.2 – The antenna model](image)

In *Directional* mode, a node can point its beam towards a specified direction with gain $G^d$ (with $G^d$ typically greater than $G^O$), using an array of antennas called array of beams. Due to the higher gain, nodes in *Directional* mode have a greater range in comparison to *Omni* mode. In addition, the gain is proportional to number of antenna beams given that more energy can be focused on a particular direction, thus resulting in increased coverage range in this particular direction. For example, with the same transmit energy, a 12 antenna array has a higher coverage range than a 6 antenna array, and a 6 antenna array covers, in turn, a larger range than a 4 antenna array. In our implementation, we have considered this feature, where different number of antenna beams possesses different gains. In order to perform a broadcast, a transmitter may need to carry out as many
directional transmissions as there are antenna beams so as to cover the whole region around it. This is called **sweeping**. In the sweeping process, we assume there is a negligible delay in beamforming in various directions.

Figure 5.2 illustrates the antenna model we consider in this paper. This model has been widely studied in the literature [64, 65, 66, 67]. In this model, the node provides coverage around it by a total of $M$ non-overlapping beams. The beams are numbered from 1 through $M$, starting at the three o’clock position and running counter clockwise. A node can receive and transmit in any of these $M$ antenna beams. In addition, in this model we assume that beams are by default *on*, but they can be switched *off* whenever needed. Whenever *on*, an antenna beam can be used for both transmission and reception. If a particular beam is *off*, a node becomes deaf in that direction. Finally, we assume that all nodes use the same directional antenna patterns and can maintain the orientation of their beams all the time regardless of mobility. As discussed in [64], this can be achieved with the aid of a direction-locating device such as a compass.
6. Spatial Reusability using Directional Antennas

6.1 Introduction

Existing research on ad hoc networks typically assumes the use of omni-directional antennas by all nodes. Such an example is the IEEE 802.11 medium access control (MAC) [1] protocol which attempts to efficiently address various issues of this type of environment. However, due to the omni-directional nature of transmissions, network capacity is drastically limited. For example, the distribution of energy in all directions other than the direction of recipient not only generates unnecessary interference to other nodes, but also decreases the range of transmissions. With directional communications, on the other hand, both range and spatial reuse can be substantially enhanced, by having nodes concentrate transmitted energy only towards their destination’s direction. On the receiving side, directional antennas enable a node to selectively receive signals only from certain desired direction, thereby increasing the signal to interference and noise ratio (SINR).

Therefore, traditional MAC protocols which have been designed under the omni-directional assumption [1, 6] are no longer directly suitable for use over directional...
antennas. The design of an efficient MAC protocol for directional antennas is then a crucial issue and needs further investigation.

6.2 Related Work

Most of the research in the area of directional antennas has focused broadband and cellular networks [61, 62, 63]. In the context of wireless ad hoc networks, research is still at its infancy. In general for ad hoc networks, two models for MAC protocols for directional antennas can be identified. In the first model [64], each node is equipped with $M$ antennas whose orientations can be maintained at any time, regardless of the node’s movement. In this model, it is assumed that nodes have directional reception capability, i.e., they can activate the antenna pointing to the direction of the desired destination while deactivating antennas in all other directions. Thus, the receiving node is not influenced by simultaneous transmissions from other nodes as long as it is not received at the antenna beam the receiver is currently listening to. Most recent research adopts this model [64, 65, 66]. In the second model [67], antennas are always active for receiving and thus transmissions to different antennas results in collision. Some MAC proposals for directional antennas assume this model [68]. In this work, we consider the first model and elaborate on the same in the next section.

In [64], a variation of RTS/CTS mechanism of IEEE 802.11 adapted for use with directional antennas is given. This protocol sends the RTS and CTS packets omnidirectionally in order to enable the transmitter and receiver to locate each other, and sends the DATA and ACK packets in directional mode. A MAC protocol that sends a directional RTS and an omnidirectional CTS is presented in [69]. Here, it is assumed that
the transmitter knows the receiver’s location, so that it can send the RTS directionally. In case location information is not available, the RTS is transmitted in omni mode in order to find the receiver. In [70] it is proposed the use of Directional Virtual Carrier Sensing in which directional RTS and CTS transmissions are employed. Here, it is assumed that the transmitter knows the receiver’s location. Similar to [69], RTS are transmitted omni-directionally in case location information is not available. Finally, [71] studies the problems that appear using directional antennas and proposes a MAC protocol to take advantage of the higher gain obtained by directional antennas. This protocol employs a scheme of directional multihop RTS transmissions so as to establish directional-directional (DD) links between the transmitter and receiver. An assumption of this scheme is that the transmitter must know the entire route to the intended receiver so that the RTS packet can be routed.

The protocols aforementioned share common characteristics that lead to several inefficiencies. In [64, 69, 72] at least one omni-directional transmission of a control packet is employed, hence limiting the coverage area. The presence of omni-directional transmissions of either RTS or CTS limit the range of directional transmissions, which is now defined by the smaller coverage range between any of these packets. In other words, given a particular transmit energy, an array of $M$ antenna beams provides an increased antenna gain in comparison with the omni mode of the order of $M$ [73, 74, 75]. This gain is doubled if there is directivity in both transmission and reception. Thus, a directional communication between two stations may significantly increase the distance between them as compared to the equivalent omni communication, a benefit that has not been explored by the above schemes.
In addition, although [65, 70] uses directional transmissions only, they do not solve the issues of increased instances of hidden terminal problem, node deafness and the determination of neighbors’ location. The first two problems are studied in [65], although a solution is not provided. The third problem originates from the fact that a node has to know through which antenna it can communicate with the intended receiver before transmitting a directional RTS. In [65, 70], nodes’ location is assumed to be known beforehand, while [69] assumes nodes’ location can be determined with the assistance of an additional hardware such as GPS.

In [65, 67] a protocol called Directional MAC (DMAC) is proposed that employs directional transmission of RTS and CTS. Similar to the previous schemes, it assumes nodes’ locations are known a priori. This protocol also suffers from node deafness and hidden node problems [76].

To overcome the shortcomings in DMAC, a scheme is proposed in [76] that employs directional transmission of RTS and CTS without previous neighbors’ location knowledge. To accomplish that, a scheme of circular directional transmission of RTS is carried out by the transmitter which tries to ensure that the RTS packet will eventually reach the intended destination. The destination then sends back a single directional CTS packet towards the source. We refer to this scheme as Circular RTS MAC (CRM). While CRM does not assume prior neighbor’s location availability, it does not satisfactorily prevent node deafness and collisions. As we discuss later, CRM has shortcomings which often result in poor performance.

Finally, [65, 69, 70, 76] propose the concept of Directional Virtual Carrier Sense (DVCS) and Directional Network Allocation Vector (DNAV) mechanisms. Here we show,
however, that this scheme has shortcomings which considerably limit network performance in directional antenna environments, and propose the Enhanced DNAV (EDNAV) approach.

6.3 The DMAC and CRM Protocols

The IEEE 802.11 limits spatial reuse of the wireless channel by having nodes in the neighborhood of a sender and receiver pair to remain silent while communication is in progress. With directional antennas, however, it may be possible to conduct multiple simultaneous transmissions in the same neighborhood. For example, in Figure 6.1 node pairs A and B, and C and D can communicate simultaneously provided the beamwidth of the directional transmissions is not very large. However, simultaneous communication between nodes E and F, and nodes A and B is not possible.

As we have seen earlier, due to higher antenna gain, directional antennas have a greater transmission range than omnidirectional antennas. This enables distant nodes to communicate over a single hop, and results in increased throughput and reduced delay.

A MAC protocol for directional antennas should attempt to take advantage of both benefits of directionality: spatial reuse and higher transmission range. The DMAC protocol described in the next section attempts to achieve both spatial reuse of the channel and take advantage of the higher transmission range by using directional-omnidirectional (DO) links. We then show that DMAC has its own limitations, and then introduce CRM. The CRM protocol tries to overcome some of the limitations of DMAC. We show that CRM itself introduces another set of issues and does not completely tackle the deficiencies in DMAC.
6.3.1 The DMAC Protocol

The DMAC protocol assumes nodes know their neighbors’ location, that is, they are aware through which antenna beam a given neighbor can be reached. Channel reservation in DMAC is performed using a RTS/CTS handshake, both being transmitted directionally. An idle node listens to the channel in Omni mode, i.e., omni-directionally. Whenever a node receives a signal from a particular direction, it locks onto that signal directionally and receives it. Please note that collisions may happen during signal reception, while the node finds itself in Omni mode. Only when a node is beamformed in a specific direction, it can avoid interference in the other remaining directions.

The RTS transmission in DMAC is as follows. Before sending a packet, the transmitter node S performs a directional physical carrier sensing towards its intended receiver R. If the channel is sensed idle, DMAC checks its Directional NAV (DNAV, explained later in this paper) table to find out whether it must defer transmitting in the direction of node R.

The DNAV maintains a virtual carrier sense for every Direction of Arrival (DoA) (i.e., for every antenna beam) in which it has overheard a RTS or CTS packet. If node S finds it is safe to transmit, it performs similar to IEEE 802.11 by entering the backoff phase and transmitting the packet in the direction of node R when the backoff counter counts down to zero.
If idle, the receiver node $R$ remains in *Omni* mode listening to the channel omnidirectionally. When node $R$ receives the RTS from $S$, it is able to detect the DoA of the RTS and lock in the corresponding direction. Upon complete reception of the RTS packet, node $R$ beamforms in the direction of node $S$ and sends the CTS packet directionally towards $S$ provided its DNAV indicates it is free to do so. Similar to IEEE 802.11, the CTS is transmitted after SIFS duration after reception of the RTS.

Note that the nodes other than $S$ and $R$, say $X$, which receive either the RTS or CTS packet, updates its DNAV in the captured DoA with the duration field specified in the RTS or CTS packet. This prevents node $X$ from transmitting any signal in the direction which may interfere with the ongoing transmission between nodes $S$ and $R$.

### 6.3.2 Problems with DMAC

As described in [65], two of the main problems with DMAC, which are also common in other directional MAC protocols, are:

- *Hidden terminal problems* – In IEEE 802.11 RTS/CTS packets are transmitted omnidirectionally to overcome the hidden terminal problem, while this is not the case in DMAC. There are two main sources of hidden terminal problems, namely, *hidden terminal problem due to asymmetry in gain* and *hidden terminal problem due to unheard RTS/CTS*. The first problem is due to the fact that nodes which are in *Omni* mode, have a smaller gain as compared to nodes which are *Directional* mode. When nodes in Omni mode go into Directional mode (e.g., to transmit a RTS), they may be unaware of an ongoing transmission and a collision may take
place. The second problem comes from the reverse situation. That is, a node in
*Directional* mode cannot listen to any other transmission in a direction other than
where it is beamformed. Therefore, when this node goes into *Omni* mode it may
transmit towards a direction where a transmission is being carried out and hence
collide. Obviously, these problems do not occur in omnidirectional transmissions
as all neighboring nodes potentially become aware of any nearby transmission.
We can see that there is a clear tradeoff between spatial reuse and collisions when
employing directional antennas.

- **Deafness** – Assume that two nodes, say $S$ and $R$, are currently beamformed in
each other direction, that is, they are in *Directional* mode. A third node $C$
which has not heard to the RTS/CTS from nodes $S$ and $R$ and which has a packet to send
to either of them, will keep on transmitting RTS to its desired destination, say
node $R$. Since node $R$ is beamformed in the direction of node $S$, it is *deaf* in the
direction of node $C$ and does not respond to its RTS. Therefore, node $C$ will keep
on transmitting the RTS towards node $R$ until the number of attempts exceeds a
threshold name *Short Retry Limit* (SRL) (defined in IEEE 802.11), when it then
reports the failure to the routing layer which takes the necessary actions. In
addition, this may result in unfairness as the backoff interval is doubled upon
every failed transmission. This problem is referred to as the *deafness*, since node
$R$ is deaf to the signals from node $C$ while $R$ is beamformed in the direction of $S$.
The deafness problem results in excessive wastage of network capacity in
unproductive transmissions, and in increased energy consumption.
6.4 The CRM Protocol

The CRM protocols attempts to overcome some of the limitations found in DMAC. Contrary to DMAC, CRM does not depend on the availability of neighbors’ location information. To accomplish that, CRM employs a circular directional transmission of the RTS packet, that is, a node $S$ with an RTS to be sent to node $R$ directionally transmits the same through all antenna beams. This way, node $R$ will eventually receive the RTS packet coming from node $S$.

Also based on this scheme, CRM may decrease the occurrence of node deafness as it informs all nodes within the transmitter’s directional radio range about the oncoming transmission. This way, nodes overhearing the RTS defer their transmission in the direction of the transmitter, hence minimizing deafness. In addition, CRM includes extra information in the RTS and CTS packets so as to enable other nodes to determine whether they need to defer in the direction of the transmitter or receiver, thus also minimizing the hidden terminal problem.

Upon receipt of an RTS packet, the receiver node $R$ delays the transmission of its CTS for a period of $T_{CRM} = K \times RTS\_Transmission\_Time + SIFS$, where $K$ is the number of antenna beams the sender node $S$ will transmit the circular directional RTS, $RTS\_Transmission\_Time$ is the time required for the transmission of a single RTS, and $SIFS$ is as described earlier. Therefore, the CTS is only transmitted after the sender node has swept through all of its beams.
6.4.1 Problems with CRM

We have identified that the CRM protocol does not completely overcome the limitations of DMAC, and itself introduces new shortcomings. First of all, CRM only prevents node deafness in the neighborhood of the transmitter node. As we have seen earlier, CRM employs a circular directional RTS transmission and a single directional CTS transmission. As a result, CRM is only able to cope up with node deafness at the sender neighborhood, while deafness may still occur in the neighborhood of the receiver.

A more serious issue with CRM is in the design of its RTS/CTS handshake. In CRM, a sender node $S$ initiates the circular directional transmission of its RTS although it is not at all sure whether its intended receiver node $R$ has correctly received its RTS or not. Consider the example in Figure 6.2 where nodes are equipped with an eight-beam antenna array. Further consider that the sender node $S$ initiates transmission of a circular RTS through antenna one and its intended destination node $R$ is located at the antenna six. As node $S$ circularly transmits the RTS packets, nodes in the corresponding directions update their DNAV for the duration contained in the RTS packet. Now assume that when node $S$ transmits its RTS through antenna six towards node $R$, node $A$ also sends a RTS to node $R$ thus causing a collision. In this case, node $R$ will not respond to node $S$’s RTS. The side effect of this is that nodes in the neighborhood of node $S$ and which correctly receive the circular RTS will not be able to initiate any transmission either towards node $S$ or node $R$, since their DNAV is set towards both nodes $S$’s and $R$. Clearly, this degrades the network capacity.
Another limitation in CRM can also be seen through the example in Figure 6.2. Here, we see that the sender node $S$ transmits its circular directional RTS through four “empty” sectors. That is, out of the eight sectors covered by the eight antenna beams of node $S$, four of them have no neighbors. Therefore, for every circular RTS transmission node $S$ wastes four of them. As shown in our simulation studies, this overhead has an increasingly larger impact as the number of antenna beams is increased.
7. Proposed MAC Protocol for Directional Antennas (MDA)

7.1 Introduction

The MDA protocol aims to effectively overcome the limitations found in both DMAC [65, 67] and CRM [76] by utilizing a combination of adaptive mechanisms. To take advantage of the increased gain feasible by directional antennas, all transmissions in MDA are directional. Secondly, MDA does not rely on prior availability of neighbors’ location, while it learns its neighbors with time as communication between nodes takes place.

To prevent node deafness and the new types of hidden node problems aforementioned, MDA employs a special form of Circular Directional Transmission (CDT) of both RTS and CTS, namely, the Diametrically Opposite Direction (DOD) procedure. The DOD mechanism includes two major enhancements over the plain CDT procedure as implemented in CRM: firstly, RTS and CTS packets are transmitted in diametrically opposite directions which ensure maximum coverage; secondly, these packets are only transmitted through the antenna beams with neighbors. In order to accomplish that, MDA employs an adaptive mechanism where it learns and caches information about those sectors with neighbors. Initially, MDA performs similar to CRM by sweeping through all antenna beams. However, as responses are received, it collects and caches neighboring
information used in future transmissions. Contrary to CRM, however, MDA does not perform full sweeping and the DOD procedure is concurrently carried out both at the transmitter and the receiver sides. In addition, the Enhanced DNAV (EDNAV) mechanism incorporated in MDA considerably improves performance by accurately differentiating between deafness and collision scenarios. To make the protocol intuitive and simple in implementation point of view, MDA design has been inspired by the IEEE 802.11 MAC [1].

7.2 Determination of Neighbors’ Location

One important component in the design of MDA is the precise determination of the antenna beam through which a given neighbor can be reached. This is a continuous process which can be divided into two distinct phases, namely, the learning and the maintenance phases.

In the learning phase, MDA relies on the very basic characteristics common to the majority of routing protocols employed over ad hoc networks [45, 46, 47, 48, 51]: the use of broadcasting. These protocols either employ a form of periodic one-hop hello packets, or at least they flood the network with route request packets before data transmission can take place. The bottom line to remember in these protocols is that, before any actual data communication starts, a network layer broadcast must be carried out either by hello packets or by flooding routing requests control packets. From the MAC layer perspective, the routing broadcast packets are mapped onto MAC layer broadcasts to be transmitted to all neighbors of a node.
Upon receipt of a network layer broadcast packet (e.g., hello or route request packet), a node, say $S$, running MDA initiates the CDT procedure of the broadcast packet through its, possibly in all antenna sectors. Assuming that the nodes possess a $M$-beam antenna array, the node $S$ has to first determine how many of these sectors are actually in idle state, that is, the Enhanced DNAV (EDNAV – explained in Section 7.4) in the direction $i, 1 \leq i \leq M$, is currently zero. The reason for this is that a packet cannot be sent in a busy sector or else there may be a collision with other ongoing transmissions in that particular sector.

If the routing protocol employs any form of hello packets, all network nodes will eventually determine all their neighbors during the learning phase, given that hello packets are periodically transmitted. More important than determining all particular neighbors of a node, this process also allows a node to determine if any of its sectors have any neighbors at all. On the other hand, if the protocol is not based on hello packets but uses flooding as a means to discover destination nodes, MDA proceeds in a similar manner as described while the only difference resides on the way the route discovery procedure is carried out. According to the majority of on-demand routing protocols for ad hoc networks, once a node initiates a route discovery; all (or most) of its one-hop neighbors will eventually re-broadcast the route request packet, consequently determining the beams through which they are reachable. According to our simulations, we have noted that very few broadcasts (usually three) are necessary for a node to figure out the beam information of all its neighbors.

The maintenance phase is conducted basically to handle node movement. As node mobility is common in ad hoc networks, after some time nodes may no longer be
reachable through the same antenna beam. Assume that a given node \( R \), which was originally reachable through antenna beam \( i \), moves out and no longer responds to an RTS packet sent by node \( S \) after SRL retries. In IEEE 802.11, occurrence of this event leads the node to report to the network layer a send failure and, in most of the cases, a new route discovery by a network layer broadcast (i.e., flooding) is initiated for the destination node. In MDA we maintain the information that a send failure has occurred, and this is used to force MDA to proceed as in the learning phase whenever a new routing layer broadcast is received, i.e., by broadcasting it through all idle antenna beams. This way, the protocol robustness is guaranteed. We note that even if the network nodes possess considerable mobility, a drastic gain can be obtained by using this adaptive mechanism.

### 7.3 The Diametrically Opposite Directional RTS and CTS

The MDA protocol is based on a novel and optimized form of RTS and CTS transmission called the Diametrically Opposite Directional (DOD) procedure. Based on the neighbors’ information (Section 7.2), RTS and CTS transmission can be significantly optimized. In DMAC, the solution was to send RTS and CTS only through the beam where the intended node is located, but this approach has its own limitations as previously described such as hidden node problems and deafness. To better understand this effect, let us analyze Figures 7.1(a) and 7.1(b). In these figures, the shaded area represents the region which is not covered by a RTS/CTS transmission between nodes \( S \) and \( R \) when employing DMAC and CRM, respectively. A closer look reveals that the shaded area actually represents the *deafness region*. In other words, nodes sitting in this region
receive neither the RTS nor the CTS packets originated from node S or R, respectively, and hence become deaf to their communication. As we can see from Figures 7.1(a) and 7.1(b), the deafness region in CRM is considerably smaller than DMAC as it employs circular directional transmission of RTS. As in the CRM, CTS is not circular, part of the region around node R defines CRM’s deafness region as shown in Figure 7.1(b).

By analyzing Figures 7.1(a) and 7.1(b), we conclude that CRM is able to considerably decrease the occurrence of the node deafness problem. Not only that, CRM handles the new types of hidden terminal problem for the case when the hidden node is around the neighborhood of the transmitter. However, collisions and deafness still occur when the hidden node sits in the deafness region.

One possible solution to handle these problems would be to apply a CDT of both RTS and CTS. That is, to extend CRM to carry out a circular directional transmission of CTS at the receiver side. However, not only the delay would considerably increase (and throughput decrease) but the coverage area of the RTS and CTS would considerably overlap, thus leading to a high number of collisions. Even if some beams are skipped as

![Figure 7.1 – Coverage Range in DMAC, CRM and MDA, and RTS/CTS/DATA/ACK exchange in MDA](image-url)
in MDA, collisions of circular RTS/CTS packets may still occur. For example, assume in Figure 7.1(c) that the initial RTS/CTS handshake between $S$ and $R$ is over. They will then start their CDT of RTS and CTS in counterclockwise direction. If node $S$ does not have any neighbors in sector 2 and 3, it will directly move to sector 4 and send its circular RTS. Node $R$ will, in turn, also start its circular CTS from antenna 4. As a result, a collision will likely occur at node $X$.

In order to effectively handle these problems at the neighborhood of both transmitter and receiver, MDA employs DOD transmission of RTS and CTS (DOD RTS/CTS) at the transmitter and receiver side, respectively. MDA incorporates major enhancements in the RTS/CTS transmission, and the steps are shown in Figure 7.1(c).

In MDA, the DOD transmission of RTS and CTS is optimized by sending these packets only through those sectors where neighbors are found. As we know, this information can be obtained through the neighbors’ location procedure.

The DOD RTS/CTS mechanism in MDA works as follows. Initially, assume that all nodes have the same number of antenna beams equal to $M$, and that node $S$ has a packet to be sent to its neighbor node $R$ through beam $A_{SR}$. If $A_{SR}$ is not idle, the backoff procedure is initiated similar to IEEE 802.11. Otherwise, the sender node $S$ has to ascertain a few key points. Firstly, it needs to determine through how many of its sectors (called DOD sectors), say $D$, besides the one it communicates with the receiver $R$ it has to transmit a DOD RTS. To illustrate this procedure, please refer to Figure 7.1(c). First of all, right before sending a RTS to $R$ node $S$ needs to estimate the antenna beam $A_{RS}$ used by $R$ to reach $S$. By simple mathematics, we can see that node $S$ can easily figure out $A_{RS}$ given that it knows $A_{SR}$ (through the neighbor information) as follows. The antenna beam
A_{XY} a node X uses to communicate with node Y can be used to derive the beam A_{YX}, which is used by Y to communicate with X. If M is even, node X can easily determine node Y’s receiving antenna by:

\[ A_{YX}(A_{XY}, M) = \begin{cases} 
A_{XY} + \frac{M}{2}, & \text{if } A_{XY} < \frac{M}{2} \\
A_{XY} - \frac{M}{2}, & \text{otherwise}
\end{cases} \quad (1) \]

On the other hand, if M is odd a more general model can be employed which relies on the angle of arrival (AoA) [70], and is given by:

\[ A_{YX}(A_{XY}) = A_{XY} + 180^0 \quad (2) \]

For simplicity, however, from now on we consider M as even. Basically, equation (1) is used to shift a node’s transmitting antenna beam and obtain the receiving node’s antenna beam. Applying equation (1) to the scenario of Figure 7.1(c), node S finds that A_{RS} is equal to 3. With this information, node S then makes its DOD-RTS_{End} as also equal to 3, while its first DOD RTS_{Start} is antenna 2. After this procedure, node S then sets D to two; as it may possibly send DOD RTS through two beams, namely, 2 and 3.

Secondly, out of these D DOD sectors MDA has to determine how many have neighbors and are idle. Let K_S, 1 \leq K_S \leq D, be the resulting number of beams (e.g., K_S = 2 in Figure 7.1(c)). Node S then sends its RTS towards node R. Once node R receives the RTS from node S, it carries out the same procedure. Similarly, let K_R, 1 \leq K_R \leq D, be the resulting number of beams calculated by node R (e.g., K_R = 2 in Figure 7.1(c)). Figure 7.2 depicts the algorithm used to calculate the D and K values.
An important aspect in the design of MDA is that the first RTS sent is always transmitted in the sector where its intended neighbor is located, and the DOD transmission of RTS and CTS is only initiated once the RTS/CTS handshake between the communicating nodes is successfully completed. We do this to overcome one of the limitations found in CRM that initiates the circular directional transmission of the RTS packet (thus reserving the channel) even before the sender node knows if any of its RTS has or will ever be correctly received by its intended destination node. As we discussed earlier and also shown later by simulation, this causes severe degradation in CRM protocol performance.

Therefore, to overcome this problem in MDA, the sender node $S$ waits for the receiver node to send back its CTS before initiating the DOD procedure. In case CTS is not received, the sender times out and retransmits the RTS as in IEEE 802.11. This mechanism is illustrated by steps in Figure 7.1(c).

**Figure 7.2 – Algorithm to calculate the D and K values**

```plaintext
Procedure CalculateK()
Input: Packet
Output: k
Begin
set $B_{xy}$ = getDstBeam(Packet);
set $B_{yx}$ = shift($B_{xy}$); //Given by Equation 1
set nodeTotalBeams = 360/BEAM_COVERAGE;
if($B_{yx}$ > $B_{xy}$)
    set D = $B_{yx} - B_{xy}$;
else
    set D = ($B_{yx} - B_{xy}$) + nodeTotalBeams;
set k = 0;
set $j$ = ($B_{xy}$+1) % nodeTotalBeams;
for (i = j; i < D; i++) {
    if(DNAV[$j$].time <= CURRENT_TIME) {
        if (hasNeighborInSector($j$)) {
            k++;
        }
    }
    $j$ = ($j$ + 1) % (nodeTotalBeams);
}
return(k);
End
```
Upon reception of an RTS packet in step (1), the receiver proceeds similar to IEEE 802.11. That is, it waits for a period of time equal to SIFS and sends back a CTS as shown by step (2). Only after the RTS/CTS handshake is completed and the channel is reserved in their direction, will both sender and receiver nodes simultaneously initiate the DOD transmission of their RTS and CTS packets, respectively, to inform their neighbor nodes. This simultaneous DOD transmission of RTS and CTS is observed to save time and effectively takes care of the hidden node problem and deaf nodes at both the neighborhood of the sender and receiver. The concurrent DOD procedure is illustrated Figure 7.1(c) by step (3). Although there is still a small deafness region in MDA, this looks to be the smallest possible deafness region so that the collision probability does not increase.

One issue still remains is how to synchronize sender and receiver again to carry out DATA/ACK transmission. To this end, the sender node $S$ includes its value of $K$ in its RTS, that is, $K_S$, and the receiver node $R$ includes $K_R$ in its CTS back to node $S$. Through $K_S$, node $R$ is able to determine the exact point in time when node $S$ will have finished its DOD transmission of RTS and hence will start transmitting DATA. Similarly, node $S$ with $K_R$ can precisely tell the moment node $R$ will be ready and waiting for DATA transmission. Clearly, the DOD procedure works extremely well in uniformly distributed networks when $K_S$ is equal or approximately equal to $K_R$ or even when there is a very small discrepancy in their difference. When there is a large difference between $K_S$ and $K_R$, one node will eventually have to wait until its corresponding node is ready. Steps (4) and (5) in Figure 7.1(c) depict the DATA/ACK transmission.
7.4 The Enhanced Directional NAV (EDNAV)

As discussed before, one of the main problems with directional antennas is the new instances of the hidden terminal and deafness problems. To cope up with this problem, MDA employs a combination of DOD transmission of RTS and CTS (as explained earlier) together with a scheme that informs the neighbors of a node about its intended future transmission. Upon receiving DOD RTS/CTS, a node has to decide if it is necessary to defer transmission in any of its direction so as to prevent the aforementioned problems.

A discussion about this problem can be found in [65, 70, 76] where a Directional NAV (DNAV) scheme [69] is employed to handle such issues. DNAV is an extension to the NAV concept used in IEEE 802.11 for directional antennas. Essentially, DNAV is a table that keeps track for each direction the time during which a node must not initiate a transmission through this direction. In IEEE 802.11, DMAC and CRM, nodes continuously update this table upon overhearing a packet transmission in order to keep it from transmitting through this particular direction and generate collisions (in the case of both DMAC and CRM) and deafness around the transmitter (in the case of CRM).

In MDA we incorporate an Enhanced DNAV (EDNAV) scheme comprised of two components: a DNAV mechanism which is manipulated differently from previous schemes, and a Deafness Table (DT) which is used to handle deafness scenarios. It is important to differentiate applicability of each of these schemes. Whenever a node has a packet to be sent over one direction, both DNAV and DT are consulted. On the other hand, upon reception of a packet the node will either modify its DNAV or its DT, not both. If the node lies in the communication path between the transmitter and the receiver
(first RTS/CTS handshake), the DNAV is to be modified. The DT is modified whenever
the node receives either a DOD RTS/CTS, that is, once the RTS/CTS handshake is over.
In this case, the node is certain not to lie within the communication path of the oncoming
transmission.

The idea behind EDNAV is to differentiate between deafness and collision scenarios, and
thus effectively overcome the limitations found in both DMAC and CRM which handle
these problems in the same way through the use of DNAV only. These two mechanisms
incorporated in EDNAV are described next.

7.4.1 The DNAV in MDA

In MDA, the DNAV is only modified for nodes lying along the communication path
between the sender and receiver. A node is said to be in the communication path of a
transmission if it can cause collision with that transmission. For example, node C in
Figure 7.3 is in the communication path of nodes S and R as it can cause collision with
any transmission between S and R, while node E is not.

![Figure 7.3 – DNAV update procedure in MDA](image-url)
To allow a node to determine whether or not it lies in the communication path of a given transmission, MDA adds a piece of information to the RTS/CTS handshake. Whenever a node $S$ transmits an RTS/CTS packet to a node $R$, it puts in the packet header the beam $S$ uses to communicate with node $R$, say $A_{SR}$. A third node $T$, upon receiving the RTS/CTS packet through its antenna beam, say $A_{TS}$, retrieves $A_{SR}$ from the packet header and checks if the beam used by node $S$ to communicate with itself, say $A_{ST}$, is equal to $A_{SR}$. If so, node $T$ determines that it lies within the communication path between $S$ and $R$, accordingly sets its DNAV($A_{TS}$) for the beam towards $S$, and if it is a RTS packet, it switches off the beam $A_{TS}$ for the time span corresponding to the duration field contained in the packet header. Otherwise, the DNAV is kept unchanged and the DT, in turn, is modified as explained in the next subsection. Switching off towards the direction $A_{TS}$ guarantees node $T$ to become deaf for the entire DATA/ACK transmission between $S$ and $R$. If this is not done (as in existing protocols), whenever node $S$ starts transmitting a packet (e.g., DATA) to node $R$, node $T$ would tune to the direction $A_{TS}$ and receive the entire transmission between $S$ and $R$. This is hereby called *persistent hearing problem* and is totally undesirable as node $T$ would, in this case, become deaf to all of its other directions through which it could eventually initiate communication or be contacted. Therefore, by switching off the beam we allow node $T$ to communicate with nodes in other directions other than $A_{TS}$ and hence improve the network performance. Obviously, a beam is again switched on upon expiration of its corresponding DNAV. It is to be noted that a similar approach cannot be adopted for CTS reception at $T$. This can be justified by the fact that the ACK transmission duration is very small as compared to that of DATA
duration. As a result, if node T also becomes deaf in $A_{TR}$, it may miss important control or broadcast packets from other nodes.

For such a scheme to work, the node T has to be able to determine if $A_{ST}$ (unknown) is equal to $A_{SR}$ (included in the packet header). Since T is aware of $A_{TS}$ (S is a neighbor of T), it can use equation (1) to calculate $A_{ST}$. Finally, we can see that in MDA whenever a node T receives both an RTS and CTS from a handshake between nodes S and R, it can reliably conclude that it lies in the communication path between S and R and will use DNAV. Alternatively, if T does not receive either an RTS or CTS, this indicates that it is not a neighbor of either the receiver or transmitter, respectively, and will leave DNAV unchanged while appropriately setting DT as described in the next subsection.

To better illustrate this procedure, consider the example in Figure 7.3. In this figure, node S starts a transmission to node R by first sending an RTS and receiving back a CTS. In this figure, node D is a neighbor of node S only, and nodes A and B are neighbors of node R only. More importantly, note that nodes C and E are neighbors of both node S and R, but only node C will be said to lie in the communication path between S and R and set its DNAV towards node S as, through equation (1), it realizes that the antenna beam S uses to communicate with R (contained in the packet header) is equal to the beam S uses to communicate with itself. Node C will reach a similar conclusion with regards to node R (also through equation (1)) whenever it receives R’s CTS. Once the RTS/CTS handshake is over and the DOD procedure is initiated, node E will receive a DOD RTS from node S but, contrary to node C, it will conclude that it should not change its DNAV towards S as the antenna S uses to communicate with R is different from the one S uses to
communicate with itself. In other words, node \( E \) realizes that it cannot cause collision to the transmission between nodes \( S \) and \( R \).

![Diagram of communication between nodes](image)

**Figure 7.4 – DNAV limitations and the DT table**

### 7.4.2 The Deafness Table Mechanism

Whenever a node \( T \) receives a RTS/CTS packet and it determines that it does not lie in the communication path between the two communicating nodes \( S \) and \( R \) (i.e., node \( T \)'s transmissions do not collide at either \( S \) or \( R \)), the DNAV is left unchanged, while another set of checks is performed so as to update the Deafness Table (DT).

DNAV is not suitable to handle deafness as it is simply an extension of the NAV as employed in IEEE 802.11. In other words, DNAV holds the duration the medium is busy in a particular direction as shown in Figure 7.4(a). To show the limitation of using DNAV to handle deafness, consider the topology in Figure 7.4(b) where node \( S \) sent an RTS and received the CTS back from node \( R \). Nodes \( S \) and \( R \) would then initiate the DOD transmission of RTS and CTS respectively, but let us confine our discussion here to node \( S \). Node \( S \)'s first DOD RTS is sent through beam 2 and is received by node \( A \) through beam 4 (also confirmed by equation (2)). In existing DNAV implementations,
node A would set its DNAV for beam 4 for the entire transmission duration between nodes S and R. While this prevents deafness as node A is now unable to communicate with node S (and maybe node R), it limits performance in case node A has a packet to send to node B and vice-versa. Note that nodes A and B could communicate without causing any collision with the ongoing communication between S and R. However, as node A’s DNAV is set for beam 4, it is unable to initiate communication with B, thus limiting its performance. The root of this problem is the DNAV, which does not account for the case where multiple nodes are reachable through the same antenna beam, that is, its granularity is not adequate.

To handle the shortcoming of DNAV for the case of deafness, we use the DT scheme depicted in Figure 7.4(c). Now, instead of storing the duration for a particular direction as in DNAV, DT incorporates a finer granularity where it maintains the duration for each individual communicating node. Returning to our previous example, upon reception of the DOD RTS packet from node S, node A would keep its DNAV unchanged (as described in Section 7.4.1) and insert an entry relative to node S in its DT. With this scheme, deafness would still be overcome as node A would attempt to communicate with S for the transmission duration between S and R. On the other hand, the DT allows nodes A and B to communicate with each other if needed as there is no impediment (neither DNAV nor DT).

In order to ensure the correct update of DT, it does not suffice only to update it in the direction through which a DOD packet has been received. When a node receives DOD RTS/CTS packet, it should not only update its DT for the node from which it received the packet so as to overcome the deafness problem, but also in the direction of the
transmission between the sender and the receiver. For example, node A in Figure 7.4(b) may have to update its DT table not only for node S but also for node R, in case R is a neighbor of A. Note that in MDA, node A would not receive a DOD CTS packet coming from R and, therefore, it has to infer the need to update its DT for node R based on the DOD RTS received from S. An attempt to handle this issue is provided in CRM. However, CRM itself introduces three main problems. First and foremost, it always uses the DNAV to prevent deafness, leading to the limitations previously described. Second, it adds excessive amount of additional information in the RTS packet, thereby increasing the protocol overhead. Third, it only solves the problem for transmitter’s neighbors, as there is no concept of circular directional CTS. In view of this, here we propose a general approach that does not assume neighbors’ location, introduces very little overhead, and solves the problem at both the transmitter and receiver sides.

This scheme works as follows. Assume in Figure 7.4(b) that node A is a neighbor of both S and R, and that it has receives a DOD RTS packet coming from S through antenna beam $A_{AS}$ (equal to 4 in Figure 7.4(b)). After determining that the DNAV is to remain unchanged as it does not lie in the communication path between S and R ($A_{SA} \neq A_{SR}$ – see Section 7.4.1), node A first updates its DT for node S. Next, node A has to determine if it also needs to update its DT for node R for the same duration of time. For this to happen, node R has to be a neighbor of node A and the antenna beam, say $A_{RA}$, node R uses to communicate with node A is equal to the antenna beam $A_{RS}$ used by node R to communicate with node S. The calculation of both $A_{RA}$ and $A_{RS}$ follows directly from equation (1), where node A uses $A_{AR}$ (discovered during the neighbor discovery procedure) to compute $A_{RA}$, and $A_{SR}$ (contained in the DOD RTS packet header) to
compute $A_{RS}$. If these conditions are satisfied, the DT at node $A$ for node $R$ is updated accordingly. An entry for node $R$ is not inserted in the DT otherwise. We note that while we have described this scheme for node $A$ which has received a DOD RTS from node $S$, the same procedure is applied for nodes receiving a DOD CTS from node $R$ and which, in this case, do not receive the corresponding DOD RTS. We have modified CTS header to include the ID of the node which sends it.

Finally, this scheme is observed to reduce the overhead of CRM, tackles the deafness problem at both the sender and the receiver neighborhood, and does not limit the network capacity by using DT and DNAV.

### 7.5 Implementation Details

In this section we describe some important implementation details of MDA. During the protocol implementation, we had to make adjustments to the timings and variables used in IEEE 802.11 given the new schemes directional transmissions of RTS and CTS, and the use of $M$ directional antennas that requires that some of the default values of IEEE 802.11 variables be reconsidered. In the following subsections, we assume node $S$ is the transmitter and node $R$ is the receiver.

#### 7.5.1 Simultaneous Transmission of RTS and CTS

As in IEEE 802.11, nodes in MDA overhearing the RTS or CTS coming from nodes $S$ and $R$ update either their DNAV or DT based on the duration field contained in the packet. As multiple RTSs and CTSs may have to be transmitted, the duration field has to
be incremented by these additional transmissions. Assume that $K_S$ and $K_R$ are the number of antenna beams through which the RTS and CTS packets have to be sent at nodes $S$ and $R$, respectively. The duration field has to be incremented by $(K_S - c) \times \text{RTS\_Transmission\_Time}$ in the RTS packet and by $(K_R - c) \times \text{CTS\_Transmission\_Time}$ in the CTS packet, where $c$ is an integer, initially equal to zero, maintained by each node that is incremented every time a directional RTS/CTS packet is sent. This way, nodes overhearing the RTS or CTS can correctly set their DNAV or DT for the entire duration of the transmission, including the DOD procedure.

### 7.5.2 Short Retry Limit (SRL)

SRL is a threshold maintained by IEEE 802.11 that controls the number of packet (RTS or DATA) transmission attempts made before a send failure is reported to the routing layer. The way SRL has been set in IEEE 802.11 assumes an omni-directional antenna is in place. However, when directional antennas are employed, the SRL can no longer be used to represent all antenna beams or an excess number of send failures may end up being reported. Therefore, we have extended the SRL to be one per each antenna beam, where the default value employed by NS IEEE 802.11 implementation (i.e., SRL = 7) is now separately defined for each antenna beam.

### 7.5.3 DOD Transmissions and EDNAV

As we have seen earlier, before the transmission of a RTS or CTS, nodes employing MDA, analyze which of its sectors are both free and have any neighbors before calculating their value of the $K$ parameter. However, it might so happen that a sector
becomes busy, if previously idle, or idle, if previously busy, after such an analysis has been performed. In the former case, a node stays silent for the corresponding transmission period if its DNAV became non-zero in a particular direction. For example if the DNAV of node $S$ or node $R$ is non-zero towards a specific direction, the RTS or CTS packet cannot be transmitted and these nodes stay silent for the corresponding transmission period. In other words, node $S$ stays silent for a period equivalent to $\text{RTS\_Transmission\_Time}$, and node $R$ stays silent for $\text{CTS\_Transmission\_Time}$. This way, collisions with other ongoing transmissions could be prevented.

In the latter case, although very unlikely as we have observed through our simulation studies, a node skips a sector which was initially busy and became idle in the meantime. The reason for this is that in MDA nodes $S$ and $R$ exchange their $K$ values in the first RTS/CTS handshake so that this can be used for determination of their rendezvous point, and this commitment cannot be broken.

### 7.6 Performance Evaluation

We have implemented a directional antenna module in NS (version 2.26). This module covers most of the aspects of a directional antenna system including variable number of antenna beams, and different gain values for different number of antenna beams among others. As for the protocol support, we have implemented DMAC, CRM, and MDA.

For the simulations that follow, we have considered CBR traffic sources at data rates of 100 Kbps, 200 Kbps, 400 Kbps, 600 Kbps, 800 Kbps, 1000 Kbps, 1200 Kbps, and 1600 Kbps. In addition, we evaluate DMAC, CRM and MDA for four, eight, and twelve
antenna beams with transmission ranges of 370, 550, and 710 meters, respectively. For IEEE 802.11, the transmission range is set to 250 meters. Also, in all the scenarios, we consider a 2 Mbps network with no node mobility. It is to be noted that in the following analysis we have enhanced DMAC with prior knowledge of its neighbor’s location. Although it makes the analysis biased towards DMAC and may be unfair to other schemes which do not need knowledge of neighbor location, this is the only way by which we can compare DMAC with MDA and CRM.

![Topo](image1)

Figure 7.5 – Linear topology evaluation

### 7.6.1 Linear Topology

As discussed Section 7.2, one of the problems in directional antennas is the hidden terminal problem due to asymmetry in gain. This problem is illustrated in Figure 7.5(a), where node $S$ sends a RTS to node $R$, and has node $A$ as its neighbor. As we know, when nodes $S$ and $A$ are in idle mode, they hear omni-directionally (i.e., with gain $G_O$). Since node $R$’s beam includes node $S$ only (see Figure 7.5(a)), node $A$ becomes a hidden node for $R$. If some form of CDT of RTS is not employed (e.g., as in DMAC), node $A$ will not
receive node $S$’s RTS. Neither will node $A$ receive node $R$’s CTS as it is listening the channel omni-directionally. As a result, node $A$ will not be aware of the transmission between nodes $S$ and $R$. When node $S$ initiates the DATA transmission to node $R$, node $R$ uses selection diversity and starts to receive the RTS packet directionally with gain $G^d$. If during node $S$’s DATA transmission to node $R$, node $A$ sends a packet towards node $R$ (e.g., a RTS to node $S$), node $R$ will receive the packet as it is in directional mode (i.e., with gain $G^d$), hence causing a collision with node $S$’s DATA transmission. Note that although we have discussed this scenario with respect to node $A$, but the same problem occurs at node $B$ if some form of CDT of CTS is not employed (e.g., as in both DMAC and CRM). MDA deals with this problem effectively by employing an optimized DOD transmission of both RTS and CTS, and hence informing nodes $A$ and $B$ about the intended transmission. Nodes $A$ and $B$ will, in turn, set their DTs in the direction of both nodes $S$ and $R$, respectively, thereby preventing them from sending packets to these nodes and generating collisions.

To quantitatively analyze the impact of this scenario on the network performance, we simulate the network of Figure 7.5(a) and compare the performance of IEEE 802.11, DMAC, CRM, and MDA. Also, we have employed an array with eight antenna beams for each node, but we note that any number of beams would produce similar results, given that nodes are aligned. In this scenario, node $S$ transmits to node $R$, node $A$ transmits to node $S$, and node $B$ transmits to node $R$. The coverage range is such that node $S$’s RTS does not include node $B$ and node $R$’s CTS does not include node $A$, as nodes $A$ and $B$ listen to the medium omnidirectionally. On the other hand, node $A$’s RTS includes node $R$ as node $R$ is listens to node $S$ (DATA transmission) directionally, and may cause
collisions. Similarly, node B’s RTS includes node S as node S listens to node R (CTS and ACK) directionally, and may also result in collisions.

Figure 7.5(b) shows the simulation results obtained for this scenario. Similar to [65, 76], our results show that directional antennas have an inferior performance for linear topologies as compared to IEEE 802.11, given that a larger range is blocked in directional antennas as compared to IEEE 802.11. Thus, IEEE 802.11 achieves a better special reuse in linear topologies. Despite of this fact, we see that MDA performs best amongst the directional MAC protocols. This is mainly due to the optimized DOD transmission of both RTS and CTS which informs the neighbors of a node in little time about the intended transmission, thus preventing hidden terminals. CRM, on the other hand, does not perform comparable to MDA as it employs circular transmission of RTS only, and does it in all sectors (even the “empty” ones). Finally, DMAC has the poorest performance as it causes many collisions due to the hidden terminals.

7.6.2 Impact of Topology on Directional MAC Performance

We have observed that the performance of directional MAC scheme depends heavily on the type of topology under consideration. Therefore, in addition to the linear topology discussed before, here we present three different topologies and show the impact. We then conclude that a better way to compare different directional MAC schemes is through random topologies, which are discussed in the next section. In this section we study the impact of deafness and the cost of circular RTS and CTS for different MAC schemes for specific topologies. In the following set of simulations, we consider each node to be equipped with eight antenna beams.
7.6.2.1 Absence of Deafness

As shown in Figure 7.6(a), our first topology comprises of four nodes all within the radio range of each other, wherein node S communicates with R and node A communicates with node B. With this setup, deafness does not arise as the flows are pair-wise node distinct. Also, node A uses the same antenna beam to reach B and S. In this particular topology, with directional antennas the communication between A and B, and S and R can go in parallel without any interference.

As evident from Figure 7.6(b), this is an ideal case for DMAC as no deafness is present (the main reason behind performing any kind of circular RTS or CTS); and hence both flows can go on simultaneously without interfering with each other. Among the directional MAC schemes simulated, CRM performance is found to be the worst. This is because CRM transmits RTS in all beams in a circular sequence; which delays the transmission of DATA packets. Also, after node A receives a circular RTS from node S in CRM, node A sets its DNAV towards S which prevents it from communicating with node B during the entire transmission duration of S and R. Finally, MDA outperforms both 802.11 and CRM as it does not send RTS or CTS through all beams. In addition, by using the concept of EDNAV the communication between nodes A and B, and nodes S and R can go in parallel.
7.6.2.2 Persistent Hearing of DATA Packets

In the second topology, we analyze the impact of persistent DATA reception on different directional MAC schemes (this issue has been elaborated in Section 7.4). To simulate this effect we have created a topology with four nodes as shown in Figure 7.7(a), where node B is a neighbor of nodes S and R whereas node A is neighbor of B only. Here, node S communicates with node R while node A communicates to node B. Note that S uses the same antenna beam to reach B and R, whereas it uses a different beam to reach A.

Figure 7.7(b) shows the simulation results obtained for the scenario of Figure 7.7(a). Amongst the directional MAC schemes, MDA outperforms both DMAC and CRM. This is because whenever node B receives an RTS from node S it concludes that it can interfere with the communication between S and R, thus setting its DNAV towards S and switching off the corresponding beam for node S’s entire transmission. As a result, node B is able to freely communicate with A, as node A’s RTS is received at a different antenna beam. Clearly, this is possible neither in DMAC nor in CRM as node B is kept busy in both of these schemes by the entire RTS/CTS/DATA/ACK exchange between S.
and R, and hence becomes deaf to the RTS sent from A. At lower data rates, however, nodes have more time to share the channel and hence the impact of deafness, circular RTS and CTS, and persistent DATA hearing is minimized, and can be seen from Figure 7.7(b).

![Topology and Throughput](image)

Figure 7.7 – Impact of persistent hearing of DATA

### 7.6.2.3 Topology with Deafness

We now study the effect of deafness on directional MAC schemes. We create a topology with three nodes as shown in Figure 7.8(a). Here, node S acts as a source for node R, whereas it is a destination for node A. Also, node S uses different antenna beams to reach R and A. In this particular scenario, unless node S uses some sort of circular mechanism to inform its neighbor A about its communication with R, node A will be totally unaware of such communication. Here we assume that all nodes are within radio range of each other.

Figure 7.8(b) shows the simulation results for this particular scenario. As we can see, 802.11 outperforms all directional MAC schemes mainly because it is not involved in any
kind of circular RTS/CTS which adds extra delay and it does not suffer from any kind of deafness given that all the nodes are within radio range. Let us now turn our attention to the performance of directional MAC schemes. At lower data rates (up to 400 Kbps), the performance of all three directional protocols are similar. At 600Kbps, however, both MDA and CRM outperform DMAC. This is because both of these schemes are able to inform their neighbors about their communications and hence can efficiently share the channel. This is not the case in DMAC. Because of the deafness, only one of nodes A and S can acquire the channel while the other repeatedly sends RTS packets which, obviously, will not get a response. These unsuccessful transmissions of RTS increment the size of the contention window and, especially, of the SRL that when exceeds seven (NS implementation of 802.11), forces the MAC to report a “node unreachable” failure to the routing layer. The routing layer, in turn, initiates a new route discovery procedure usually by flooding. Although the negative effect of route discovery is not so severe in this scenario (with only 3 nodes), it may adversely affect the network performance in large networks.

![Figure 7.8 – Impact of deafness](image.png)

(a) – Topology  (b) – Throughput

**Figure 7.8 – Impact of deafness**
An interesting situation arises in DMAC when the data rate exceeds 800 Kbps. Here, one flow takes over the channel leading to the complete starvation of the other flow. This is the result of deafness which totally dominates the communication in DMAC. Results show that from 800 Kbps the aggregate throughput in DMAC is actually the throughput of a single flow. CRM and MDA, on the other hand, are able to share the channel given their transmissions of RTS/CTS. Among these two, MDA achieves better performance given its improved schemes. We would like to note that although fairness is out of scope of this work, channel capture is something to be avoided given that it leads to a negative impact on the overall network performance, especially when we consider protocols such as TCP.

7.6.3 Random Topology

As shown in the previous section, the performance of directional MAC schemes depends heavily on the type of topology being investigated. A better way to compare the performance of different protocols is then through random topologies where source and destination pairs are also selected randomly.

7.6.3.1 Gain by Spatial Reuse

Initially, we first evaluate the performance of different MAC protocols when all nodes are within radio range of each other. Given that the shortest transmission range is 250 meters in case of IEEE 802.11, all the nodes are confined within a circle of 250 meters diameter in the network topologies evaluated here. By doing so, we plan to evaluate the
spatial reuse gain provided by directional antennas as compared to omnidirectional antennas. In the next section, we will focus on the gain by increased coverage range.

We consider a scenario comprised of 16 nodes randomly distributed. We have run a total of 10 random topologies and the results presented here are the average of their individual results. In each scenario, we randomly select five nodes as source, which then randomly select five other nodes as destinations. As a result, some nodes can act as both source and destination which may lead to deafness.

A. Aggregate Throughput

Figures 7.9(a), 7.9(b), and 7.9(c) show the aggregate throughput of each directional MAC schemes when nodes possess four, eight, and twelve antenna beams. Intuitively, IEEE 802.11 performance is practically the same when all stations are within the radio range of each other.

Given all the nodes are within the radio range of each other, IEEE 802.11 does not suffer from deafness, does not have any sweeping delay and all the flows tend to share the channel. On the other hand, by randomly selecting source and destination nodes leads to situations where a single node is both source and destination, hence increasing the chances of deafness in DMAC. Due to a larger number of nodes, the effect of deafness on DMAC is considerably more severe than what has been shown in Section 5.2.3. Therefore, in this scenario the network is overloaded with route discovery packets as more nodes rebroadcast the route request, hence affecting the overall data throughput.
In Figure 7.9(a), we observe that MDA outperforms all other schemes including IEEE 802.11. It is also interesting to note that CRM performance is inferior to IEEE 802.11. CRM spends a lot more time than MDA performing the circular transmissions. In
addition, it often happens that when a transmitter node using CRM is performing its CDT, one of its RTS happened to collide at its intended receiver with some other CDT of RTS carried out by other nodes. Thus, many circular RTS transmissions end up being useless while they still prevent neighbors from transmitting for the entire duration.

When the number of antennas increases from four to eight and twelve (Figures 7.9(b) and 7.9(c)), we see that MDA performance is further enhanced by increased spatial reuse. As for CRM, its throughput is again below that of IEEE 802.11. Once more, with increase in the number of antenna beams, CRM carries out far too many CDTs. In conclusion, we believe that CRM may not be a good solution when the number of antenna beams is high as it generates too much overhead. On the other hand, the performance of DMAC improves with the increment in the number of antenna beams. This can be attributed to the fact that a higher number of antenna beams leads to more room for spatial reusability, although it also increases the chances of deafness as nodes are reachable through different antenna beams. This is why the performance of DMAC is still close to IEEE 802.11 as the increase in spatial reuse is offset by increased deafness.

B. Average Delay

It seems to be general consensus that directional MAC protocols employing some sort of CDT to inform their neighbors about their anticipated communication add extra delay. While this seems to be true, they hardly show the delay associated with deafness. In deafness scenarios, each unsuccessful transmission of RTS doubles the size of the contention window and hence the delay associated with the delivery of the packet. In the
following set of simulations, we evaluate the impact of deafness and CDT on the average end-to-end packet delay.

In calculating delays, we do not consider packets which are dropped. Our delay is based only on the packets which are successfully received at the destination. At the end of the simulation, and for a given node, we divide the total delay associated with all packets with total number of packets received as to calculate the average delay at that node. We then get the average delay for all nodes. Figures 7.10(a), 7.10(b), 7.10(c) show the corresponding results for four, eight and twelve antenna beams.

Surprisingly, the average delay in MDA proved to be better than all of the simulated directional MAC schemes and, in the majority of cases, also better than IEEE 802.11. Indirectly, the results show that sweeping is not the only factor which contributes to packet delay; rather, the impact of deafness is more detrimental. After each unsuccessful transmission of RTS, a node backs off which increases the delay for not only this packet but also for the all the packets waiting in the queue. As more RTSs fail, they add on the delay for each packet. Eventually, a node may have to resort to a router discovery procedure which considerably increases the delay. This is why the delay of DMAC is inferior to MDA. Also, the lower delay of MDA is not only due to its optimized DOD procedure which tackles the deafness problem, but it is also due to EDNAV which helps in channel sharing and hence a decrement in the delay associated with each packet.

Despite using CDT of RTS, CRM has a higher delay than DMAC. First of all, nodes receiving an RTS or CTS in CRM, always set their DNAV. Thus, CRM does not make a good use of spatial reusability, which forces packets to wait longer in the queue. In addition, CRM also suffers from deafness at the receiving side. Finally, delay
characteristic of IEEE 802.11 outperforms CRM and DMAC in all cases. Whenever nodes are within radio range of each other, IEEE 802.11 does not suffer from deafness while the only delay is due to channel sharing, which forces packets to wait in the queue.

C. Average Energy Consumption

In this section we evaluate the average network energy consumption. Our focus here is to analyze the impact of sending of multiple RTS and CTS, deafness (sending of multiple RTS and, as a consequence, a possible route discovery) and persistent hearing of DATA (reception of DATA packets not intended for a node) on the overall energy consumption. We calculate the total data delivered per unit of energy consumption (or, Mbits delivered per Joule) for each of the directional MAC schemes and IEEE 802.11. This is calculated as the total data delivered by all the flows divided by the total amount of energy consumption over all nodes (Mbits/Joule). The energy consumption is calculated based on the three parameters, namely, the power at which a packet is transmitted, the energy consumed in sending a packet, and the energy consumed in receiving a packet.

As shown in Figures 7.11(a), 7.11(b), and 7.11(c), in spite of doing DOD transmissions for RTS and CTS, the energy consumption of MDA is found to be minimum as compared to all other schemes including IEEE 802.11. The main contributor towards better energy performance of MDA over other schemes is the selective reception of DATA packets. In MDA, a node which receives an RTS which is not meant for it, switches off (i.e., becomes deaf) its corresponding antenna beam for entire DATA duration. As DATA packets are usually large, nodes spend a considerable amount of energy in packet
reception. By switching off the antenna beam, the nodes save a significant amount of energy. Performance of DMAC is far below MDA, but it performs better than IEEE 802.11 and CRM. It is important to note that as the number of antenna beam increases, we obtain a better energy performance for DMAC. This is because that with an increment in the number of beams, there are fewer nodes which are covered through same antenna beam. Thus, an increasingly smaller number of nodes receive packets which are not meant for them, resulting in energy savings. However, in DMAC nodes in the communication path between source and destination still spend a considerable amount of energy in receiving unwanted packets. CRM, in turn, performs worst than DMAC as it not only receives unwanted DATA packets, but it is also involves sweeping of RTS. Finally, the performance of 802.11 is inferior to both MDA and DMAC, and this is because that almost all nodes in the vicinity of a transmission receive all the packets.

7.6.3.2 Gain by Increased Coverage Range

Contrary to the previous section, here we focus on the second advantage of directional antennas, namely, the increased coverage range due to directionality. Therefore, in this section we evaluate the performance under scenarios where not all pairs of source and destination nodes are within radio range of each other. Given that IEEE 802.11 range is 250 meters, it may have to resort to the routing protocol in order to deliver a packet to a particular destination. On the other hand, it may be the case that MDA, CRM and DMAC do not need to resort to routing as they can transmit for longer ranges.
For the scenarios that follow, we have used the DSR routing protocol [51], and the distance between pairs of source and destination nodes is uniformly distributed between $[350, 750]$ meters depending on the number of antenna beams being used. Note that we
need to add extra nodes in order to keep the network always connected. We have simulated a total of 10 scenarios and the results presented are the average of their individual results. As the results exhibit the same trend for the various numbers of beams and due to space limitations, here we present the results for eight antenna beams only. Figures 7.12(a), 7.12(b), and 7.12(c), show the throughput, delay and energy characteristics for scenario under investigation.

As expected, the directional MAC protocols considerably outperform the omni-directional IEEE 802.11. Similar to the Section 5.3.1, MDA is shown to provide the best performance among all protocols considered given its unique combination of components, while CRM performance is inferior to DMAC for similar reasons to those already discussed.
8. Deafness and Self-Induced Blocking in Directional Antennas

8.1 Introduction

Some major issues still need to be addressed to make directional antennas an attractive alternative for MANETs. For example, the increased instances of deafness in directional antennas needs to be properly handled as it may drastically impact the network performance. Hence a detailed investigation is needed to determine different factors that contribute to deafness. A second important issue with the performance of directional MAC protocols is the way buffering is provided in the MAC layer. All the aforementioned protocols, including MDA, assume a traditional network layer model where the link layer has a single queue of packets waiting to be handed over to the MAC layer which has a single buffered entity. Whenever the network layer has a packet to send, it determines the next hop for the packet and places it in the link layer queue. In case MAC is in IDLE state, it signals for a packet from the link queue and subsequently buffers it. It then determines the antenna beam required to transmit the packet and enters into SEND state. The MAC will only request another packet from the link layer queue when it has successfully transmitted or given up (e.g., the next hop is unreachable) on the packet currently being handled. In existing directional MAC protocols, in the event that
the packet to be transmitted is for a beam whose DNAV was set, it waits for the medium to become idle. While doing so, it could so happen that other packets in the link layer queue could be transmitted over beams which are not busy at that time. In such a scenario, waiting for the medium to become idle reduces overall throughput of the system. We call this as “self induced blocking” phenomenon which results from using a single MAC buffer for all antenna beams.

We are planning to handle each of the MAC layer issues separately. In the following section we give a brief description of the problem associated with deafness, self induced blocking and outline our approach to solve them.

**8.2 The Deafness Problem**

In general, deafness is caused when a node X repeatedly attempts to communicate with node Y, but is not successful, because Y is presently tuned to some other antenna beam. At each unsuccessful attempt, the backoff interval is doubled hence degrading network performance. Deafness may also occur if Y’s DNAV is set in the direction of X and hence it is unable to reply with a CTS. In this section we outline different scenarios which may cause deafness. We refer to Figure 8.1 for illustration purposes and assume an ongoing communication between nodes S and R. Obviously, severity of deafness depends on the specific MAC protocol under consideration; hence we also explain which protocol is more susceptible to what kind of deafness. We have classified directional MAC protocols into four categories based on how they transmit the RTS/CTS: ORTS-OCTS, ORTS-DCTS, DRTS-OCTS, and DRTS-DCTS.
Figure 8.1 - Deafness in Directional Antennas

- **Destination engaged in communication:** This kind of deafness problem is more prevalent in DRTS-DCTS protocols like DMAC. DMAC sends RTS and CTS only in the direction of its prospective destinations. Hence, there is no way a third node which is reachable through a different antenna beam will come to know that its intended destination is currently engaged in a communication. In Figure 8.1, since node S sends its RTS only in antenna 1 (towards node R), there is no way its neighbor node D can determine that S is presently engaged in a communication with R. As a result, if D sends an RTS to S, it will not receive any reply as S is presently tuned to beam 1 and hence is deaf to beam 2. Schemes using ORTS-OCTS can better overcome this problem since they try to send RTS and CTS through all beams. ORTS-DCTS and DRTS-OCTS are similar to DMAC with the difference that the impact of deafness is now confined to the neighborhood of the destination or the source side, respectively.

- **Persistent hearing of DATA:** This kind of deafness problem occurs in almost all directional MAC protocols. When a node sends RTS/CTS (either directional or omni), all neighbors who receive it set their DNAV accordingly. Whenever the source node starts transmitting DATA, neighboring nodes which are reachable through same
antenna beam and are currently idle (e.g., node C in Figure 8.1) move to directional mode to receive the DATA packet, hence becoming deaf to all other directions. For example, although node C in Figure 8.1 knows about the communication between S-R as it received the previous RTS/CTS, it still moves to directional mode so as to receive the DATA packet. Therefore, if node F tries to send an RTS to C (beam 4) during the data transmission between S and R, node C will not reply as it is tuned to node S’s DATA transmission. This result in a poor spatial reuse and negatively impacts overall system throughput. In Section 8.2.2, we will outline a scheme to overcome the persistent hearing of data packet at a destination node.

- **Precautionary Deafness at the Receiver:** This is a different variant of the problem discussed above wherein a receiver node avoids sending CTS if it knows that it may result in collision with an ongoing transmission. For example, let us assume that node C wants to send an RTS to node E (reachable through beam 2) and its DNAV is only set in beams 1 and 3 due to ongoing transmission between S and R. Obviously, node C is unaware of the fact that the antenna used by node E to receive packets from C and S is the same. Thus, if node C sends an RTS to E, it will either result in a collision at E or E will avoid sending a CTS back to C as its DNAV in that particular antenna beam is already set. Mostly all directional protocols suffer from this deafness since there is no way a source node can determine if its destination’s beam towards him is blocked or not. By assuming neighbor location information availability, in Section 8.2.2.1 we will outline a scheme which handles this kind of deafness.

- **Unheard RTS/CTS:** Suppose node D wants to communicate with E while transmission is going on between S and R. In this scenario, as S is tuned to antenna
beam 1 it will miss the RTS/CTS handshake between D and E (if sent in his direction), and hence will be unaware this future communication. When node S finishes communication with R and if it has any packet to be sent to either node D or E, it will unsuccess fully attempt to communicate with these nodes given that its DNAV is not set towards the corresponding directions. This problem exists in almost all directional MAC protocols and is difficult to handle.

8.2.1. Impact of Deafness on Network Performance

Deafness not only degrades the performance at the MAC level, but it also considerably affects the performance of higher layers. Whenever a node sends an RTS and does not receive back a CTS, it backoffs (according to IEEE 802.11) and tries to retransmit the RTS at some later time. This amounts to excessive wastage of network capacity in control packet transmission. Larger backoff intervals also result into unfairness wherein a flow completely captures the wireless shared medium. To illustrate this, assume that in Figure 8.1, two flows are present in the network: flow S-R from nodes S and R, and flow E-S from nodes E and S. We have simulated this scenario and the result of individual flow throughput is shown in Figure 8.2. As we can see, after a specified sending rate the flow S-R captures the medium forcing the flow E-S to completely shut down. This is because node S becomes deaf in the direction of node E, as the flow S-R is constantly sending packets.

The impact of deafness on the routing layer is also very severe. Each consecutive unsuccessful transmission of a packet (RTS or DATA) at the MAC causes the increment of a variable called Short Retry Limit (SRL). In the IEEE 802.11 standard, an SRL
threshold is maintained (with default value equal to 7) that controls the number of packets transmission attempts made before a send failure is reported to the routing layer. The way SRL has been set in IEEE 802.11 assumes an omni-directional antenna is in place. If a node is not able to reach its destination in 7 attempts, it reports a route failure to the routing layer which, in turn, initiates a route discovery procedure throughout the network. Clearly, this results in considerable network performance degradation, as route request packets are often flooded. One possible solution would be to increase the value of SRL (e.g., multiply it by the number of antenna beams), but it might not be an efficient solution for two reasons. Firstly, higher values of SRL mean longer delays in discovering the movement of a destination node; secondly, even a higher value of SRL does not guarantee that a route request will not be triggered while it may only delay it. In Section 8.2.2.2 we outline an improved method to handle SRL in directional antenna systems.

The impact of deafness is severe in the route discovery phase as well. This problem is outlined in [82] where a node misses a better route to its destination as one of the nodes in the shortest path was deaf to its route request broadcast packet and hence was not able to reply back.

Finally, deafness may also impact the performance of the transport layer. Deafness may preclude a node from receiving a TCP ACK, for example. Clearly, this negatively impacts TCP performance as it may continuously enter its congestion control mechanisms.
8.2.2. The Proposed Schemes

Although, in practice, it may not be feasible to completely overcome all deafness scenarios as discussed in Section 8.2, we can certainly minimize its effect. To this end, we propose such enhancements to directional MAC protocols which proactively try to prevent deafness situations.

Our first proposed enhancement attempts to eliminate deafness caused by persistent hearing of DATA, and is implemented by smartly handling the RTS/CTS handshake. For example, in Figure 8.1, after receiving RTS (antenna 3) and CTS (antenna 1), node C sets its DNAV accordingly. During the remaining duration of DATA transmission between S and R, C does not go to directional mode in antenna 3. With this, we are suggesting that node C should become deaf to its antenna beam 3 for duration of node S’s DATA transmission. It is to be noted that a similar approach cannot be adopted for antenna 1 (CTS reception antenna). This can be argued by the fact that the ACK transmission duration is very small as compared to that of DATA duration. If node C also becomes deaf in antenna 1, it may miss important control or broadcast packets from other nodes.
Note this would not happen in antenna 3 mainly because collisions may occur with ongoing DATA packets.

The implementation of the aforementioned enhancement is very simple. We just added a flag in the DNAV table maintained at each node. This flag basically indicates if the DNAV presently set was originally due to an RTS or not. It is worthwhile to note that this kind of deafness problem affects other nodes only at the antenna beams used by the sender and receiver to communicate (node S’s beam 1 and node R’s beam 3 in Figure 8.1). Hence, neighboring nodes receiving an ORTS/OCTS through a different antenna beam do not suffer from this kind of deafness. We have enhanced our protocol with this feature.

In our second proposed enhancement we assume that each node is aware of the location of its neighbors and uses the same number of antenna beams (NUM_ANTENNA_BEAMS). We also assume that all nodes use the same directional antenna patterns and can maintain the orientation of their beams at all times. Given the location information of its neighbor node Y, a node X can calculate Antenna(Y,X), the antenna used by the neighbor Y to reach X as given in equation (1). In the following subsection we describe how this information can be used to handle deafness.

\[ \text{Antenna}(Y, X) = \left\lfloor \frac{\text{Angle}(Y, X)}{\text{NUM\_ANTENNA\_BEAMS}} \right\rfloor \]  

(1)

### 8.2.2.1 Estimating Destination Status

Based on RTS/CTS, each node maintains a neighbor transmission table (NTT) for all ongoing transmissions in its neighborhood. The NTT stores the source node address
which sent the RTS and the duration of the corresponding transmission. As for the CTS, we have made one modification to its header. CTS now also include the sender address too.

![Figure 8.3 - Proactive Handling of Deafness](image)

Given the above modification, if a node X wants to send an RTS to node Y, it first verifies if the DNAV for the antenna beam used by X to reach Y is set. If it is, X defers its transmission. Otherwise, X searches all ongoing transmissions in its neighborhood by checking if the duration field in any entry of its NTT is set. If the resulting set is non-empty, by equation (1) node X calculates the beam its destination node Y is going to use to reply with a CTS, say $A_{Y,X}$. Then, for each node T in the NTT whose duration field is set, it verifies if the antenna beam used by T to reach Y, say $A_{T,Y}$, is equal to $A_{Y,X}$. If so, node X determines that a collision may take place and defers sending its RTS for the corresponding duration.

To illustrate this scheme please refer to Figure 8.3. Let us assume that S and R are presently engaged in a communication and node A wants to communicate with B. First of all, our first enhancement ensures that once the RTS and CTS from S and R is over, node A becomes deaf to antenna beam 3, while it can still receive and reply in antenna beam 1, 2 and 4. Without the second enhancement, if node A sends an RTS towards B, B will not
reply as its DNAV is set for beam 4 and hence it is deaf in the direction of A for the
duration of the DATA communication between S and R. The second enhancement
enables node A to overcome this by determining in advance if it should or not send the
RTS. To do so, node A checks if Antenna(B,A) is equal to Antenna(B, S). Since A is a
neighbor of S, R, and B, it has the location information for all of them and hence can use
equation (1) to calculate the corresponding antenna beams. Once determining that
Antenna(B,A) is the same as Antenna(B,S), node A defers the transmission of its RTS for
the corresponding duration field of node S. This prevents unwarranted transmission of
RTS from node A. Please note that node A does not need to be a neighbor of both source
and destination, so as to calculate the various antenna beams. Being a neighbor of the
destination suffices as CTS packets now carry the information about the sender too.

8.2.2.2 Handling of SRL in Directional Environment

As outlined in Section 8.2.1, in IEEE 802.11 standard, an SRL threshold is maintained
(with default value equal to 7 in most of the implementation) that controls the number of
packets transmission attempts possible before a send failure is reported to the routing
layer. However the absence of reply from a destination may be contributed by several
factors. For example in an omni-directional environment, a receiver might not have
received RTS correctly (collision), it may be an exposed terminal, its CTS might be lost
or it is moved out of the transmission range of the sender. On the other hand, in
directional environment, assuming the nodes are static, the main factor which contributes
to the increment of SRL is beamforming (deafness) of a receiver in a different direction.
Hence, it is necessary to identify absence of a reply because of beamforming of a receiver and in those cases special handling of SRL is required. For example, a sender node should not report a broken link error if it can detect that the absence of reply was because of its destinations beamforming in a different direction. However, the question remains how a source node S will know if its destination R is not able to reply because of beamforming. Here we argue that, depending on the type of directional MAC protocol employed, a sender can determine absence of reply because of deafness by continuously listening (MAC layer snooping) the packets in its neighborhood.

In proposed approach, if node B receives an RTS from S, and if it has a packet to sent to S, it resets its SRL as well as its contention window. We argue that resetting of contention window in this case helps node B to reach S, during S post-backoff period. We have incorporated this feature in our proposed enhancements of directional MAC protocols.

### 8.2.3. Performance Evaluation

In addition to the directional antenna module, we have also implemented ORTS-OCTS (referred as OMAC), and DMAC schemes. We used dynamic source routing (DSR) as the routing protocol for our simulation work.

For the simulations that follow, we have considered CBR traffic sources at data rates of 200, 400, 600, 800, 1000, 1200 and 1600 Kbps, and we measure the total network aggregate throughput of all flows. In addition, we evaluate DMAC, OMAC, and the proposed Enhanced DMAC (E-DMAC) and Enhanced OMAC (E-OMAC) schemes, for four and eight antenna beams with transmission ranges of 350 and 550 meters,
respectively. To reduce the sweeping overhead in OMAC, in E-OMAC nodes send the RTS-CTS only to beams with neighbors (similar to MDA). Also, in all the scenarios we consider a 2 Mbps network with no node mobility. For the radio propagation model, a two-ray path loss model is used. Since DMAC requires prior knowledge of neighbors’ location, we have provided all protocols with such information for a fair analysis.

We first evaluate the gain by using the first enhancement alone. To do so, we have created a topology as shown in Figure 8.4. In this scenario, node B is a neighbor of nodes S and R whereas node A is neighbor of B only. Also, node S sends packets to node R while node A sends packet to node B. Note that the antenna used by S to reach both B and R are same.

![Figure 8.4 - Persistent Hearing of DATA/ACK](image1)

![Figure 8.5 - Effect of persistent hearing of DATA/ACK](image2)

Figure 8.5 shows the simulation results obtained for this scenario. Amongst the directional MAC protocols evaluated, E-DMAC performs slightly better than E-OMAC. This is because E-DMAC does not employ circular directional transmission of both RTS and CTS which serves to inform the neighbors of a node about the intended transmission, thus minimizing hidden terminals. In the particular scenario of Figure 8.4, circular RTS/CTS does not provide any benefit for deafness as Antenna(S,B) is the same antenna
as Antenna(S,R), and the same is true with respective to node R. As the traffic increases, our proposed enhancement gives a considerable improvement for both the existing schemes. This can be argued by the fact that at lower traffic rate nodes have sufficient time to share the channel without being affected by neighboring transmissions, while it is not true for higher traffic rate.

In addition, Figure 8.6 shows that the enhanced scheme improves the sharing of the medium as opposed to the original scheme depicted in Figure 8.2. Although it is worthwhile to note that the improvement depends on the topology under consideration.

![Figure 8.6 - The Enhanced Scheme Prevents Channel Capture](image)

We now simulate a topology comprised of 16 nodes distributed in a 4 by 4 grid. Nodes are placed at a distance of 175 meters. We randomly select 4 source and destination nodes. We have simulated a total of 10 scenarios and the results presented here are the average of their individual results. In this set of simulations, we implement both of our enhancement schemes in OMAC. Figures 8.7(a) and 8.7(b) show the results when nodes...
possess four and eight antenna beams respectively. It is to be noted that in DMAC a sender does not employ any kind of sweeping mechanism to tackle deafness in its neighborhood (except the beam at which its destination is), hence we eliminate DMAC in following set of simulation results.

In Figure 8.7(a), we observe that for four antenna beams the performance improvement gained by using our enhanced schemes is marginal, whereas for eight antenna beams, we obtain a significant performance improvement as shown in Figure 8.7(b). This is due to the fact that as the number of antenna beams increases, chances of different nodes being at different antenna beams are higher thus increasing the likelihood of deafness scenarios.

(a) 4 beams

(b) 8 beams

Figure 8.7 – Throughput Gain by using Enhanced Scheme (Random Topology)

8.3 Handling *self induced blocking* in directional antennas
We propose to overcome the problem of “self induced blocking” in the Enhanced DAMA (DAMA: Directional MAC scheme which does sweeping of both RTS and CTS packets) protocol by employing a cross-layer design approach wherein the network layer is aware of different antenna beams at the MAC layer. The MAC, in turn, has separate buffers for each antenna beam. Accordingly, the link layer follows this approach by maintaining separate queues for each beam. The modified protocol stack of EDAMA is shown in Figure 8.8. As we can see, in ED the MAC layer has multiple buffers for each corresponding antenna beam, where each of them corresponds to a specific queue in link layer. In addition, EDAMA employs separate backoff timers for each these antenna beams to allow for simultaneous execution.

Figure 8.8 – Traditional and EDAMA protocol stack

In order to place the packet in the correct link layer queue, the network layer needs to determine the antenna beam which the MAC will use for transmission of this packet. We tackle this issue by augmenting the routing table with an additional entry called “Antenna
Beam”, which corresponds to the antenna beam the MAC uses to reach the corresponding next hop. This entry in the routing table is self-learning and its computation incurs no additional overhead. Whenever the MAC receives a packet from a node, it informs the network layer the antenna beam through which it received the packet. The network layer, in turn, updates the beam entry for that destination in the routing table. As time progresses, the network layer will eventually learn about the antenna beams used to reach each of its neighbors. In case the network layer’s beam entry field is empty for a given next hop, a simple broadcast is done when this entry is needed. We note, however, that this does not result in any overhead as the majority of existing routing protocols rely on some sort of broadcasting. As a result, once the network layer is aware of the destination’s antenna beam, it puts the packet in the link layer queue corresponding to this antenna beam. It is to be noted that broadcast packets are kept in a special dedicated queue as they are to be transmitted through all antenna beams.

In EDAMA, whenever the MAC enters an IDLE state it explicitly requests a packet from the link layer for which the DNAV is not set. In scheduling the next packet, we follow a simple round robin strategy for determining the next unblocked antenna beam. If no packets are available for that beam, then a packet for the next unlocked beam is sought. Upon receiving a packet, the MAC first stores it in the buffer allocated for this antenna beam and makes an attempt to transmit it. It may so happen that in the time interval between determining an antenna beam to be unblocked and actually attempting to transmit it, the beam may become locked (e.g., medium busy or DNAV set). In addition, the beam may get blocked while waiting for DIFS or backing off. In all these cases, we should first start backoff in this particular beam and then invoke the scheduler to move to
next available antenna beam. This is continued until the MAC receives a packet which it successfully transmits, or all the buffers for the each antenna beam are full. In the former case, the MAC uses the round robin scheduler to select the next antenna beam, whereas in the later case the MAC simply waits for one of its backoff timers to expire before attempting transmission. In case of a virtual collision (e.g., two backoff timers expiring simultaneously), their transmissions are attempted one after the other. We note that this is different from IEEE 802.11 where the MAC freezes the backoff counter and waits for the medium to be idle again before resuming it.

It is to be noted that round robin strategy to handle scheduling in MAC have several pitfalls. It includes increased delay and possible starvation of packets in a particular direction. Comparison of different scheduling algorithm is, however, beyond the scope of this work.

8.3.2 Performance Evaluation

As discussed in the previous section, one of the issues in directional antennas is the phenomenon of “self induced blocking” problem. As a result of this, if a packet for a particular antenna beam is blocked, the node will not be able to transmit in any other directions until the blocked packet is successfully transmitted. To illustrate the effect of single MAC buffer and corresponding gain by employing separate MAC buffers for each antenna beams as in EDAMA, we redefine random topology and run the simulations for 6, 12, and 18 antenna sectors. For the sake of clarity, in this set of simulations we have only considered the directional protocols DAMA, EDAMA and CRM.
In this scenario we simulate a randomly distributed topology of 16 nodes. Out of these 16 nodes, 3 are chosen as traffic sources that, in turn, randomly select two of its neighbors as destinations. We have simulated a total of 10 scenarios and the results presented here are the average of their individual results. The corresponding plots for 6, 12 and 18 antenna sectors are shown in Figure 8.9.

As can be seen from Figures 8.9(a), 8.9(b), and 8.9(c), EDAMA consistently outperforms DAMA and CRM. The throughput of these protocols is approximately the same for the case when each traffic source generates data at 400 Kbps. This is because, in this case, the network in under loaded and the benefits of directionality are not observed. Also, the effect of the “self induced blocking” problem or the circular transmission of RTS on throughput is minimal. However, as the network load increases the effect of the above factors become increasingly worse and considerably affects the performance of DAMA and CRM, while CRM is affected more because of its circular RTS.

![Figure 8.9 - EDAMA aggregate throughput in random topology](image-url)
9. Routing in Directional Environment

Although there are several attempts towards designing an efficient directional MAC scheme, design of a routing protocol tuned to the underlying directional environment has mostly remained unexplored. Existing directional routing schemes either assume a complete network topology beforehand [83] or simply use omnidirectional routing protocols [82] to forward packets in underlying directional environment. Here we argue that a routing protocol specifically tuned to the underlying MAC layer can reap interesting performance benefits. For example, in a directional routing protocol, a source node can exploit the antenna beam information towards its destination for an efficient route recovery. Keeping this objective in mind, in this chapter we are going to propose Directional Routing Protocol (DRP) for MANETs. Our contribution towards designing an efficient directional routing protocol can be summarized as follows:

I. A detailed study of issues related to routing in directional antenna systems. We also outline the behavior of different IEEE 802.11 system parameters in a multihop directional environment.

II. Designing a cross-layered directional routing protocol called DRP. The main features of DRP include an efficient route discovery mechanism, establishment and maintenance of directional routing and directional neighbor tables (DRT and DNT respectively) and a novel directional route recovery mechanism among others.
III. Comprehensive simulation comparison of DRP with DSR over both omni-directional and directional antenna models. Our simulation compares both static and mobile scenarios.

9.1. Related Work

In [81] authors propose a scheme to estimate the direction of the destination relative to the source in order to confine the spread of route discovery packets using directional transmission. However, the strategy is more effective for route rediscovery at the source. In addition, the flooding overheads due to directional sweeping have not been addressed. In DRP we propose a novel mechanism for the direction estimation based on the available route to the source. This mechanism is used both at source and intermediate nodes to provide a more robust mechanism to handle route failures.

In [83], notion of exploiting maximally zone disjoint routes to reduce the contention at the MAC layer has been introduced. Directional communication is shown to be effective in both discovery and use of such routes. But, the proposed protocols require all nodes to be completely aware of the network topology and ongoing neighborhood communications. A MAC and a proactive routing protocol over ESPAR antennas have been suggested in [84]. This is a complex MAC, incurring considerable control overhead. In [85], the authors illustrate the effectiveness of directional antennas by overcoming partitions introduced in the network due to the mobility of nodes. They advocate the use of larger ranges of directional antennas only in the event of a link failure. In [82] authors evaluate the performance of DSR over DMAC and omni directional antennas. Several
issues ranging from directional route discovery to mobility management are explored in
the context of directional communication, which is shown to be more effective when
topologies are sparse and random. However DMAC, as discussed in Chapter 7 is
susceptible to deafness and hidden node problems which limits its multi-hop routing
performance in many scenarios.

In this work, we attempt to provide a complete cross layer routing solution over single
switched beam antennas so that both the spatial reuse and larger ranges offered by these
antenna systems can be exploited. Our simulation results validate the efficacy of our
scheme.

9.2. Preliminaries

9.2.1 Dynamic Source Routing (DSR) Protocol

DSR is a source routed reactive routing protocol [51]. The protocol consists of two major
phases: route discovery and route maintenance. When a mobile node has a packet to send
for some destination, it first consults its route cache to determine whether it already has a
route to the destination. If no such route exists, it initiates a route discovery by
broadcasting a route request (RREQ) packet. This route request contains the address of
the destination, along with the source node’s address and a unique identification number.
All nodes, except the destination node, rebroadcast this packet exactly once. While doing
so, they append their own address to the route record field in the RREQ packet. Hence,
the path followed by this route request gets included in the RREQ packet.

On receiving the RREQ packet, the destination node responds by sending a route reply
(RREP) message to the source. Since a bi-directional link is assumed between all the
nodes, the route reply is a unicast message, following a path obtained by reversing the route followed by the route request. The route received at the source is cached for subsequent communication. DSR facilitates route maintenance through the use of route error (RERR) packets. In the event of a link failure at an intermediate node on a source route, a RERR packet is generated and sent to the source. All intermediate nodes including the source node remove all the routes in their caches which have that broken link. DSR also has provisions for nodes to learn and cache routes by overhearing RREPs or data packets containing source routes. Such cached routes can reduce flooding overheads in the network and reduce route discovery latencies.

9.3. Directional Routing Issues

In this section, we investigate different issues related to directional communication and their impact on routing. For the discussion below we assume that omni-directional DSR protocol running over a single switched beam directional antenna system. This will serve as a foundation for developing our DRP protocol.

9.3.1 Directional Broadcasting Overhead

In a single switched beam directional antenna systems, sweeping is needed across all antenna beams in order to cover a node’s one hop neighbors. Each forwarding node, in effect, transmits $M$ (the number of antenna beams) packets into the network. For a single switched beam antenna system, this adds to both packet redundancy and delay. Since the Route Request (RREQ) packets are flooded throughout the network, an inefficient broadcasting strategy may negatively impact the quality of routes [82] source node gets.
Hence, a careful route discovery is necessary to obtain optimal routes with minimal route discovery latency (RDL) and redundancy. In DRP, we employ a novel directional broadcasting strategy (described in Section 9.4.2.1) aimed at reducing the broadcast redundancy and RDL.

9.3.2 Address Resolution Protocol (ARP) in Directional Environment

Once a destination node receives a RREQ packet, it sends a unicast a route reply (RREP) back to the source (assuming a bi-directional link). However, before forwarding the RREP packet, the destination needs to do an ARP to obtain the MAC address of its previous hop (this is also true for all intermediate nodes forwarding the RREP packet). Since the ARP-Request is a broadcast packet, nodes will do a sweeping to locate its previous hop. However, sending ARP-Request through sweeping has some potential problems in directional environment. To illustrate please refer to Figure 9.1, wherein node D is the final destination of a RREQ packet, and it needs to send the RREP back to the source through an intermediate node C.

As shown in Figure 9.1(a), after receiving the RREQ (step 1), and before sending its RREP, node D is required to sweep a ARP-Query to obtain the MAC address of node C. If at the instant when node D broadcasts its ARP-Query (step 2) towards node C, node C is beamformed in other direction to sweep its RREQ packet (RREQ is a broadcast packet), the ARP-Query at node D will fail.
(a) – Interaction between DSR RREQ and ARP-Query

(b) – Interaction between ARP-Query and ARP-Response

Figure 9.1 – Directional ARP Issues. Node D is the final destination and node C is the immediate preceding hop

A similar situation can also arise for ARP-Query and ARP-Response as shown in Figure 9.1(b), wherein node D can miss ARP-Response from C because of being beamformed in other direction to transmit ARP-Query. To tackle this issue, we recommend a directional broadcast of an ARP-Query packet. Since D is aware of the antenna beam required to reach its previous hop C (the beam where D received the RREQ packet from C), rather than sweeping, it can send the ARP-Query only in the desired direction. This eliminates the redundant transmission of ARP-Query packets, and minimizes the chances of RTS failures.

It is to be noted that node D remains deaf for the entire duration of ARP-Query sweeping. Hence it may miss a RREQ packet with a better route, received from some alternate path. This issue has been studied in [82]. In order to increase the chances of obtaining optimal routes, we extend the idea of delayed route reply as proposed in [82]. In DRP destinations delay sending the RREP by a time duration $T$, calculated from the time it received the first RREQ. This additional time will allow the destination node to pick the best amongst
all routes which arrive within the time duration $T$. We take $T$ as the time required for a complete sweep.

### 9.3.3 Directional Antenna Beam Handoff

Another important issue to address in designing a directional routing protocol is the movement of a nexthop within the transmission range of a node. In a single switched beam directional antenna system (where a transmitter has no way to continuously track the location of its nexthop) special care needs to be taken for the case where the next-hop moves, and is reachable through a different antenna beam (direction) from the sender.

A recent directional MAC protocol [76], suggests sending RTS packet to all antenna beams. Hence the sender need not worry about the movement of its nexthop within its transmission range, since RTS is sent to all the antenna beams. On the other hand, it may result in excessive control overhead as well as delay because of the sweeping involved in each RTS transmission. Some approaches [78, 82] first try to reach the destination in its previous beam location, and after $m$ such RTS failures ($m < 7$) (e.g., for example, in [78, 82], $m$ is 5), the remaining RTS are sent to the all antenna beams (referred to as *scanning*).

However, in DRP we claim that a relationship exists between the beamwidth and the number of adjacent beams which should be scanned. For example, as shown in Figure 9.2, even if node $B$ is a neighbor of $A$ (after movement from beam 0 to beam 4), the link from $B$ to $C$ is already broken. In DRP, we take this into consideration and employ an efficient and novel algorithm for scanning adjacent beams as described in Section 9.4.2.2.
9.3.4 Deafness and Node-Movement

Effects of deafness on route discovery are well understood in the literature [82]. However, the relationship between deafness and node movement has not been adequately investigated [86]. For example, even if the next-hop (receiver) has not moved out of the transmission range of the sender, an absence of CTS from the receiver due to deafness may be perceived as a link failure by the sender. This may ultimately result in a route error leading to a new route discovery.

MDA (MAC layer of DRP, described in Chapter 7 together with scheme proposed in [86]) has some provisions to distinguish deafness from node movement. Consider a node $X$ which has a packet for its next-hop $Y$. For example, MDA requires any sender/receiver to explicitly inform all its one-hop neighbors of any of its ongoing transmissions to avoid collisions and deafness. This is achieved by a circular transmission of RTS/CTS packets and the setting of a Directional-NAV (DNAV) in each beam. Hence, $X$ will be aware when $Y$ is busy in some other transmission/reception. It would only initiate a transmission towards $Y$ when its DNAV towards the direction of $X$ is free. With this
support at the MAC layer, a node may reasonably comprehend that the absence of a CTS in response to a RTS is primarily due to node movement.

9.3.5 Directional Neighbor Discovery

A node at any time needs to be aware on which antenna beam its one hop neighbors lie. This information is necessary for the sender’s MAC to resolve the beam in which it must initiate communication. A periodic exchange of hello packets amongst all the nodes is the most trivial solution to this problem. However, as discussed before, a directional broadcast amounts to a lot of overhead. In addition to the large number of packet transmissions, the broadcasting node becomes deaf during the entire sweeping duration. To eliminate these, we propose a novel method of both establishing and maintaining a directional neighbor table. In DRP, a directional neighbor table (DNT) is established during the route discovery phase. To this end, DRP uses routing control packets such as RREQ and RREP to facilitate neighbor resolution. Any neighboring node Y which receives this packet on its beam “i”, can easily comprehend that it needs to send a packet on its “i

th” beam in order to communicate with X. Similarly, with the RREP packet, node X can also resolve node Y to one of its antenna beams. In addition, similar to [81] DRP employs MAC layer snooping for maintaining the DNT. By setting the MAC in a promiscuous mode, a node overhears all the traffic in its vicinity. By simply overhearing these packets, a node updates its DNT as well as track new neighbors in its surroundings.

9.3.6 Anomaly of Directional Multihop Packet Forwarding

It has been shown that, directional communication suffers from an increased instance of hidden terminal problem in a linear scenario (MDA in Chapter 7). Unfortunately the
route obtained for a specific destination, is more likely to have some linear path. For example, in Figure 9.3, let us assume that a part of the route to a destination follows a linear path \([X, Y, Z]\).

Let us now analyze the effects of linearity of path on directional packet forwarding. Node \(X\) after a successful DATA transmission to \(Y\) will begin its post-backoff before its next transmission attempt. In the meantime, \(Y\) will attempt to forward the packet to \(Z\). While \(Y\) is sending its RTS to \(Z\), if the post-backoff of \(X\) expires and it has another packet for \(Y\), it will initiate RTS towards \(Y\). Several unwanted side effects may result because of this. First it may result into a packet collision at \(Z\), and force \(Y\) to try again. Secondly, at \(X\), the RTS will fail (deafness at \(Y\)) and it will increment its STA Short Retry Count (SSRC) [1].

![Figure 9.3 - Multihop Packet Forwarding](image)

In essence, the post-backoff period is designed for omni environment, where a node can listen about the transmission in its neighborhood. On the other hand, in a directional environment the post backoff period may not be sufficient for a node (\(Y\) in this case) to complete sweeping and inform all its neighbors about its transmission. It is to be noted that the presence of hidden terminal problem is more severe for the case when the nodes do not employ a circular sweep of RTS, which increases the chances of DATA packet collision because of their longer duration.
One way to handle this issue is to increase the post-backoff period for directional antenna systems and make it at least equal to the duration of one complete antenna sweep. In this manner $Y$ can complete its circular sweep of RTS and inform $X$ about its transmission to $Z$. However, pause and resume functions involved with the backoff mechanism may force the node to wait for long and hence can negatively affect channel sharing. An alternative way to handle this issue would be to introduce the concept of post-defer after each successful DATA transmission. However, designing an optimal post-backoff or post-defer period in directional environment is an open issue and beyond the scope of this paper.

### 9.4 Directional Routing Protocol (DRP)

DRP is an on-demand directional routing protocol, and is inspired in large by omnidirectional Dynamic Source Routing (DSR) protocol used heavily in MANETs. DRP closely couples the routing layer with the MAC layer and assumes a cross-layer interaction between some of the modules. DRP is built on top of an underlying directional MAC scheme called MDA (described in Chapter 7). A pictorial view of the protocol stack of a DRP aware mobile node is shown in Figure 9.4. In DRP the Directional Routing Table (DRT) is local to routing layer and maintains the routing information to different destination. The Directional Neighbor Table (DNT) on the other hand is shared with MAC.
Unlike DSR which maintains only the index of the node ID in a forwarding path; DRP also maintains node indices and the beam IDs used by the nodes to receive a packet in the forwarding path. The beam ID stored in the DRT helps the source node to estimate the angular position of its destination relative to itself. Although a similar scheme of maintaining beam IDs has been suggested in [81], DRP uses the beam ID kept in the DRT to do a novel route recovery as described in Section 9.4.2.2.

Figure 9.5 illustrates the basic working principle of DRP. In this figure, suppose node $A$ has a packet for node $E$. After a successful route discovery, suppose node $A$ finds a route to $E$ as $\{B(2), D(3), E(3)\}$. This implies that the route taken by a packet from $A$ to $E$, follows the path $B$, $D$, and $E$, and the antenna beams used by $B$, $D$, and $E$ to receive a packet from uplink is 2, 3, and 3 respectively. This information is stored in DRT of the source node $A$. Similarly the content of DNT at $A$ is as shown in Figure 9.5. This information in DNT is used during the sweeping of RTS-CTS.
In addition to the shared DNT, in DRP the network layer is aware of the different antenna beams at the MAC layer. The MAC, in turn, has separate buffers for each antenna beams. Accordingly, the link layer follows this approach by maintaining separate queues for each beam as shown in Figure 9.4. In order to place the packet in the correct link layer queue, the network layer determines the antenna beam which the MAC will use for transmission of the packet (through DNT), and puts the packet in the link layer queue corresponding to this antenna beam. It is to be noted that broadcast packets are kept in a separate dedicated queue.

### 9.4.1 DRP Medium Access Control

DRP uses a new MAC protocol for Directional Antennas (MDA) described in Chapter 7. In addition it uses some MAC layer optimization to handle deafness self-induced blocking problem as described in Chapter 8.
9.4.2 DRP Basic Operation

In the following sub-sections, we discuss the key modules of DRP.

9.4.2.1 DRP Route Discovery

The route discovery mechanism in DRP works similar to DSR. For a given source $X$, and destination $Y$, if $Y$ is not in the DNT of $X$, $X$ floods a $RREQ$ packet in the network. DRP enforces a broadcast optimizations proposed in [87] to reduce packet redundancy and route discovery latency. Whenever a node receives a $RREQ$ packet it starts a delay timer. If the same $RREQ$ packet is received again before the expiration of this timer, the node makes a note of all the beams where that packet arrived from. The node forwards (or sweeps) the packet in only those beams/directions other than those in which the packet arrived. Amongst the selected beams, DRP initiates a rebroadcast in the beams which are vertically opposite to the beams where the node received the broadcast packet. Next, the beams which are adjacent to these vertically opposite beams are chosen. This shall continue till all the selected beams are covered.

The IEEE 802.11 basic Carrier Sense Multiple Access (CSMA) [1] is followed before transmitting in the first beam of a particular sweep. For subsequent beams of the same sweep, we simply carrier sense and transmit. However if a beam has been marked as busy (i.e., the Directional NAV is set in this direction), that beam is ignored and the next free beam amongst the selected beams is chosen. It should be noted that we do not wait for the beam to become free. Deferring in every beam would lead to an extremely high sweeping delay. Further, we do not post-backoff after successfully transmitting in a beam and
before initiating transmission in another beam. A node post-back offs after completing a sweep of all the selected beams.

The sequence of hops taken by the route request packet as it propagates through the ad hoc network during the route discovery phase is recorded in a data structure in the packet, called directional route record. The directional route record appends both the node indices of the intermediate nodes and the beam ID used by these nodes to receive the packets from uplink. For example, an intermediate node $Z$ which forwards the route request packet, also adds the antenna beam at which it received the RREQ packet in addition to its own ID.

### 9.4.2.2 DRP Route Maintenance

The function of the route maintenance module is to monitor the operation of the route to a destination and inform the sender of any intermediate link failures or routing errors. In DRP, routes are generally associated with the antenna beam to be used to reach a particular nexthop. Hence any change in the location of the nexthop which changes the beam, even within the transmission range, needs to be handled carefully.

Similar to DSR, in DRP when originating or forwarding a packet using a source route, each node transmitting the packet is responsible for confirming that data can flow over the link. A link layer acknowledgment as in IEEE 802.11 is used for this purpose. As discussed in Section 9.3, in a directional environment it is necessary to distinguish between the movements of a nexthop within the range (nexthop is accessible through a different antenna beam) or the nexthop has moved out of the range. In the first case the sender need not send a route error packet back to the source and should try to locate the
node within its range. Hence in DRP we use separate phases for route maintenance. *Location tracking* and *two-hop directional local recovery phase* are local to the node which detect a link breakage. On the other hand, the *Route Recovery Phase* is done at the source. We now provide a comprehensive description of each of these phases and how they interwork.

**Location Tracking Phase:** Due to the continuous movement of the nodes, the antenna beam used by a node to reach its next hop and vice versa may change. Several methods have been proposed in literature to track such movements. The approach in [88] uses two antenna beams to continuously locate the position of a mobile node within the transmission range. This approach requires special hardware support which makes the cost of the overall system very expensive. The scheme discussed in [89] uses the concept of tones and extensive network state information at each node to track the position of a mobile node. On the other hand, [64] uses the concept of circular directional transmission of both RTS and CTS packets which eliminates the need of any specific tracking mechanism within the transmission range of a node. However, this results in a considerable overhead in the transmission of control packets. Use of GPS is also suggested as a means to track location of a mobile node, however the associated mechanism and control overhead has not been discussed.

DRP employs a two phase location tracking mechanism. Suppose node $X$ is presently forwarding a packet to node $Y$. If the transmission of an RTS from $X$ to $Y$’s previous location (say antenna beam “i”) fails for 3 consecutive attempts, node $X$ tries to locate $Y$ in its adjacent antenna beams for the remaining tries. Hence the $4^{th}$, $5^{th}$, $6^{th}$ and $7^{th}$ RTS
is sent at \( n \) adjacent antenna beams, including \( i \). Clearly, the value of \( n \) depends on the antenna beam-width. The reason behind scanning adjacent antenna beams is obvious. If a node is not reachable through adjacent antenna beams, the validity of the old directional path to the same destination becomes questionable. For example, in Figure 9.6(a), we show two positions of node \( Y \), one at position \((x_1, y_1)\), where \( Y \) can still maintains the connectivity to \( Z \), whereas at position \((x_2, y_2)\) the path from \( Y \) to \( Z \) is already broken. This simple example helps us to understand the antenna beams of \( X \) at which node \( Y \) can move, and may still have connectivity to \( Z \). In addition it also shows the number of antenna beams we need to send our RTS packet to locate \( Y \). This approach of locating \( Y \) to only a subset of antenna beams is different than some of existing schemes [65], which recommends sending RTS to all beams.

To illustrate the above, please refer to Figure 9.6 (b). Here node \( Y \) is the intermediate node between \( X \) and \( Z \) for a particular route. The shaded region is the portion where \( Y \) can move and can still maintain a link with both nodes \( X \) and \( Z \). If \( d \) is the separation between nodes \( X \) and \( Z \) and \( r \) is the communication radius, then the angular region where node \( X \) must scan for node \( Y \) is: \( 2 \times a \times \cos (d/2r) \). For \( d=1000 \) and for a 8 beam model, this angle is approximately equal to 67 degrees. This means that a node needs to just scan in the \((i-1)\)th and \((i+1)\)th beams. However, for a 12 beam model, this angle works to around 90 degrees. Hence a node needs to scan for \( i-1, i-2, i+1 \) and \( i+2 \) beams. DRP incorporates the above, scanning different number beams depending on beam-width. Table 9.1 lists the adjacent beams to be ideally scanned with increasing beam width.
Now if all the RTS retries fail, a broken link is reported to higher layer. This ends the location tracking phase in a node.

**Two-Hop Directional Local Recovery Phase:** Figure 9.7 illustrates the two hop directional local recovery in DRP. After detecting a broken link to Y, node X identifies the second nexthop in its path (*through the DRP packet header, Z in this case*) and generates a directional RREQ packet to find the route to Z with maximum propagation limit set to 2. This RREQ packet is sent only towards the direction (beam) of Z and intermediate nodes which receive this packet are also supposed to forward the packet in that direction. We call this *two-hop directional local recovery* in DRP.

After sending a two-hop directional RREQ, the sender node starts a timer for duration $T_l$ (Local Recovery Timeout) within which it expects a RREP. Here $T_l$ is selected such that

<table>
<thead>
<tr>
<th>Beam Width</th>
<th>Antenna Beams to be scanned about beam “i”</th>
</tr>
</thead>
<tbody>
<tr>
<td>90</td>
<td>“i-1”, “i”, “i+1”</td>
</tr>
<tr>
<td>45</td>
<td>“i-1”, “i”, “i+1”</td>
</tr>
<tr>
<td>30</td>
<td>“i-2”, “i-1”, “i”, “i+1”, “i+2”</td>
</tr>
<tr>
<td>20</td>
<td>“i-3”, “i-2”, “i-1”, “i”, “i+1”, “i+2”,</td>
</tr>
<tr>
<td></td>
<td>“i+3”</td>
</tr>
</tbody>
</table>
it would allow two hop route recovery to succeed. If a reply is received within this duration, node X stops its timer, and informs node S about the new route. We have used Route Error (RERR) packet to convey route update information to the source. We have used a \textit{LOC\_RERY} flag in the RERR packet to identify if it’s a two-hop directional route recovery packet. If the LOC\_RERY flag is set, the RERR packet includes the updated route. Source after receiving a RERR packet with LOC\_RERY flag set, updates its route to the corresponding destination.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure9.7.png}
\caption{Two hop directional local recovery in DRP}
\end{figure}

Figure 9.7 illustrates the route before and after the two hop directional route recovery procedure. If node X fails to get any reply in duration $T_i$ it generates a RERR Packet and sends it towards the source. This time \textit{LOC\_RERY} flag is set to false.

\textbf{Route Recovery Phase:} After receiving a RERR packet with \textit{LOC\_RERY} flag set to false, the source node S first tries a \textit{zonal route repair} to locate its destination. The concept of a \textit{zonal route repair} is to limit the zone in which the route request packet is propagated. For this purpose, A first estimates the location of the destination node relative to itself. Let us revisit Figure 9.5 and assume that node A requires to rediscover a route to $E$, and the previous route to $E$ maintained at its route cache was \{B(2), D(3), E(3)\}. 
Assuming all the nodes to be equipped with four beam antennas, A begins by approximating the relative position of B. Since B receives a packet from A in its antenna beam 2, by symmetry B will lie in the antenna beam 4 of A. If the average separation between the nodes is $R$ (which is assumed to be half of the nodes transmission range), then B is assumed to lie at distance $R$ on the angular bisector of antenna beam 4 of A. Hence, the co-ordinates of B relative to A are $(R \cos x, R \sin x)$. Next the co-ordinates of D and then E are estimated. Finally, A calculates the angular position of E relative to itself. A will then pad this angle by 45 degrees on either side. It will send the $RREQ$ packets in only those beams which lie within this angle. Hence, in above example A shall send route request packet in beams 1 and 4. All the nodes receiving this route request packets are supposed to forward the route request in antenna beams 1 and 4 only. This limits the zone of the transmission of route request packets.

To evaluate the accuracy of our direction estimation algorithm we created a random topology of 64 nodes in a 2250m by 2250m area. We then selected 10 different source destination pairs and a route was calculated between them over 4, 8 and 12 antenna beam models. For each such pair, the angle of the destination relative to the source is computed using our algorithm. Then the deviation from the actual angle (which is calculated based on actual locations of source and destination) is calculated. The results are listed in Table 9.2. Two observations can be made from this. Firstly, the algorithm performs better for lower beam widths. This can be easily explained as we approximate the next hop to lie on the angular bisector. With lower beam widths, the margin of error gets reduced. Secondly, the algorithm estimates destinations to a reasonable degree of accuracy.
Table 9.2 - Efficiency of Direction Estimation

<table>
<thead>
<tr>
<th></th>
<th>4-Beam</th>
<th>8-Beam</th>
<th>12-Beam</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean Dev.</td>
<td>22.98</td>
<td>12.81</td>
<td>11.34</td>
</tr>
<tr>
<td>Standard Dev.</td>
<td>4.67</td>
<td>5.19</td>
<td>4.38</td>
</tr>
<tr>
<td>Max. Dev.</td>
<td>34.74</td>
<td>38.79</td>
<td>22.87</td>
</tr>
<tr>
<td>Min. Dev.</td>
<td>9.79</td>
<td>0.583</td>
<td>3.69</td>
</tr>
</tbody>
</table>

In case this zonal route repair packet fails, source restarts a route discovery, flooding the route request throughout the network.

9.5 Performance Evaluation

We have implemented DRP on top of MDA. We assume CBR traffic and a 2Mbps channel for all our scenarios. Simulation is run for 200secs and all results are averaged over 10 different seeds. We compare the performance of DRP with DSR over omni-directional antennas (referred simply as OMNI or DSR) and DSR over directional antennas (referred to as DDSR). We mention DRP and DDSR over an M beam model as DRP_M and DDSR_M respectively. DDSR also uses MDA at the MAC layer. In the following subsections we thoroughly evaluate all the modules of DRP under static and mobile scenarios.
9.5.1 Route Discovery Phase

9.5.1.1 Route Discovery Latency

We assume a square grid of 64 nodes with inter-node spacing as 250 meters. We have implemented the *delayed route reply* optimization for both DDSR and OMNI so that the destination always responds by a single most optimal route. Figure 9.8 depicts the behavior of route discovery latency with varying source-destination separation. An eight beam model is used for both DSR and DDSR. DRP with its novel broadcasting approach is seen to consistently outperform both DSR and DDSR. The differences are more profound as the source-destination separation increases. Moreover, both DRP and DDSR outperform DSR as the range of an 8 beam antenna is higher in comparison to an omni antenna.

9.5.1.2 Routing Control Packets Redundancy

In this section we evaluate the broadcast redundancy of DRP as compared to DDSR which does not uses any kind of broadcast optimization. For a fixed source-destination separation, we measure the average number of redundant route query packets received at each node during a route discovery. Figure 9.9 depicts the average number of route query packets at each node for DRP and DDSR against increasing beam-width. A beam-width of 360 corresponds to OMNI. While OMNI exhibits minimum redundancy, DRP again scores over DDSR in controlling redundancy in the network. For 8 (45 degrees) and 12 (30 degrees) beam models, there are almost 50% more packets in the case of DDSR in comparison with DRP. A general trend observed for both DRP and DDSR is that
redundancy decreases with increasing beam-width. This is in tune with the fact that as the number of beams increases, greater number of packets gets transmitted into the network.

9.5.2. Hop Length – Route Optimality

To evaluate the benefits of directional transmission in getting a shorter route, we vary the source-destination separation between two nodes and calculate the hop length of the received routes at the source. We observed little or no variation in the quality of routes (in terms of hop-count) for DDSR and DRP. Therefore, in this section we just compare DRP and OMNI. For a given separation, we picked as many as 5 different source-destination pairs and calculated the hop length for each route. The hop length occurring with the highest frequency is assigned to that separation. Figure 9.10 plots this variation for OMNI and DRP_4, DRP_8 and DRP_12. For larger separations, we observe that DRP_8 and DRP_12 yield shorter routes than a DRP_4 and OMNI. We also notice that there is little or no variation in the hop length for DRP_4 and OMNI. The reasoning is that the range of DRP_4 does not lead to any extra nodes getting covered in our topology (nodes separated by a distance of 250 meters) in comparison to OMNI. The same
reasoning can be extended to explain the same hop lengths obtained in the case of DRP_8 and DRP_12.

### 9.5.3 Throughput in static scenario

In this subsection we compare the throughput of DRP with OMNI in a static scenario for single and multiple flows. Once again, we have omitted DDSR from our comparison since DDSR performs almost similar to DRP in a static scenario. We use the grid topology as described in Section 9.5.1.1, and select the separation between the source and the destination node to 1500 meters. Figure 9.11(a) gives the result for a single flow. As evident from Figure 9.11, DRP_8 and DRP_12 outperform OMNI. A 5 hop route in the case of OMNI as opposed to a three hop route for DRP_8/DRP_12 explains the result. The poor performance in case of DRP_4 is mainly contributed by its limited transmission range. In addition, DRP_4 incurs MAC protocol overheads (sweeping to avoid hidden terminal problem). DRP_8/DRP_12 also incurs the same; however their larger transmission range, which results into shorter routes, offset these limitations. We also observe that throughput saturates at different values for different protocols. For multiple flows, we created two parallel flows separated by 250meters. The result (Figure 9.11(b)) is consistent with our findings for single flows and DRP_8/DRP_12 are found have better aggregate throughput as compared to OMNI.
9.5.4 Route Recovery Mechanisms

DRP uses a three-phase mechanism to recover a route in the event of a link failure at the MAC layer. In this subsection, we evaluate each of these mechanisms individually. We design special topologies to test our modules against DDSR. No comparisons are made with DSR since the idea here is to stress the need for special routing modules when directional antennas are to be used. However, we do compare all the three different protocols under random mobile scenarios in the later sections.

9.5.4.1 Location Tracking Mechanism

To evaluate the performance of our antenna beam handoff module, we construct a linear topology of 6 nodes with inter-node spacing equal to 500 meters. All nodes have an eight beam antenna system. It should be noted that the chances of a handoff are greater in an 8 beam model as compared to a four beam model. CBR traffic with data rate of 100Kbps...
was started between nodes 1 (source) and 6 (destination). Intermediate nodes were made to oscillate about their initial positions (Figure 9.12(a)) with varying speeds. Such a behavior causes rapid antenna handoffs. Our result (Figure 9.12(b)) indicates that DRP with its antenna handoff module is able to maintain a fairly constant throughput with increasing node speeds. In contrast, frequent route failures in DDSR leads to a decreasing throughput.

![Diagram of network topology with nodes oscillating](image1)

(a) – Topology to evaluate Location Tracking Module. Along the dotted arcs, nodes oscillate.

![Graph of throughput variation with mobility](image2)

(b) – Variation of throughput with mobility

**Figure 9.12 – DRP Location Tracking**

### 9.5.4.2. Local route recovery

In this subsection we evaluate DRP’s *two-hop local recovery mechanism*. To this end, we use a grid topology of 64 nodes as shown in Figure 9.13(a). Nodes 24 and 28 (with four beam antenna system) are chosen as the source and destination nodes respectively. Before the start of the simulation, a linear optimal route of (24, 25, 26, 27, 28) is hard-coded in the route cache of the source node. This is done to offset the initial advantage DRP may have over DDSR due to its enhanced route discovery mechanism. Next, a timer is implemented at the routing layer which periodically fires at 20sec interval. The purpose
of this timer is to artificially simulate route failures. Every time the timer fires, the current route is picked and an intermediate node is made inactive. For our entire simulation duration of 200secs, 10 such failures are generated. The antenna handoff module in DRP is disabled, so that the local route recovery module will be invoked whenever there is a link failure. We vary the packet generation rate from 10 packets per second to 80 packets per sec. Three performance metrics are used to gauge the effectiveness of the local recovery mechanism:

- **Packet Delivery Ratio**: The ratio of the packets received to packets generated
- **Routing Overhead per received packet**: Ratio of the total number of routing control packets (including route requests, route replies and route errors) generated/forwarded to the data packets received correctly at the destination.
- **Average End to End packet delay**: The average end to end delay encountered by each data packet.

The variation of the packet delivery ratio with increasing data rate at the source is shown in Figure 9.13(b). For data rates of 50 packets per second, both DRP and DDSR have nearly the same packet delivery ratio. Beyond this point, the packet delivery ratio falls very steeply in the case of DDSR as compared to DRP. The frequent route failures force DDSR to initiate route discoveries at the source. The combined effect of a greater route discovery latency (DDSR) and increasing data rate at the source lead to a large loss of packets. DRP, on the other hand, buffers packets and quickly recovers routes to the destination. The dip in the packet delivery ratio for DRP can be explained for cases when the local recovery fails. Whenever the local recovery fails, a source rooted discovery follows. Hence for such scenarios, the performance is actually worse than DDSR.
However, from our simulation results we conjecture that in most of the scenarios, DRP is able to locally repair the route.

Next, Figure 9.13(c) depicts the routing overhead per received packet at the destination node. For all data rates, the overhead is more in the case of DDSR as compared to DRP. This again is intuitive since DRP does not always resort to a route discovery at the source whenever a link fails. It should be noted that at high data rates (>50 packets per sec), the packet delivery ratio is very low in the case of DDSR. Inspite of this, the overhead at these rates is still more than DRP. This clearly demonstrates the efficacy of the local recovery module of DRP. Figure 9.13(d) depicts the end to end latency experienced by each received packet. Again for higher data rates, this latency is substantially greater in the case of DDSR. Packets wait for a route reply from the destination whenever a route-error occurs. As such, they encounter larger latencies.
9.5.4.3 Zonal Route Recovery

Zonal recovery is initiated when both antenna handoff and local recovery fail in DRP. In order to evaluate the effectiveness of this module, we picked six different source-destination pairs in our grid topology. In addition we disabled the handoff and local recovery module in DRP. As in the above case, a node was disabled in an active route to generate a link failure. This prompted a zonal recovery in the case of DRP and a source rooted route discovery in the case of DDSR. Figure 9.14(a) and 9.14(b) illustrates the comparison of the two protocols with respect to both routing overhead and the route discovery latency. Route recovery is faster in the case of DRP. In addition, the routing overhead is also significantly lesser than DDSR.
9.6. Mobile Random Scenario

In this section we compare the performance of DSR, DDSR and DRP in a random scenario. We generate 64 randomly placed nodes in an area of 2000m by 2000m. Nodes follow the random waypoint mobility model with varying speeds. Two pairs of source and destination nodes were selected randomly and CBR traffic with a data rate of 100Kbps was started between them. The packet delivery ratio, routing overhead per packet and the average end to end latency per packet is calculated against increasing node speeds. For each topology, we average the results over 10 different seeds. Figures 9.15(a), 9.15(b), and 9.15(c) plot the above stated metrics for four and eight beam model. Several interesting observations are in order. DRP has a very high packet delivery ratio in comparison to DDSR and DSR for both the four beams and eight beam directional antenna models. For an eight beam model, both DRP and DDSR have an almost 100% packet delivery ratio. This can be attributed to the larger range of these models, which result in very few hops.

Figure 9.14 – Zonal Route Recovery
Figure 9.15 – Mobile Random Scenario
For a four beam model, both DDSR and DSR have an almost equal packet delivery ratio. This ratio drops to less than 50% in cases of high mobility. The trends observed for the routing overhead per received packet were similar for both four and eight beam antenna models. DRP exhibits the least overhead, and DSR the maximum. We suspect that there are greater link failures in the case of DSR as compared to DDSR because of the restricted range of omni-directional antennas. This results in frequent route discoveries leading to a greater overhead. Our results are again consistent for packet latency for both four beam and eight beam models. We observe that DRP has the least latency, whereas DDSR has the maximum latency. The route recovery mechanisms of DRP are responsible for quicker route repair and lesser end to end latencies. DDSR has higher latencies than DSR. This can be explained in context of the MAC overhead incurred in MDA. Intermediate nodes sweep MAC control packets to avoid hidden terminal and deafness problems in DDSR [82]. DRP also incurs the same as it also uses MDA. However, since it doesn’t resort to source rooted route discovery at each link failure, its MAC overhead gets offset.
In this PhD dissertation, we have addressed the issue of power control and spatial reusability in mobile ad hoc networks. We first address the issue of power control in omni directional antennas. We have elaborated in detail the issues related to power control in MANETs. We have proposed a single channel Spatial Reuse enabled Power Control MAC (SRM) protocol for MANETs. Through extensive simulations studies we show that SRM provides a very high ratio of data delivered per joule of energy as compared to IEEE 802.11 and PCM.

Next we have addressed the issue of spatial reusability in IEEE 802.11 using directional antennas. We first consider the problem of medium access control for ad hoc networks employing directional antennas. We have discussed the shortcomings of existing work and have proposed a new MAC protocol for Directional Antennas (MDA) that implements unique mechanisms, including simultaneous diametrically opposite directional transmissions of RTS and CTS packets, an optimized form of sweeping, and an enhanced DNAV mechanism. Through our extensive performance evaluation, we have observed that MDA performs better than IEEE 802.11 and existing directional MAC protocols such as DMAC and CRM in all scenarios except in the linear topology. The linear topology case, is particularly degrading to all directional MAC protocols, but MDA
is still observed to perform best in terms of all directional MAC protocols considered, with IEEE 802.11 performing best overall.

We have used our MDA scheme and built a Directional Routing Protocol (DRP) on top it. In this regard, we provide a detailed study of issues related to routing in directional antenna systems. We also outline the behavior of different IEEE 802.11 system parameters in a multihop directional environment. Through a comprehensive simulation work, we show that how DRP can benefit the performance of routing protocol running over directional antenna system.

An important next step in continuation of our work would be to evaluate the performance of TCP over directional antenna systems. Performance of a directional MAC protocol over heterogeneous environment, where different nodes have different types of directional antenna system still needs to be addressed. In addition, it would be interesting to design a perfectly scheduled MAC protocols for a multihop directional environment.
Bibliography


