Routing in Heterogeneous Wireless Ad Hoc Networks

By

Sivaram M.S.L. Cheekiralla

Submitted to the Department of Civil and Environmental Engineering
in partial fulfillment of the requirements for the

Doctor of Philosophy
at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2008

Author____________________________________
Sivaram M.S.L. Cheekiralla
Department of Civil and Environmental Engineering
May 22, 2008

Certified by ________________________________
John R. Williams
Associate Professor of Civil and Environmental Engineering and Engineering Systems
Thesis Supervisor

Certified by ________________________________
Daniel W. Engels
Associate Professor of Electrical Engineering at the University of Texas at Arlington
Thesis Supervisor

Accepted by ________________________________
Daniele Veneziano
Chairman, Departmental Committee for Graduate Students

Routing in Heterogeneous Wireless Ad Hoc Networks

by

Sivaram M.S.L. Cheekiralla

Submitted to the Department of Civil and Environmental Engineering
on May 22, 2008, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in the field of Information Technology

Abstract

Wireless ad hoc networks are used in several applications ranging from infrastructure monitoring to providing Internet connectivity to remote locations. A common assumption about these networks is that the devices that form the network are homogeneous in their capabilities. However in reality, the networks can be heterogeneous in the capabilities of the devices. The main contribution of this thesis is the identification of issues for efficient communication in heterogeneous networks and the proposed solutions to these issues.

The first part of the thesis deals with the issues of unambiguous classification of devices and device identification in ad hoc networks. A taxonomical approach is developed, which allows devices with wide range of capabilities to be classified on the basis of their functionality. Once classified, devices are characterized on the basis of different attributes. An IPv6 identification scheme and two routing services based on this scheme that allow object-object communication are developed. The identification scheme is extended to a multi-addressing scheme for wireless ad hoc networks. These two issues and the developed solutions are applicable to a broad range of heterogeneous networks.

The second part of the thesis deals with heterogeneous networks consisting of omnidirectional and directional antennas. A new MAC protocol for directional antennas, request-to-pause-directional-MAC (RTP-DMAC) protocol is developed that solves the deafness issue, which is common in networks with directional antennas. Three new routing metrics, which are extensions to the expected number of transmissions (ETX) metric are developed. The first metric, ETX1, reduces the route length by increasing the transmission power. The routing and MAC layers assume the presence of bidirectional links for their proper operation. However networks with omnidirectional and directional antennas have unidirectional links. The other two metrics, unidirectional-ETX (U-ETX) and unidirectional-ETX1 (U-ETX1), increase the transmission power of the directional nodes so that the unidirectional links appear as bidirectional links at the MAC and the routing layers. The performance of these metrics in different scenarios is evaluated.

Thesis Supervisor: John R. Williams
Title: Associate Professor of Civil and Environmental Engineering and Engineering Systems

Thesis Supervisor: Daniel W. Engels
Title: Associate Professor of Electrical Engineering at the Univeristy of Texas at Arlington

To:

the memory of my late undergraduate advisor Lt. Prof. Madhav N. Kulkarni, my parents, Kasi Parameswara Gupta and Lalitha Kumari, my brother, Kiran, and my grandmother, Rajeswari

Acknowledgments

During my graduate student life, I had the privilege to meet and interact with a lot of wonderful people, who have influenced my thinking and approach to problem-solving in several ways. The acknowledgments are a way of personally thanking these people.

First and foremost, I would like to thank my advisor Daniel Engels for taking me as a student and mentoring me. He has been a great advisor academically, professionally, and personally. His style of working ensured that I was being productive and at the same time enjoying my work. I have immensely enjoyed discussing academic and non-academic matters.

John Williams, for agreeing to be my thesis committee chair and for his advice and suggestions during various committee meetings. George Kocur for allowing me to be a teaching assistant (TA) for his wonderful courses, for being on my thesis committee, and for his advice on professional and personal matters. I cherish the conversations with him during the period when I was his TA, and I hope I can carry whatever I have learnt from him to my professional life. He has been a role model to many students, and I am no exception.

Rory O'Connor for being a wonderful mentor and friend on whom I can always rely on. I have learnt the foundations of research with him. His style of learning by doing is something that I hope to continue. I thoroughly enjoyed working with him and I appreciate the care he has provided me during my initial years at MIT. I am forever grateful to him for telling me that there is more to life than academics and for the trust and confidence he has placed on me.

Thanks to Cynthia Stewart, Kris Kipp, and Jeanette Marchoki for all the help with the administrative matters and for their timely reminders about different deadlines.

Thanks to the Thurbers (Bob and Susy), who gave me the fellowship during the crucial stage of my graduate studies. Thanks to Lama Nachman and Mary Murphy-Hoye for providing me an opportunity to work at Intel Corporation and learn how the industry works and get a flavor for research in the industry.

Life at MIT would have been so tough without the wonderful company of my

friends. I would like to thank my friends: Hari, M.N.Srini, J.Srini, Deepak, Vijay, Sreekar, Bhanu, Phani, Dhanush, Rags, Vikram, and Madhu for being there. I have learnt a lot from each of you and thoroughly enjoyed spending time with you. I would also like to thank my roommates over the years: Brendan Green, Rajappa, Prahladh, Lav, Biz, and Thomas.

Special thanks to Hari, J.Srini, M.N.Srini, and Vijay for listening patiently to my practice talks and giving me valuable and honest feedback on my research and presentations.

Thanks to Hari for being a friend, office-mate, and a mentor. Life at MIT, would have been really tough with out his friendship. I learnt so much from him and I have enjoyed his company in the courses, sharing the office space, and discussing a myriad number of topics ranging from research to sports. I look forward to sharing the office space in the future. Thanks to M.N. Srini for his friendship, for his positive attitude and his humor, and for making our (Hari's and mine) office space lively with his presence. Thanks to J.Srini, for sharing his knowledge on carnatic music, honest advice, his humor, and his friendship. Vijay for his humor, advice on running, and the "gult" companionship. Thanks to the members of the "baddy badshahs" for having fun and agreeing to eat where I wanted to eat.

I would like to thank Swami Tyagananda for his discourses on the Hindu Philosophy at MIT. His teachings and talks have created a new avenue in my life, which I hope to explore in future.

Special thanks to Pushpinder Singh for providing wonderful and tasty food for four years.

Stefanie Delichatsios (alkidel) for being a wonderful labmate. I have thoroughly enjoyed her company in the lab and havig coffee with her and Dan. Thanks for attending my first presentation at a conference and proof-reading my papers. It was fun sharing the lab with her. The work on directional antennas has started as a course project with Ariadna Quattoni. I would like to thank her for her insights on directional antennas and getting started on directional antennas.

I would like to thank my undergrad friends Vikas, Satya, Kunde, and Murthy for their wonderful friendship. Special thanks to Kunde and Murthy for all the mentorship during the past 10 years.

I would like to thany my relatives: pinni, babai, Manasa, Jyotsna, mamayya, attayya, and Meghana for providing a home away from home and taking care of me. Special thanks to pinni for her help during my initial days at MIT. I could only repay it in cash and not in kind.

Words cannot express my gratitude for my family: amma, nannagaru, kitchu, and ammamma. Their love and support made me reach where I am today. I I also would like to thank my uncle, Mr. Krishnamurthy, for being a source of inspiration and for his encouragement since my childhood days.

Thanks to my wonderful wife, Mani Brundha for her support in the last few months, and it wouldn't have been possible to complete this thesis without her support. Her love has enriched my life in many ways.

Thanks to IEEE for allowing me to republish some of my work in this thesis (Chapters 2, 3, and 6). The material published in these chapters is with the permission of IEEE. Such permission of the IEEE does not in any way imply IEEE endorsement of any of the Massachusetts Institute of Technology (M.I.T.)'s products or services. Internal or personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution must be obtained from the IEEE by writing to pubs-permissions@ieee.org.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Wireless devices such as cellular phones, laptops, personal digital assistants (PDAs), etc. have become indispensable. The prevalence of wireless devices can be attributed to the mobility they provide. With the development of new wireless standards and new wireless technologies, the usage of wireless devices is going to increase in the future.

A wireless network is a network of nodes or devices that have wireless communication capability. Based on the communication model, wireless networks are classified as cellular networks (Figure 1-1) and ad hoc networks (Figure 1-2). In a cellular network, a set of devices communicate with a central device, called the base-station or the gateway. The gateway is usually fixed or static, while other devices are usually mobile. The gateway and any other device in the network are directly connected via a wireless link. An example of cellular networks is a wireless local area network (WLAN). Cellular networks have a centralized communication architecture with the gateway coordinating the communication activity.

Wireless ad hoc networks don't have a dedicated routing infrastructure and rely on multi-hop communication. Nodes in an ad hoc network cooperatively forward other nodes' data. These networks have a distributed communication architecture, where individual nodes make the decisions on routing and medium access. We discuss wireless ad hoc networks in the following section.

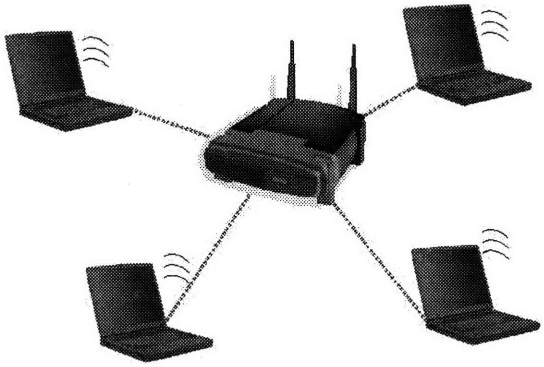


Figure 1-1: Cellular network

1.1 Wireless ad hoc networks

Wireless ad hoc networks are classified as static ad hoc networks or mobile ad hoc networks depending on the mobility of the nodes in the network. In this thesis, we focus on static wireless ad hoc networks and henceforth, refer to them as wireless ad hoc networks.

Static wireless ad hoc networks are classified as mesh networks or sensor networks depending on the intended application and the communication model. In sensor networks, a set of devices use multi-hop communication to relay data to a gateway device or a base-station. Common sensor network applications include infrastructure monitoring [10], environmental monitoring [5], and wild-life habitat monitoring [68].

Mesh networks are characterized by a high degree of connectivity between the nodes and are used in applications such as wireless personal area networks, or providing Internet connectivity to remote locations [6].

A common assumption about wireless ad hoc networks is that they are homogeneous. In a homogeneous network, all the devices have the same communicational and computational capability. However in reality, wireless networks are heterogeneous. We discuss heterogeneous wireless ad hoc networks in the next section.

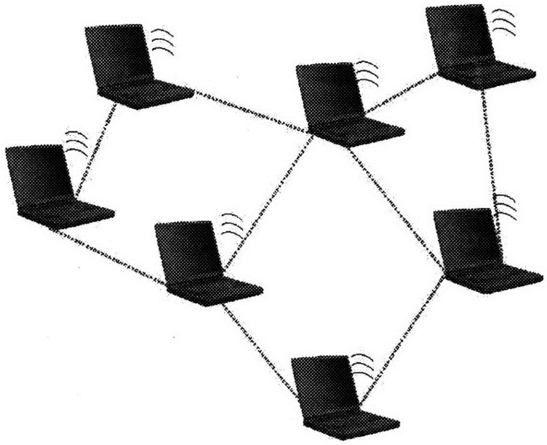


Figure 1-2: Ad hoc network

1.2 Heterogeneous wireless ad hoc networks

In a heterogeneous wireless ad hoc network, the devices differ in their communicational aspects such as transmission power, antenna type, modes of communication, etc. Economic and application constraints lead to differences in communicational aspects of devices in wireless networks. For example, many sensor network applications [68] require a tiered communication architecture, where the devices in the network have different communicational capabilities.

In the following section, we discuss a few issues related to communication in heterogeneous wireless networks.

1.2.1 Issues in heterogeneous wireless networks

Communication is the fundamental aspect of networks, and for efficient communication, several conditions need to be met. Efficient communication in homogeneous networks is relatively easier than in heterogeneous networks. Heterogeneity in the network imposes additional requirements. We focus on the problem of communication in heterogeneous static wireless ad hoc networks in this thesis. We first identify two broad issues that need to be addressed for efficient communication in wireless heterogeneous networks.

1. **Unambiguous classification of devices**

Since a heterogeneous network consists of devices with different communicational capabilities, there is a need for unambiguously defining the devices in a network.

2. **Device identification**

   To enable communication in a network, a unique identifier and an address are required for every device in the network. A unique identifier uniquely identifies a device, where as an address gives the logical location of the device in the network. An appropriate identification scheme and an addressing scheme are also needed for assigning identifiers and addresses in networks.

The above issues are applicable to different types of heterogeneous networks. Smart antennas improve the performance of wireless ad hoc networks [93]. Existing research focusses on homogeneous networks consisting of smart antennas. However, the research on heterogeneous networks that consist of smart antennas and omnidirectional antennas is very little. In this thesis, we consider communicational aspects of such networks. In the following, we discuss the issues that arise in such heterogeneous networks.

1.2.2 Issues in heterogeneous wireless networks with omnidirectional and directional antennas

Heterogeneity in wireless networks arises from several factors. In this thesis we consider heterogeneity when the nodes in the network either use an omnidirectional or a smart antenna.

A smart or a beamforming antenna is realized through an array of antennas, whose signals are combined (or beamformed) to achieve a desired beam pattern [43]. Having a desired beam pattern improves the signal quality in the desired direction and reduces interference in other directions. Thus, these antennas are also known as directional antennas. Figure 1-3 shows the radiation pattern for an omnidirectional and a directional antenna.

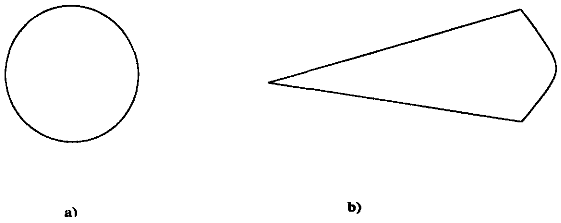


Figure 1-3: Radiation pattern in a) isotropic antenna and b)the simplified radiation pattern for a directional antenna

One of the important aspects of heterogeneous ad hoc networks that consist of omnidirectional and directional antennas is the presence of unidirectional links. The difference in gain between a directional and an omnidirectional antenna creates these links. Consider Figure 1-4, when node A (an omnidirectional antenna) broadcasts, node B (a directional antenna) is able to receive the message. However when node B broadcasts (using the omnidirectional mode), node A is unable to hear. The presence of unidirectional links needs to be considered when designing medium access control protocols and routing metrics.

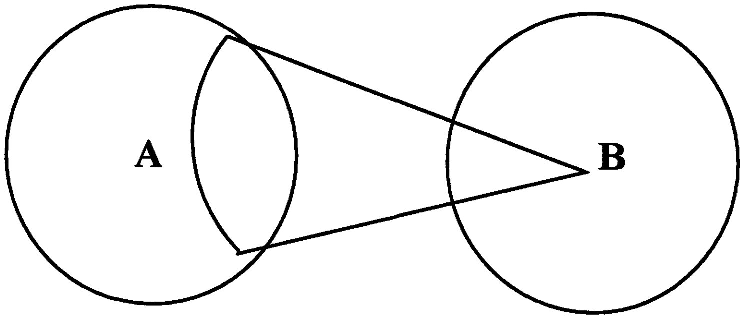


Figure 1-4: Unidirectional links in heterogeneous networks

We discuss medium access and routing issues in networks with omnidirectional and directional antennas in the following.

3. Medium access control

Wireless communication is essentially broadcast, and hence an efficient protocol to coordinate the communication activity in the network is needed. Existing MAC protocols, such as the 802.11 assume that an omnidirectional antenna is used at the physical layer. Hence, using a directional antenna at the physical layer would need significant changes to the MAC layer. Existing modifications to 802.11 [17] accommodate directional antennas at the physical layer cause the deafness problem in wireless ad hoc networks. The deafness problem leads to a wastage of transmissions and hence a decrease in the throughput. Thus, a MAC protocol to solve the deafness issue is needed.

4. **Routing**

   To deliver the data in a network, a route is needed between the source and the destination nodes. The lack of a dedicated routing infrastructure, the broadcast nature of the wireless medium, and the heterogeneity of wireless ad hoc networks make routing a challenging task. A routing protocol and routing metric(s) to account for the unidirectional links in the network are needed for efficient routing.

We discuss the implications of unidirectional links in heterogeneous networks at the MAC and routing layers in this thesis.

To summarize, we discussed the broad issues in heterogeneous networks and the issues related to the usage of omnidirectional and directional antennas. We develop solutions to these issues in this thesis. We discuss research contributions in the next section.

1.3 Research Contributions

The central objective of this thesis is:

To develop routing metrics for heterogeneous wireless ad hoc networks that consist of devices equipped either with a smart antenna or an omnidirectional antenna.

We outline the detailed contributions of this thesis in the following.

1.3.1 Functional Taxonomy

To solve the issue of unambiguous classification of devices, we develop a functional taxonomical classification scheme for classifying different types of wireless communication devices (WCDs). We define WCDs as devices that are used in wireless ad hoc networks. The classification scheme defines the devices based on the functionality and characterizes them on the basis of several attributes. Functionality is primarily defined from a communication perspective and the chief attributes used for characterization are: communication, power, memory, and sensors. WCDs are classified into the following categories [9]:

1. Passive RF devices
2. Active RF devices
3. Ad hoc networking devices
4. Gateway devices

The above classification scheme allows an unambiguous way of defining several types of devices ranging from RFID tags to laptops. The attributes and the sub-attributes allow different levels of characterizing the device. The above taxonomical representation of devices is scalable and can be extended to other RF digital devices and other possible devices that may find application in wireless ad hoc networks in the future.

To summarize, the taxonomical representation scheme solves the issue of unambiguous classification of devices in heterogeneous networks.

1.3.2 IPv6 identification scheme

To solve the issue of device identification in wireless networks, we develop an IPv6 identification scheme. This scheme is used for identifying all kinds of physical objects including objects that are tagged by RFID tags to network interfaces. We initially define the requirements of a globally unique identification scheme and show that the IPv6 identification scheme satisfies these requirements. The format of the IPv6 identifier is similar to the format of the IPv6 unicast address, but is distinct and distinguishable from the IPv6 unicast address. Further, we also define the notion of a *corresponding address* for an *identifier* and vice-versa [11].

We develop two routing schemes that allow generic object-to-object communication. These schemes assume the existence of an IPv6 identifier. The first routing scheme is based on a naming scheme for objects that uses the IPv6 identifier, and these names are used in conjunction with the domain name system (DNS). The second routing scheme is a distributed scheme that use the routers for routing data packets to objects or their networked proxies. This scheme assumes that the routers treat an IPv6 identifier in the same manner as an IPv6 address in the data packet. Thus, a packet which has an IPv6 identifier in the destination address will be routed to the *corresponding address* [11].

We propose a novel multi-address assignment scheme, called the viral IP address assignment scheme for wireless ad hoc networks. This scheme uses the IPv6 identifiers to define an address space from which nodes can allocate addresses to other nodes. The process of assigning addresses mimics a viral growth and hence is termed as viral address assignment. One of the assumptions for commonly used address assignment schemes is that address and identifier are the same, and hence are used in an interchangeable fashion. An identifier uniquely identifies an entity, while an address gives the logical location of the entity in the network. The viral address scheme makes this distinction between an address and an identifier. The multi-address scheme provides redundancy to wireless networks and makes routing easier as the address assignment scheme is based on a prefix-based addressing scheme [13].

To summarize, the IPv6 identification scheme satisfies the requirements of a global identification scheme and the developed routing schemes allow a generic object-to-object communication. Since, the identification scheme is based on the Internet Protocol (IP), the identification scheme can use the existing Internet infrastructure and the developed routing schemes can coexist with the existing Internet routing protocols. Further, the proposed addressing scheme provides redundancy and makes routing easier in heterogeneous ad hoc networks. The IPv6 identification scheme solves the issue of device identification in wireless networks.

The developed solutions, functional taxonomy and the IPv6 identification scheme solve the broad issues pertaining to heterogeneous wireless networks. We now discuss the medium access control and routing in heterogeneous networks with omnidirectional and directional antennas.

1.3.3 MAC protocol for directional antennas

We discuss the existing MAC protocols for directional antennas and discuss their limitations. Based on these limitations, we develop a new MAC protocol, request-to-pause directional medium access control (RTP-DMAC). This protocol uses information from the routing layer to improve the performance of the MAC layer. The RTP-DMAC protocol defines an additional frame, request to pause (RTP), whose format is similar to the request to send (RTS) packet of the 802.11 MAC protocol. The protocol uses information from the routing layer to decide to which nodes the RTP packet should be sent. The RTP-DMAC is an extension to the 802.11 DCF MAC protocol and uses the mechanisms designed for directional antennas, directional network allocation vector (DNAV) and directional handshake scheme. The RTP-DMAC scheme is designed to solve the deafness problem and reduce the impact of deafness in ad hoc networks with directional antennas.

1.3.4 Routing in heterogeneous networks

We develop novel routing metrics for heterogeneous networks that consist of directional and omnidirectional antennas. We develop and evaluate three new routing metrics that are extensions to an existing routing metric for homogeneous wireless networks, ETX [20]. The first routing metric, ETX1 uses a higher transmission/broadcast power to overcome some of the problems caused by the unidirectional links [12]. The other two routing metrics, unidirectional-ETX and unidirectional-ETX1, use the higher gain available to directional antennas, and improve the routing performance in the presence of unidirectional links. We also discuss some of the changes that are needed at the MAC and the physical layers to accommodate these routing metrics. The problem of routing in heterogeneous is novel and the designed routing metrics improve the routing performance compared to the standard (i.e. those designed for homogeneous networks) routing metrics when used in a heterogeneous network.

In this thesis, we are concerned with different issues that arise in communication in heterogeneous networks. We discuss these issues and the proposed solutions in a greater detail in the remainder of the thesis. We discuss the thesis outline in the next section.

1.4 Thesis Outline

The remainder of the thesis is organized as follows.

Chapter 2 covers the functional taxonomy of wireless communication devices. The taxonomy allows an unambiguous definition of devices based on their functionality and characterize them on their attributes. We provide a few taxonomy-based examples of classifying devices.

In Chapter 3, we develop an IPv6 identification scheme that is used for identifying wireless devices ranging from RFID tags to wireless gateways. We develop two routing mechanisms and a viral IP addressing scheme based on IPv6 identifiers for ad hoc networks. The routing schemes allow a generic object-to-object communication and the multiple addressing scheme provides redundant routes in wireless ad hoc networks. The overall focus of this thesis is on communication in heterogeneous networks, and in this regard Chapter 2 and Chapter 3 deal with issues that are applicable to a generic case of heterogeneous wireless networks.

Chapters 4, 5, and 6 consider communication in heterogeneous networks that consist of omnidirectional and directional antennas. In Chapter 4, we discuss heterogeneous networks that consist of omnidirectional antennas and directional antennas and the details of the antenna model that we use in this thesis.

In Chapter 5, we discuss the MAC layer issues with directional antennas, develop the RTP-DMAC protocol and compare its performance with existing MAC protocols for directional antennas.

We study the need for new routing metrics in heterogeneous networks, and develop and evaluate new routing metrics for heterogeneous networks in Chapter 6.

Finally, we draw the relevant conclusions and suggest directions for future work in Chapter 7.

Chapter 2

Taxonomy of Wireless Communication Devices

We describe a functional taxonomy of wireless communication devices in this chapter. We give the motivating reasons for such a classification scheme, describe the classification scheme, and provide a few examples of using the classification scheme. This chapter is based on the work by Cheekiralla and Engels [9] [1].

2.1 Introduction

With the recent technological developments, low-powered and cheap computing technology is readily available. The development of standards for wireless personal area networks (WPAN) and wireless industrial automation and control has increased the usage of wireless devices. A Wireless ad hoc network is a network of devices that use RF-based multi-hop communication for transferring data. We define *Wireless Communication Devices* (WCDs) as devices that are used in wireless ad hoc networks. Wireless ad hoc networks are broadly classified as wireless sensor networks (WSNs) and wireless mesh networks (WMNs). WSN applications include civil infrastructure monitoring, wild-life habitat monitoring, and environmental monitoring, and WMN

[1] Copyright ©2005 IEEE. Parts of this chapter are reprinted from: S. Cheekiralla and D.W. Engels. A functional taxonomy of wireless sensor network devices. Broadband Networks, 2005 2nd International Conference on, pages 949956 Vol. 2, 3-7 Oct. 2005.

applications include providing Internet connectivity to remote places [6].

Wireless ad hoc networks tend to be heterogeneous in nature as devices of different capabilities are used. In such a heterogeneous network, defining WCDs in an unambiguous manner becomes necessary. We now discuss the motivating reasons for a taxonomical classification of WCDs.

2.1.1 Motivation

The increasing use of wireless ad hoc networks necessitates an unambiguous way of defining WCDs. For example, in WSNs, the loaded use of terminology for describing devices causes ambiguities. The word "motes" is often used to refer devices used in a WSN. However, such a usage of the word limits the range of devices that can be used in a WSN. Technologies such as ultra wide band (UWB) [65] and radio frequency identification (RFID) are also used for WSN applications. The usage of these diverse technologies for a single application makes the network heterogeneous. In such a heterogeneous scenario, a classification scheme gives a better perspective of the role of different WCDs in the network.

There is an increasing convergence of WSNs and WMNs for some applications. The existing schemes for describing devices usually concentrate on WSN devices or describe the devices from a hardware [60] or a database perspective [35]. Thus, there is a need for a scheme to describe devices that are used in WSNs and WMNs. We use the term WCDs to refer to devices used in wireless ad hoc networks (both WSNs and WMNs).

We describe a classification scheme that allows a spectrum of WCDs to be classified on the basis of their functionality. As far as we know, this kind of classification scheme is novel. For our classification scheme, we consider devices that use RF-based digital communications and devices that could potentially be used in ad hoc network applications.

The remainder of the chapter is organized as follows. In Section 2.2, we discuss the previous work on classifying devices used in ad hoc networks. In Section 2.3, we describe the functionality based classification of WCDs. In Section 2.4, we state the different attributes of WCDs that are used for characterizing them. In Section 2.5, we represent a couple of WCDs using the taxonomical approach. We draw relevant conclusions in Section 2.6.

2.2 Previous Work

Existing work on classifying WCDs is limited to WSN devices. Most of the WSN devices that are classified are "mote" like devices with varying capabilities. Vieira et al. [60] describe important characteristics like power consumption, computational and communication resources of the motes. Tilak et al. [89] describe WSN from a networking point of view, classifying micro-sensor networks on the basis of communication and network parameters. Hellerstein et al. [35] describe WSN devices ranging from RFID devices to remote sensing from a database perspective. Hill et al. [36] give a tiered view of WSN devices and classify them on a hierarchical basis. A generic survey on WSNs is given by Akyildiz [2], where the architecture, communication protocols, and algorithms for different aspects of WSN are discussed. Engels and Sarma [27] define an encapsulation scheme for classifying different kinds of RFID devices based on their functionality.

There is an increasing convergence of WSNs and WMNs and using devices with varying capabilities. Hence, a new and a generic classification scheme is needed for classifying a broader class of devices. We describe our classification scheme in the following section.

2.3 Functional Classification

In this section, we describe the functionality-based classification of WCDs. We classify devices into the following categories (Figure 2-1):

1. Passive RF devices

2. Active RF devices

3. Ad hoc networking devices

4. Gateway devices

The above order of listing the categories has an inherent hierarchy with passive RF devices having the least communication and computing capability and gateway devices having the most. For WCDs, functionality is defined in terms of communication, computing capabilities, and power requirements. Devices are characterized on the basis of attributes after classifying them on their functionality.

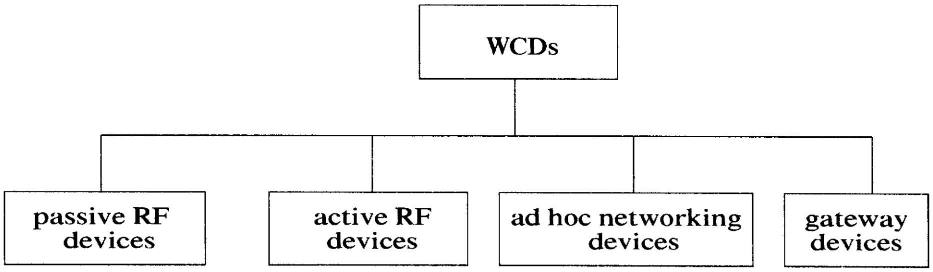


Figure 2-1: Tree view of the functional classification

Passive RF devices

Passive RF devices have a passive communication module and a minimal amount of memory. They operate only in the presence of another device from which they draw energy. For example, passive RFID devices, which operate only in the presence of a reader [2]. These devices cannot communicate with other passive RF devices. Engels and Sarma [27] define the minimum functionality of a passive RF device as the ability to respond back with data when queried by a reader. We generalize their definition to devices that can operate only in the presence of another device.

Active RF devices

An Active RF device has an active RF transmitter. These devices usually have an on-device power source for actively transmitting. Additionally, these devices may

[2] A reader is a device which emits electromagnetic energy and reads the reflected energy from these devices to communicate with them.

have memory to store data. Specific examples of this type are active RFID devices and radio ICs.

Ad hoc networking devices

Ad hoc networking devices have the ability to communicate in an ad hoc manner. They usually have:

- An intelligence unit that controls the communication and sensor modules (if present).
- A dedicated communication unit usually in the form of radio ICs.
- A power source in the form of a battery and in some cases additionally energy harvesting schemes are used.

Specific example an ad hoc networking device is the mote. “Motes are tiny, self-contained, battery-powered computers with radio links, which enable them to communicate and exchange data with one another, and to self-organize into ad hoc networks. Motes form the building blocks of wireless sensor networks” [58]. Further, an ad hoc networking device itself could have components that are either passive RF devices or active RF devices.

Gateway devices

Gateway devices either collect data from a cluster of devices or connect with other gateway devices to form a network. An example of a gateway device is a laptop which collects data from motes.

The basic categories of WCDs have been defined on the basis of their functionality. These can be characterized further on the basis of attributes, which are described in the next section.

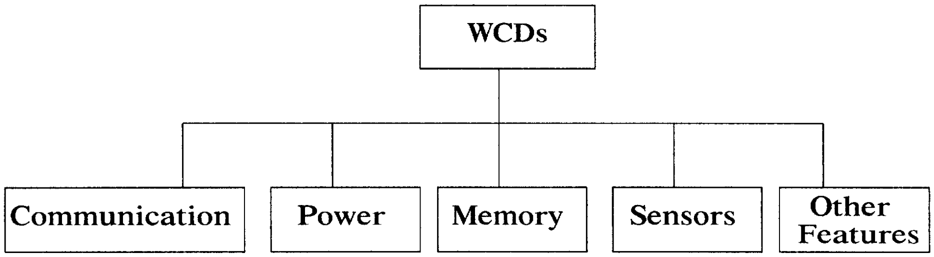


Figure 2-2: Tree view of attributes

2.4 Attributes of WCDs

In this section, we describe the attributes for characterizing WCDs. The attributes (Figure 2-2) are broadly classified into the following groups:

1. Communication
2. Power
3. Memory
4. Sensors
5. Other features

Each of these attributes is broken down further and these sub-attributes can be broken down further depending on the level of detail that is required for an application.

2.4.1 Communication

The communication attribute is broken down into different sub-attributes (Figure 2-3). These are:

- Communication protocols/standards
- Communication modes
- Number of communication modules
- Antenna type

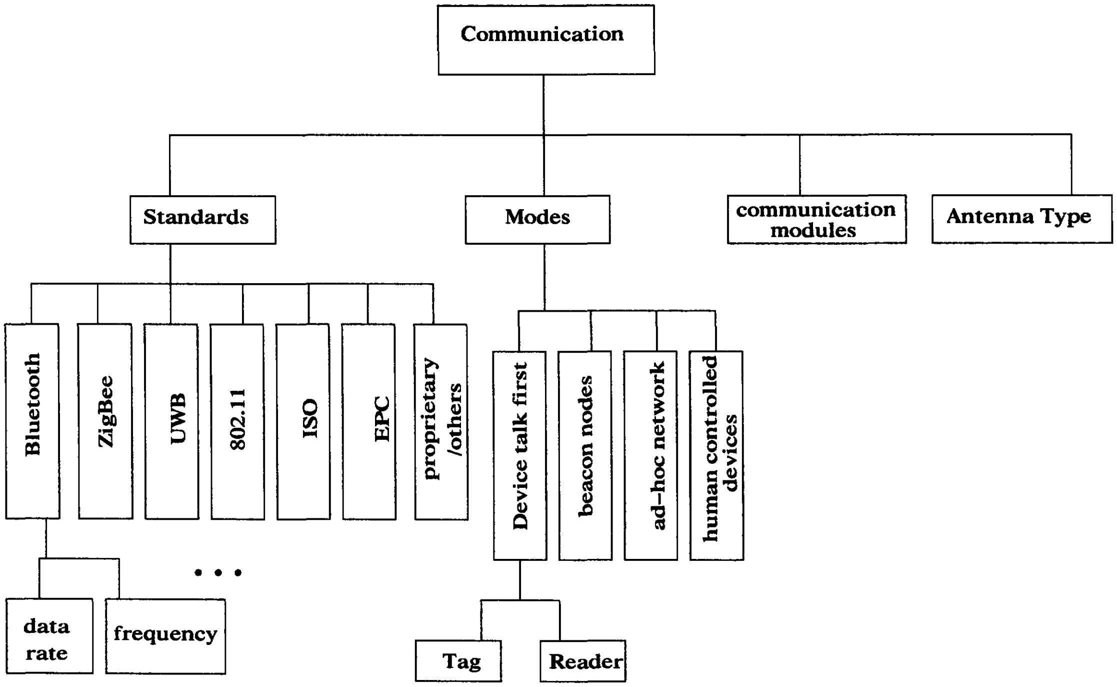


Figure 2-3: Tree view of communication attribute

Standards

Standards are important for characterizing WCDs as they specify the maximum data rate, the frequency of operation, and a portion of the communication stack. We classify the standards as shown in Figure 2-3. Table 2.1 summarizes the maximum available data rates and the frequency of operation for different standards. We briefly discuss some of the important standards.

1. Bluetooth is an industrial consortium formed to develop a standard for wireless personal area networks (WPAN). Bluetooth is a spread spectrum technology operating in the 2.45 GHz industrial, scientific, and medical (ISM) band. Typical communication range is 10 m for bluetooth devices [37]. Leopold et al. [48] in their feasibility study of using a Bluetooth radio for WSNs show that Bluetooth is not a good option for scatter net kind of networks, and maintaining networks even in low duty cycles is power expensive. Another disadvantage of using Bluetooth is that applications cannot access low level relevant information, which is needed for synchronization and device discovery.

2. ZigBee is an industrial consortium that developed a new standard for low-cost, low-powered wireless monitoring, and control [94]. ZigBee uses direct spread spectrum technology with a maximum data rate of 250 kb/s. The networking and application layer of ZigBee are implemented over the IEEE 802.15.4 standard for WPAN [21].

Standard	**Typical Data rate**	**Frequency of Operation**
Bluetooth 2.0	2.1 Mb/s	2.45 GHz
ZigBee	250/40/20 kb/s	2.4 GHz/915 MHz/868 MHz
UWB	up to I Gb/s	3.1-10.6 GHz
IEEE 802.11a	54 Mb/s	5 GHz
IEEE 802.11b	11 Mb/s	2.4 GHz
IEEE 802.11g	54 Mb/s	2.4 GHz

Table 2.1: Typical data rates and frequency of operation for different standards [94, 64, 37, 59]

3. IEEE 802.11 is the standard for wireless local area networks (WLAN). The three important versions of this standard are 802.11a ,b, and g [59]. This standard is mainly used for gateway devices so they can interface easily with PCs, laptops, or PDAs. Future versions of the 802.11 include 802.11s and 802.11n, which specify the standards for mesh networks and multiple-input multiple-output (MIMO) antenna based devices respectively.

4. Ultra wide band (UWB) technology refers to a modulation technique based on transmitting in very short pulses [64]. Work done by Oppermann et al. [65] show significant promise for low-power, low-cost wide-deployment of sensor networks. The signals being noise-like in nature are resistant to multi path effects and jamming. Ad hoc networks based on UWB radios provide better locationing and have better battery lives. The IEEE standard for UWB, 802.15.3.a is under development.

5. ISO standards specify world-wide industrial and commercial standards that are published by the International Organization for Standardization [41]. For exam-

ple, the ISO 8000 series specifies standards for the air-interface communication parameters [30] for different kinds of RFID devices.

6. EPC (Electronic Product Code) standard is primarily for using the EPC with RFID devices [28].

Communication modes

Engels and Sarma [27] define different kinds of communication modes for RFID devices. We generalize and extend them to WCDs. These are:

1. "Device talk first", which is relevant to RFID devices. This mode is further classified into
   - "Tag talk first" devices are those that respond first in the presence of the reader's electromagnetic energy.
   - "Reader talk first" devices are those that wait for an instruction from the reader.
2. "Beacon" devices are those that periodically announce their identification and other relevant data.
3. "Ad hoc" devices are those that have ad hoc communication capability.
4. "Human controlled" devices are those that are controlled by humans.

Some of the WCDs can have more than one mode of communication. For example, a node in a network can have both the "beacon" and the "ad hoc" modes.

Communication modules

This attribute refers to the number of RF communication modules a WCD has. WCDs usually have one communication module, but some of them have more than one communication module. For example, gateway devices have more than one communication module.

Antenna type

This attribute refers to the type of antenna a device uses. One of the common assumptions in wireless ad hoc networks is that devices have omnidirectional antennas. However it is possible for the devices to have directional antennas (such as yagi antennas), smart antennas, or MIMO antennas.

2.4.2 Power

WCDs need power to operate. The attribute *power* is classified into three categories: *storage*, *energy harvesting mechanisms*, and *transfer.* Power consumption and the duty cycle of a device determines its lifetime, which in turn determines the lifetime and the connectivity of the network. In WSNs, many of the devices are expected to operate with minimum human intervention, therefore optimizing power consumption is crucial. Sensing, communication, and computation are the main tasks of a WSN device. A lot of work done in this area involves developing low-power communication protocols for routing, resource discovery, etc. The tradeoff is usually seen between communication and computation, and sensing is often assumed to be a less power consuming task than the other two. This assumption in general, is not a valid one as some applications require sensors which consume more power than communication, and computation tasks. We give typical power consumption values for communication and computation tasks. These values are representative and can vary widely depending on the application. Many WCDs run on batteries and some of them may be powered via power outlets. The storage attribute doesn't cover these kind of devices and whenever a device is powered from the wall, we would mention it so.

Table 2.2 shows the values for energy[3] consumption and data rates of devices based on various standards and different radio ICs. The energy consumption in Table 2.2 refers to the energy consumed per bit, which is defined as

$$e_b = e_{tx} + e_{rx} + E_{dec}/\eta;$$

[3] Energy = Power *time. At some locations, we give power consumption values as it is easier to give those values and for some cases energy consumption makes more sense.

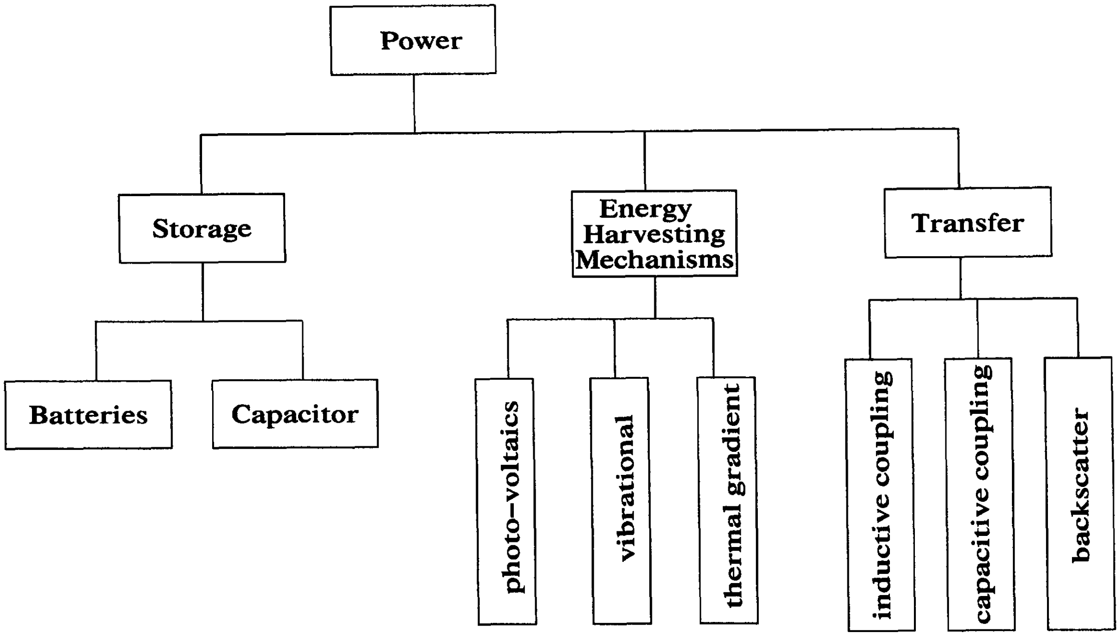


Figure 2-4: Tree view of the power attributes

where e_b is the energy per bit, e_{tx} and e_{rx} are the transmitter and receiver power consumption per bit, respectively, E_{dec} is the energy required for decoding a packet, and η is the payload length in bits [65].

Technology	Energy per bit
ZigBee (@ 40 Kbps)	5 x 10^{-7} Joules
UWB (@ 5Mbps)	5 x 10^{-12} Joules
Bluetooth (@ 1Mbps)	2.5 x 10^{-7} Joules
RFM TR1000 (@57.6kbps)	8.5 x 10^{-7} Joules

Table 2.2: Energy Consumption of various technologies [65]

Warneke et al. [90] give typical energy values required for computation. For example, typical instructions for microprocessors need energy in the order of pico Joules. The power consumption for sensing depends on the type of sensor used and the type of signal processing circuitry used.

Storage

Storage refers to the way WCDs store power for their operation. Storage is done either by using batteries or by using capacitors. Batteries are usually used when a longer life is required. Capacitors, on the other hand are used in applications which require bursty powers for very short durations. Batteries can be further classified into different types on the basis of their operation. Vieira et al. [60] compare a few battery technologies available. Capacitors can also be classified into different types, but the operating principle of a capacitor is the same irrespective of its type.

Energy harvesting mechanisms

Some WCDs have energy harvesting mechanisms by which they can harvest power from the ambient environment. Some of these mechanisms are:

1. Harvesting light energy using Photo-voltaic (PV) materials. PV materials use photo-electric effect to convert light energy into electrical energy. The pico radio project at Berkeley developed a radio, which uses ambient light energy for communication [72]. Recently, Lin et al. [52] have designed a energy harvesting module for commonly used sensor nodes. The module uses PV cell enclosure for powering the sensor nodes.

2. Harvesting ambient vibrational energy. Meninger et al. [55] in their paper discuss methods to convert vibrational energy into electrical energy.

3. Energy harvesting using thermal gradients. For example, it is possible to use body heat to store energy and use this energy for powering medical sensors [82].

Transfer

Energy transfer is the way by which passive RFID devices are powered. This takes place in the following ways: inductive coupling, capacitive coupling, and passive backscattering. Inductive (capacitive) coupling refers to the phenomenon of energy transfer via a magnetic field (electric field). Passive back scattering refers to method of scattering an RF signal and modulating the signal by varying the impedance.

2.4.3 Memory

WCDs need memory for storing data, which can be either user defined or application-related. For WSN applications, memory is needed for primarily storing application related data and performing computations on this data. We classify memory into two kinds: one depending on the purpose of storage and the other on the accessibility to memory.

Based on the purpose of storage, memory is classified as user memory and program memory. User memory is defined as the memory available to store user/application-related data. Program memory is the memory available for programming the device. This memory also stores any identification data that the device may have.

Table 2.3 shows the amount of total memory present for different WCDs. Memory can be classified into three categories on the basis of its accessibility. They are:

1. Read-only memory; this type of memory cannot be accessed for writing but can only be read. The contents of the memory are written during its manufacturing stage.

2. Write-once memory; this type of memory can be accessed only once for writing data and once written, the memory cannot be used for making changes.

3. Read and Write; this type of memory allows multiple reads and writes.

Devices	**Typical Memory**
Passive RFID devices	O(100 b)
Active RFID devices	O(1 kB)
Motes	O(100 kB)
Gateway devices	O(100 MB)

Table 2.3: Typical values of total available memory for different categories of WCDs

2.4.4 Sensors

Many WCDs consist of sensors. Commonly used sensors for WSN applications include temperature, pressure, humidity sensors, etc. The application determines what type

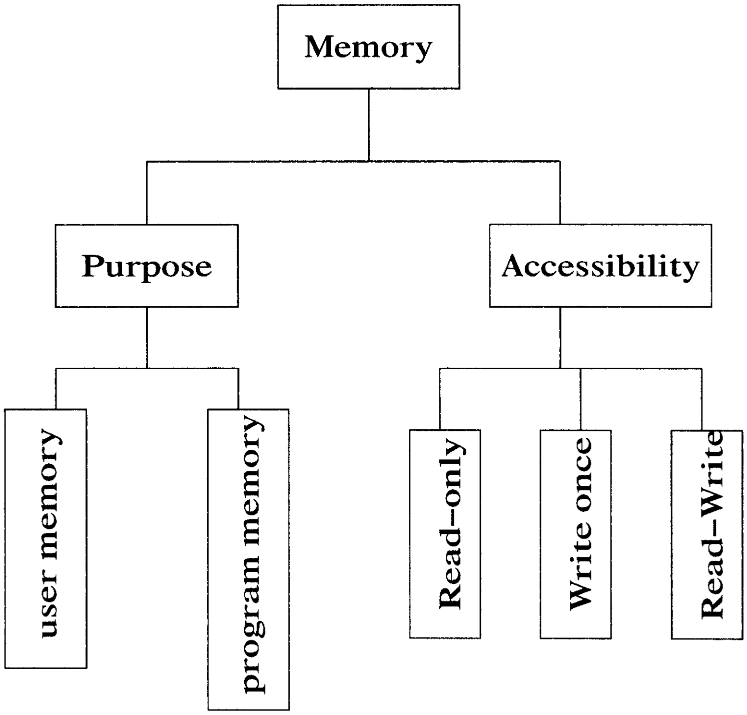


Figure 2-5: Tree view of memory

of sensors the device needs. WCDs usually provide capabilities for interfacing external sensors.

2.4.5 Other features

In this section, we consider two attributes, which cannot be categorized into any of the attributes. These are programmability and price. Programmability allows the devices to be reconfigured. For example, Mica motes are programmable and they can be programmed to control parameters such as sensor sampling rate, etc.

Another important feature is the price of the device. To have wider deployments, the price of the devices needs to be as low as possible. The price in turn is actually governed by the market demand for the applications. In this regard, passive RFID devices have very nominal prices (typically $.10, when bought in tens of thousands). This is because of the realization of the increasing need of RFID devices in the supply chain management. On the other hand, motes and gateway devices cost on the order of $100.

2.5 Examples

We give a few example representations of devices using our classification scheme [4]. The following are represented:

1. Mica mote (Figure 2.6)

2. High frequency RFID device (Figure 2.6)

2.6 Summary

To summarize, we developed a taxonomical scheme for classifying a wide range of WCDs on their functionality and characterized them on their attributes. Our classification scheme allows scalability and will allow a wider range of devices to be included in the future.

Having described an unambiguous way of classifying WCDs, which enables the users to know what the device is, we next discuss identification, which enables communication between devices.

[4] Numerical values are given in [ ].

Mica mote

- Ad hoc networking device
  - Communications
    - Standards
      - Proprietary/Others
        - RFM
          - Frequency
            - [916.5 MHz]
          - Data rate
            - [19.2 kb/s]
    - Modes
      - Ad hoc
    - Communication modules
      - [1]
    - Antenna type
      - [omnidirectional antenna]
  - Power
    - Storage
      - Battery
        - Ni/Li AA cells
  - Sensors
    - Optional accelerometer, light sensor, temperature, etc.
  - Memory
    - Purpose
      - User memory
        - [256 kB]
      - Program memory
        - [10 kB]
    - Accessibility
      - Read-Write
  - Other features
    - Programmable
      - TinyOS
    - Price
      - [$100]

Figure 2-6: Taxonomical representation of the mica mote

High frequency passive RFID tag

- Passive RF device
  - Communications
    - Standards
      - EPC
        - Frequency
          - [13.56 MHz]
        - Data rate
          - [10 kb/s]
    - Modes
      - Device talk first
        - Tag talk first
    - Communication modules
      - [1]
    - Antenna type
      - [omnidirectional antenna]
  - Power
    - Transfer
      - inductive coupling
  - Sensors
    - None
  - Memory
    - Purpose
      - User memory
        - [0]
      - Program memory
        - [128 b]
    - Accessibility
      - Write-once
  - Other features
    - Programmable
      - not programmable
    - Price
      - [$0.10]

Figure 2-7: Taxonomical representation of a HF RFID device

Chapter 3

An IPv6-based Identification Scheme

In this chapter, we propose an IPv6 identification scheme that can be used for identifying all kind of physical devices. We then propose routing schemes based on this identification scheme. The first routing scheme is for devices that use the wired Internet as a backbone for communication and the second routing scheme is for devices in wireless ad hoc networks. We describe some of the issues with the identification scheme, and the the advantages and disadvantages of the routing schemes.

This chapter is based on the work by Cheekiralla and Engels [11, 13] [1].

3.1 Introduction

Globally Unique IDentification schemes (GUIDes) enable a broad range of applications and provide the basis of secure and efficient functionalities. *Unique identifiers* enable secure and efficient communication capabilities, and they may act as pointers

[1] Copyright ©2006 IEEE. Parts of this chapter are reprinted from:

1. Sivaram Cheekiralla and Daniel W. Engels. An IPv6-Based Identification Scheme. In Proceedings of ICC 2006, Istanbul, Turkey, June 2006.

2. Sivaram Cheekiralla and Daniel W. Engels. Viral IP Address Assignment. In Proceedings of IEEE LCN 2006, pages 574575, Nov. 2006.

to additional information and services related to an object [26]. Examples of unique identifiers in the United States are zip codes for identifying postal areas, and social security numbers (SSNs) for identifying people.

In addition to a unique identifier, an object may have a *name* and an *address*. A name may be the same as the globally unique identifier, but it need not be unique just as a person's name may not be unique, but their SSN is unique. An address identifies either an object's location or the location where services exist for that object. Multiple objects may have the same address, just as many people may live at a single address, and the address need not specify an object's current location, just as a person's home address does not always specify where they are at any moment in time.

An object's name and address may change over time. The object and its owner may be mobile, possibly changing addresses and even names often. Similarly an object's owner may change over time since companies are known to sell their products from time to time. With either a change of location or a change of owner, an object's address and/or name are likely to change. The object's identifier, however, should never change.

A name or an address may not allow one object to talk to another object or even find out more information about another object. A unique identifier, however, is capable of acting as the reference that enables communication and services. In the networked world, a globally unique identifier that is based upon the Internet Protocol (IP) address scheme could easily be a reference to a name or a network address.

Objects may have communication capability inherent in their base functionality, e.g. routers and network interface cards have a network interface distinct from their base functionality in order to allow communication. A network interface to any object is possible by using a radio frequency identification (RFID) tag. An RFID tag consists of at least a microchip containing the identifier and an antenna for communication. A passive RFID tag does not have a power source of its own and only operates in the presence of a reader. The reader acts as the gateway for RFID tagged objects. All communication with such objects is through a gateway. The tag has limited functionality and networked proxies may be used to provide additional functionality. We define a proxy of an object as a device that provides services related to an object. Possible services include information services and location services. An object's networked proxy provides the intelligence for the object.

RFID tags allow object-to-object communication via the reader. There are potential applications of object-to-object communications in applications such as supply chain management, healthcare monitoring, and military operations. For example, RFID-tagged surgical instruments ensure that each instrument is placed in its proper container.

To summarize, an identifier is needed that:

- is capable of identifying all physical objects
- is persistent
- has a distributed allocation scheme
- may act as a network interface identifier
- acts as a pointer to information about the object the identifier identifies
- facilitates object-to-object communication
- can work with the existing Internet infrastructure

In the following, we propose an IPv6-based GUIDe that meets all of these requirements and is practically capable of uniquely identifying all physical and virtual objects. In Section 3.2 we discuss the requirements of a globally unique identification scheme. In Section 3.3 we discuss the IPv6-based identification scheme. Section 3.4 covers the IPv6-based name and routing service. In Section 3.5, we discuss previous work and compare it with our work. Section 3.6 extends the identification scheme to wireless ad hoc networks and discusses how the identifier can be used for allocating addresses in an ad hoc network. Section 3.7 discusses the details of the viral IP address assignment scheme, which allocates multiple addresses to nodes in the network. Section 3.8 concludes the chapter with the discussion on benefits of IPv6-based identification scheme and directions for future work.

3.2 Requirements of a GUIDe

A GUIDe is used for generating unique identifiers for a set of applications. A unique identifier generated from a GUIDe should be globally unique and should have global scope. Global scope implies the meaning of the identifier is the same everywhere. The identifier should be persistent and may be used to identify an object even beyond its lifetime. The GUIDe should be scalable and extensible for identifying different types of objects [26, 81]. While these requirements target global identification, they are applicable to all unique identification schemes regardless of their scope.

An identifier should have a partitioned structure that is either fixed or determined from the identifier itself. The partitioned structure itself should contain a tree-like topology of interpretation precedence and the number of identifiers possible within each partition must be manageable for the applications using the identifier. Such a partitioned structure allows hierarchical representation of identifiers and allows scalability and extensibility of identifiers and their allocation. Apart from these requirements, there are requirements on the identifier encoding. An identifier encoding is a symbolic representation of the identifier. It should allow an easy comparison of two or more encodings in a straight forward manner, and should have the capability to be communicated over a communication system [26].

Having discussed the requirements of an identifier and a GUIDe, we discuss the IPv6-based identification scheme in the following section.

3.3 IPv6-based Identification Scheme

We briefly discuss the IPv6 addressing scheme and then we propose our new IPv6 identification scheme. We then compare and contrast an IPv6 address with an IPv6 identifier.

Table 3.1: IPv6 address allocation [39]

allocation	**binary prefix**	**fraction of address space**
Unassigned	001	1/8
Provider-based Unicast address	010	1/8
Link local address space	1111 1110 10	1/1024
Site local address space	1111 1110 11	1/1024
Multicast	1111 1111	1/256

3.3.1 IPv6 Address

An Internet Protocol (IP) address is used as a network address for defining the logical location of a network interface on the Internet. An IP address is needed for communicating in the Internet. Routers, which are the connecting bridges between different networks, use IP addresses for routing the traffic. IPv6 is the next generation Internet protocol that offers expanded addressing, and provides support for quality-of-service (QoS), better end-to-end support, and easy management of routing tables [39].

The different types of IPv6 addresses are: unicast, multicast, anycast, and link-local addresses. Table 3.1 shows the different types of addresses and their allotted address space. The most important address is the provider-based unicast address. Table 3.2 shows the format of a unicast address. A unicast address has a 5-bit registry ID, which is the ID of the agency that is responsible for assigning network addresses in a geographical area. For example, the Asia-Pacific Network Information Center (APNIC) is in charge of assigning addresses for networks in Asian and Pacific countries. The other registries are: American registry for Internet Numbers (ARIN) for North America, Reseaux IP Europeens Network Coordination Centre (RIPE NCC) for Europe, Middle-East, and Central Asia, Latin American and Caribbean Internet Addresses Registry (LACNIC) for Latin America and Caribbean, and AfriNIC for Africa. The provider ID in the IPv6 address is the 16-bit ID of the Internet service provider (ISP) and is obtained from the registry. The subscriber ID is the 24-bit

Table 3.2: IPv6 unicast address format [39]

010	registry ID	provider ID	0	subscriber ID	0	subnet ID	interface ID
3	5	16	8	24	8	16	48

Table 3.3: Format of the IPv6 *general identifier*

value	0010	agency ID	domain name	0	object class	serial number
no. of bits	4	5	48	7	16	48

ID of the subscriber and is obtained from the provider. The subnetwork ID is the 16-bit ID of a sub-network and the interface ID is the 48-bit unique identifier within a subnetwork. Following the provider ID and the subscriber ID, 8 bits each (total of 16 and all set to "0") are reserved for future extension purposes [39].

3.3.2 IPv6 Identifier

An IPv6 address has 128 bits and can potentially address $2^{128} (\approx 3.4 * 10^{38})$ objects, or every molecule on the surface of the earth. Table 3.1 shows a part of the IPv6 namespace allocation. For the complete allocation, the reader is referred to [39]. For IPv6 identifiers, we propose to use the unassigned IPv6 namespace that has the binary prefix "001". This constitutes $1/8^{th}$ of the namespace and should be sufficient for identifying all the physical objects that are manufactured in the foreseeable future.

We propose two formats for the identifiers (Table 3.3 and Table 3.4); the first one, which we call the *general identifier* has a format that is similar to a provider-based

Table 3.4: Format of the IPv6 *pseudo-random identifier*

value	0011	agency ID	random number
no. of bits	4	5	119

unicast address (Table 3.2) and the second one is a *pseudo-random identifier*. The *pseudo-random identifier* is a flat identifier and hence provides a sense of privacy by not revealing any information about the object that it identifies.

In the *general identifier*, a 5-bit agency ID is used to represent the agency that is responsible for allocating the identifier. It is analogous to the registry ID of the provider-based unicast address. The domain name represents the company or organization's name that is using the identifier. The 7 bits of zeroes that follow after the domain name are reserved for future extension purposes. The object class is assigned by the company and is used for identifying different types of objects. The serial number uniquely identifies objects belonging to an object class.

The concepts of domain name, object class, and serial number are similar to the practical deployed numbering schemes such as the electronic product code (EPC) [77]. For the *pseudo-random identifier*, the random number in the identifier is assigned by the agency that is responsible for allocating the identifier. For defining future versions of identifiers, we propose to use the unused namespace.

Consider the following example: company "X" manufactures an object of type "Y". Assume that the agency ID or the identifier assigning agency for the location where the company is located is "R". We assume that "R", "X", and "Y" are the appropriate bit representations of the agency ID, domain name, and object class respectively. For a particular object manufactured by this company, of type "Y", the identifier would be "0010-R-X-Y-0000000-SN". The suffix "SN" is used for uniquely identifying the object and is assigned by the company. On the other hand, a flat identifier would look as "0011-R-RN", where "RN" is the bit representation of a random number assigned by the agency.

An IP address is used for locating a network host in the Internet, while an IP identifier is used for identifying physical objects. The prefix of an IPv6 address is "010" and that of an IPv6 identifier is "001". There are many similarities between the *general identifier* and the provider-based unicast address. Both of them have a similar partitioned structure. The registry ID and the agency ID have similar function and it is possible for the Internet registries to take the responsibility of the allocation of the identifier space. The domain name is similar to the combined provider ID and subscriber ID. It is possible to allocate the IP address/identifiers in such a manner that an organization will have a domain name which is the combination of the provider ID and subscriber ID (including the 7 bits of "0" used for extension purposes). The object class and subnetwork ID are similar as they identify a particular object/subnetwork given a domain name/provider ID and subscriber ID. The serial number is analogous to the interface identifier. A serial number (interface identifier) uniquely identifies a particular object (network interface) of an object class (in a particular subnetwork).

Because of the similarities of the structure of an IPv6 address and an IPv6 identifier, we define a *corresponding* address for an identifier and vice-versa. The *corresponding* identifier (address) for an address (identifier) is obtained by changing the 3-bit binary prefix. By defining the identifier in a similar format to the unicast address format, an organization can have the *corresponding* identifier space for its address space. This concept is utilized in providing functionalities for an object.

The IPv6 identifier may be used to obtain the IP address of the services related to an object. These services include locating the information provider of an object or finding the address of an object or its gateway so that communication may be established.

The IPv6-based identification scheme satisfies all the requirements of a globally unique identification scheme as discussed previously, and has sufficient identifier space to identify all physical objects. Since physical objects are owned by different persons/organizations at different points of time, we suggest two methods to track objects across multiple domains. These methods use the existing core concepts of the Internet as described next.

3.4 IPv6 ID services

In order to communicate with an object, the IPv6 address of the object is needed. We assume that objects that don't have communication capability use RFID tags or similar automated identification technology and we are interested in communicating with the gateway of the object in such a case. For the rest of the chapter, when we refer to address, we mean the IPv6 address. We also define the *creator's domain* as the domain in which the object is assigned an IPv6 identifier. Apart from communicating with the object, one may also like to find information or proxy services about the object. We propose two methods for finding the address of the object and the address of the object's information provider. When we refer to IPv6 identifier in these two methods, we mean the *general identifier*. In the first method, we propose a name system that translates identifiers to addresses. This name system is based on the identifier of the object and relies on the domain name system (DNS)[56] for finding the address of the object or that of the information provider. The second method uses the identifier of the object in the packet header for communication or locating the information provider or proxy.

3.4.1 Name System

An object may have multiple names and multiple addresses over time but the identifier must remain the same. At any instant of time, the mapping between an identifier and a name is one-to-many and the mapping between an identifier and an address is one-to-one (for physical objects). The name of an object or its proxy may be constructed from the object's IPv6 identifier. It is possible to have aliases for names while it is not possible to have aliases for identifiers. A taxonomy in designing naming systems and the issues associated with it are given in [92]. The name system described in our work uses the DNS for finding an object's (or its proxy's) address from its name.

Table 3.5 shows an example of an object's name and it's proxy based on IPv6 identifiers. The first column shows the bits in the IP identifier, the second column shows the name of the object, and the third column shows the name of the proxy. The complete object name and proxy name are shown in the last two rows of the table. The names are written in the reverse order in which they are constructed. All proxy names and object names end with "obj" and a "." is the delimiter for the partitions in the identifier. We assume that a new top-level domain (TLD) is created to accommodate these names in the DNS and for the rest of this chapter

Table 3.5: Naming system based on IPv6 identifiers

bits	object name	proxy name
0-2	obj	obj
3-7	apnic	apnic
8-55	d-name	d-name
64-79	o-class	o-class
80-127	sn	-
object name	sn.o-class.d-name.apnic.obj	
proxy name	o-class.d-name.apnic.obj	

we assume that DNS has "obj" records. In the table, we use APNIC (which is an Internet registry) as the agency ID for IP identifiers, "d-name" as the domain name of the object, "o-class" as the object class, and "sn" as the serial number. The serial number is a 48-bit number and in actual names, "sn" will be replaced by the bits in hexadecimal format. The compressed representation used for IPv6 addresses can be used for representing the "sn".

Typically, when an object is created, the creator of the object assigns the identifier, and based on the identifier the name is also assigned. An appropriate DNS record for the object or its proxy is created. This is done only if the owner of the object decides that the object or its proxy can be reached over a communication network. The initially assigned name is the canonical name of the object and any other names assigned later are aliases. When the object moves to a different domain, the new owner just updates the existing DNS record with the new IP address of the proxy or of the object. If the owner wishes, he/she creates a new name, which will be an alias of the canonical name and update the DNS records. The time to live (TTL) field in the DNS specifies the time for which the name-address mappings should be cached. It is possible to set this value to "0" to prevent stale mappings [80]. The TTL value is a design parameter and the value depends on the rate at which the object changes domains. An object that moves into a different domain gets an IP address using the auto-configuration scheme described for IPv6 or using an existing method like DHCP or uses its proxy (gateway) for communication. For security reasons, the DNS

Table 3.6: Translation table in a gateway router

Index	IP identifier	Address of proxy
1	0010...1000...1001 0010...1000...1010 0010...1000...1011 0010...1000...1100 0010...1000...1101	0100...1000...1011
2	0010...1001...1101	0100...1000...1011
3	0010...1010...1000	0100...1000...1011
4	0010...1010...1001	0100...1010...1001

records should only be changed by a DNS gate keeper or the authenticated proxy of the object.

DNS is not designed for dynamic updates of mappings [70]. Hence, a locationing service should be provided that provides the location of the object. The locationing service will have a fixed name/address to avoid DNS updates. This locationing service is provided by the proxy.

3.4.2 Address forwarding scheme

The address forwarding scheme is similar to the mobile IPv6 scheme. Mobile IPv6 specifies routing support to IPv6 hosts by allowing them to use their permanent "home address" even when they move across different domains. In mobile IPv6, the "home agent" takes care of the routing issues associated with the "mobile node" [67].

For our scheme, we assume that routers are configured to distinguish identifiers from addresses. In this scheme, the IPv6 identifier is used as the destination address in the datagram instead of the IPv6 address. When routers see an identifier instead of an address in the datagram, they treat the packet as if it were addressed to the *corresponding* IP address. We further assume that the *creator's domain* owns the *corresponding* address space of its identifier space; however this need not be true.

When an IP identifier is assigned to an object, the *corresponding* IP address is the address of its proxy. In order to reach the proxy of the object, one uses the IP identifier in the IP datagram, and the router routes the packet to the *corresponding* address. However, it might happen that multiple objects have the same proxy. For example, objects of the same class have a single server providing information about all of them. Further, the same proxy could also serve information about multiple objects. To address this issue, the local or gateway router is configured to route packets that use identifiers as the destination address to the object's proxy. Thus, the local or gateway router performs a translation service for IP identifiers. Table 3.6 shows a snapshot of the local router's translation table for IP identifiers. The first 3 entries (corresponding to the indices from 1-3) in Table 3.6 shows objects belonging to different classes having the same proxy. The 1st entry corresponds to objects of the same class having a single proxy. While entries 3 and 4 have objects belonging to the same class but have different proxies. It is possible to use the net mask representation to compress the entries in the routing table. Since a proxy can serve objects of multiple classes, the IP identifier in the datagram is used for delivering the information about the right kind of object.

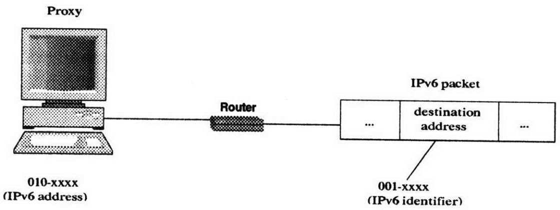


Figure 3-1: Routing packets with IPv6 identifier as the destination address

When a user tries to reach the object that is in the *creator's domain* (say it is called "d"), the datagram uses the IP identifier as the destination address. When an external router sees an identifier in the datagram, it sends the traffic to the *corresponding* address (see Figure 3-1). Since the *corresponding* address belongs to domain "d", the traffic passes through the gateway router of domain "d". The gateway router sends the datagram to the appropriate proxy depending upon the identifier in the datagram. Over time the proxy of an object might change and all the routing tables of the "d"'s routers will be updated accordingly.

A problem arises when a user tries to reach the proxy of an object that is not in the *creator's domain* by using its identifier in the datagram. For resolving the mobility issue we use the idea of "home agent" in mobile IPv6. When the object moves to a domain that is different from the *creator's domain*, the new proxy informs its address to the old proxy. Further, the new proxy also informs that any traffic for the object/proxy should be forwarded to the new proxy's address. When a user uses the IP identifier for communication, the IP packet will be routed to the new proxy via the original proxy.

This method can be further extended if the object moves across different domains. The new proxy only informs the original proxy if the new owner wishes that the object should be reached. This method leverages the similarity between the IPv6 address and the IPv6 identifier format. This method is not efficient if the object keeps moving across multiple domains. In our work, we do not address the security and privacy concerns that arise from this approach.

3.5 Previous work

Numerous identification schemes are deployed commercially, these include proprietary schemes as well as industry adopted schemes such as the vehicle identification number (VIN) for automobiles and the universal product code (UPC) for retail. Global unique identifiers have only recently gained widespread adoption with the deployment of the EPC. The EPC is an identification scheme for identifying all physical objects with Radio Frequency IDentification (RFID) tags. The EPC was originally specified by the Auto-ID Laboratory, MIT. The present EPC Standard is specified by the EPC Global Inc. EPC was created to enable the Internet of Things using RFID tags. It is mainly used in supply chain management applications today. EPC is a meta-code that accommodates various existing identification schemes. The EPC identification scheme also defines a General IDentifier (GID) that is independent of the existing schemes. The GID encoding has 4 fields; these are: the "header field", the "General Manager Number", the "Object Class", and the "Serial Number". The "General Manager Number" identifies the organizational entity which is responsible for assigning the

"Object Class" and the "Serial Number". The "Object Class" identifies a particular type of object, and the "Serial Number" identifies a unique object in a given "Object Class" [77]. The EPC in conjunction with the Object Name Service (ONS), is used for locating the network address of services associated with an object. The ONS takes the EPC encoding in uniform resource indicator (URI) form and returns an URL to the querying application [63, 31].

The IPv6 identification scheme name system proposed in Section IV is similar to the ONS. However it should be noted that the ONS is a separate service from DNS and in our case we are directly relying on the DNS. However, our system requires a new TLD, which the ONS doesn't require. Using IPv6 identifiers also allows the routers to perform translation service. This is similar to a distributed database scheme allowing scalability. However, the EPC lacks such an advantage. Since our system uses IP, it can easily integrate with the existing Internet infrastructure and using IPv6 identifiers truly creates an "Internet of Things". It allows a wide variety of devices having different capabilities to be identified using a single scheme that is harmonized with the IPv6 network address scheme.

Other relevant work on identifiers includes the work on the host information protocol (HIP), keyed hash identifiers (KHIs), and distributed hash tables (DHTs). HIP resides in between the IP and transport layers and is designed for providing improved mobility support, multi-homing, and trust between systems. HIP uses IPv6-based identifiers as host identifiers; host identifiers use an unallocated IPv6 namespace and have a fixed 4-bit binary prefix. A host identifier is inherently cryptographic in nature because it is the public key of an asymmetric key-pair. The reader is referred to [57] for more details. Even though HIP uses an IPv6-based identifier, it does not address the issue of identifying all physical objects using IPv6. As such , there are significant problems in scaling to all objects on earth.

KHIs are IPv6-based identifiers that are designed to be statistically unique and non-routable. Depending on the context, they can be used in different protocols such as HIP and mobile IPv6. Work on KHIs is ongoing and more details can be found at [62]. It is possible to use the work done on HIP/KHI for the *pseudo-random identifier.*

DHTs use identifiers based on hashes and are usually longer than 128 bits (e.g. Chord [84] uses 160-bit identifiers) and are used in applications such as peer-to-peer networks. Other applications of DHTs include using them as an indirection mechanism for providing better communication support (such as multicast, anycast, etc.) in the Internet [83]. DHTs are not intended as universal identifiers.

Having discussed the IPv6 identification scheme, we discuss how this scheme can be extended to wireless ad hoc networks.

3.6 IPv6 identifiers for wireless ad hoc networks

With the advances in wireless technology, ad hoc networks such as sensor networks and mesh networks are becoming a reality. The fundamental aspect of these networks is communication. Most work on wireless ad hoc networks assume that node addresses are assigned either using auto-configuration schemes or using a specifically designed address assignment scheme. Both these schemes allow a node to acquire an address when it joins a network. Address assignment schemes for wireless ad hoc networks assume that the identifier and the address are the same. In these schemes an address doesn't have any location information, but is purely used as an identifier. However, we assume that an address and an identifier are two different and distinguishable entities.

We propose a new address assignment scheme, where nodes have multiple addresses, and each address corresponds to a logical location of the node in the network. Further, nodes assign address to each other in a contagious fashion resembling a viral growth. We state the requirements of such a scheme and discuss a few issues with this scheme.

In the following Section, we discuss the details of the viral address assignment scheme.

3.7 Viral address assignment

We assume that the network is a relatively static network with few nodes joining and leaving over long intervals of time. We further assume that a node joining the network has an IPv6 identifier. It may be argued that the MAC address of an interface could be used as a node identifier. However, work done by Thoppian and Prakash [69] discusses the non-suitability of MAC address as an identifier.

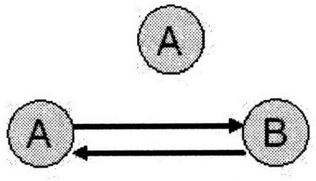


Figure 3-2: A single node exists in the network before another node joins the network.

Given an identifier, we define a *corresponding* address space from which a node assigns address to itself and other nodes. This address space is part of the IPv6 site-local address space. The node also allocates a part of its address space to other nodes when it discovers them. Initially, a single node (say A) exists in the network and when another node (say B) joins the network, the new node (B) searches for other nodes and finds the existing node (A). After the discovery stage, both nodes assign an address and a part of their address space to the other node. After this step both the nodes have two addresses, one of which is assigned by the other node. Now, node C and node D discover A. Node C and node D get addresses and address spaces from A. These addresses are from As and Bs address space. Similarly, E and F discover B. Node B assigns these nodes addresses from As and Bs address space. Now, all the nodes have 2 addresses, one relative to A and the other relative to B. This process is repeated as more nodes join in the network. Since the address assignment process is similar to viral growth and therefore is termed as viral address assignment.

An important issue is to map identifiers to address spaces. A simple solution to this issue is to allocate the address space based on the identifier. For example, a node having an identifier “001...A-B-C”, where A,B, and, C represent the last 118

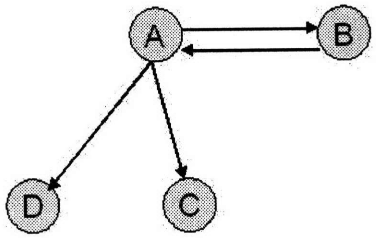


Figure 3-3: Additional nodes discover node A.

bits, would have an address space of "1111 1110 11-A-B/C". Once the address space is chosen on this basis, A, B, and, C should be chosen so that a node has sufficient address space to allocate to its n-hop neighbors, where n is a design choice.

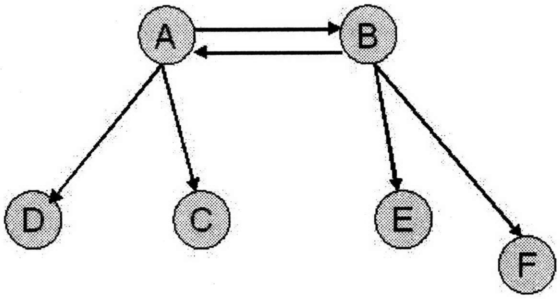


Figure 3-4: All nodes now have two addresses, one with respect to A and the other with respect to B.

If nodes keep assigning addresses to each other, maintaining the routing tables would be memory intense. Thus, we need to restrict the number of address assigning nodes to a limited number (say 5-10). This implies that a node can potentially have 5-10 addresses.

It may happen that some of the nodes have identifiers whose bit values differ only by a few suffix bits. In such case, existing methods for detecting duplicate addresses need to be employed [69]. These methods need further optimizations to account for multiple addresses that nodes have.

The address allocation is done on the basis of prefixes. Nodes that are the one-hop neighbors from a given node have the same prefix. Prefix-based addressing (Fig.3-5) gives the logical location of a node with respect to the node that owns the address space. Prefix-based addressing is a well studied concept and has been used recently by Eriksson et al. [29] for assigning addresses to nodes in a wireless ad hoc network. Having an address which has logical location information makes routing simpler and efficient.

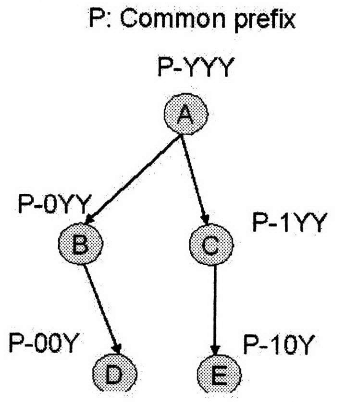


Figure 3-5: Example of prefix-based addressing

Nodes with multiple addresses provide redundancy to the system. Wireless links are prone to more failures than wired links, and thus, redundancy becomes an essential feature. Multiple addresses also allow multiple routes between a source and a destination. The benefit of multiple routes is that each route can be used for a particular kind of traffic, and potentially QoS guarantees could be achieved by reserving specific paths.

We discuss existing work on address-based routing in wireless ad hoc networks.

3.7.1 Relevant Work

Eriksson et al. [29] have proposed an address-based routing scheme that is primarily designed for ad hoc and mesh networks. They propose a new routing scheme that is based on the concept of addresses having location information. For their routing scheme, they assume that nodes have an identifier. Similar ideas have been proposed for sensor networks. Pal Chaudhari et al. [8] propose an addressing and routing architecture for sensor networks, which is based on constructing prefix trees in an efficient manner. Motegi et al. [79] propose an on-demand addressing scheme, where nodes are only assigned addresses when the base-station has to communicate with the node. However, our concept of viral address assignment is novel as nodes have multiple addresses.

We draw the relevant conclusions in the next section and discuss directions for future work.

3.8 Conclusions

In this chapter we have presented an IPv6 identification scheme that can be used for all physical objects, including network interfaces. The scheme allows objects to have identifiers within the IPv6 namespace that are distinct from and inter-operable with IPv6 addresses.

Unique identifiers enable a platform of applications and can be used to improve security and provide intelligence to objects. A distinct identifier is required to ensure that an object may be consistently identified through out its life, even as it moves and changes ownership. The main advantage of this method is the ability to use the existing network infrastructure to provide communication capability to objects. We have proposed two ways of reaching an object or its proxy when the object moves from one domain to another. The first method is based on a naming system using IPv6 identifiers. This method relies on the DNS to keep track of the mappings between object (proxy) names and object (proxy) address. Having names for objects is also beneficial for applications where there is human involvement, as humans are more comfortable dealing with names rather than numbers. The second method is similar to the mobile IPv6 concept. Both the IPv6 ID services use the existing core Internet technologies and these systems have been studied widely and their performance has been characterized.

The identification scheme also considers the issue of network connectivity, which some of the schemes don't consider. Since the identification scheme uses IPv6 identifiers, it is possible to use the existing Internet protocols. The IPv6 identifier also acts as a pointer to information and services about an object. It also facilitates object-to-object communication and satisfies all the requirements of an identifier that are stated in Section I. The object-to-object communication enables us to realize the vision of the "Internet of Things" [7]. The IPv6 identification scheme allows the realization a distributed service with the routers providing translations from the identifiers to the addresses. This is in contrast to the EPC system, which uses a centralized service to provide services about objects [63].

We also suggest that the Internet registries should take the additional responsibility of assigning IPv6 identifiers. This way, a company can get an address and identifier space which are *corresponding*. This allows easy management of both the address and identifier spaces. Finally, our identifier scheme uses IPv6-based identifiers and hence can coexist easily with the Internet architecture.

Having a single global identification scheme that is harmonized with the Internet enables efficient allocation of identifiers and provisioning of networked information services that can be used to include business processes and provide additional services to consumers.

We also extend the IPv6 identification scheme and propose a novel viral IP address assignment scheme. The viral IP address assignment scheme subsumes many of the existing concepts such as prefix-based addressing, the concept of nodes having IPv6 identifiers, and existing work on detecting duplicate addresses in wireless ad hoc networks. To summarize the Viral address assignment scheme, it provides the following advantages. Since multiple addresses are used, multiple routes can be found. Multiple routes imply redundancy in wireless ad hoc networks. Since wireless links are error prone and their quality can fluctuate with time, redundancy is a desired feature in the network. Further it may be possible to achieve QoS guarantees with multiple routes by reserving specific paths for a particular kind of traffic. However, having multiple addresses is resource expensive and this scheme may not be scalable to a large number of nodes.

3.8.1 Future work

This chapter provides the initial steps for developing the IPv6-based identification scheme. Further work needs to be done to make this identification scheme usable. One of the most important areas is that of security and privacy. We have not addressed security and privacy here. Security and privacy issues are common to other identification schemes [78] and to the mobile IPv6 service and the DNS [4, 3].

The effect of the TTL value in the DNS record needs to be analyzed. It affects the performance of the DNS as some objects move across different domains at a faster rate and some of them may not move at all. This issue is considered in some detail in [80].

Apart from these issues, reachability and existence must be addressed. Various methods need to be developed so as to test the identification scheme such that the uniqueness of identifiers is guaranteed and so that this identification scheme can be used.

In this chapter, we also proposed a novel concept of viral IP address assignment scheme, where nodes have multiple addresses. We identified a few design areas and issues in our scheme. These include assigning address spaces on the basis of identifiers and an efficient way to detect duplicate addresses. We plan to address these as part of future work.

Having discussed taxonomy and identification schemes, which are applicable to a broad class of heterogeneous networks, we discuss a specific case of heterogeneous networks in the next chapter. These networks consist of nodes that either use omnidirectional antennas or smart antennas.

Chapter 4

Heterogeneous Wireless Ad Hoc Networks

In the previous chapters, we discussed the taxonomy scheme and the IPv6-based identification scheme. These schemes are applicable to a broad class of heterogeneous networks. In this chapter, we discuss a specific case of heterogeneous networks in which the nodes are equipped either with a smart antenna or with an omnidirectional antenna.

The remainder of the chapter is organized as follows. In Section 4.1, we provide motivating examples of heterogeneous networks and discuss previous work on heterogeneous networks. In Section 4.2, we discuss the different types of smart antennas and the details of the antenna model that we use in this thesis. In Section 4.3, we discuss benefits and issues of directional antennas.

4.1 Motivation

Many wireless ad hoc network applications involve inherent heterogeneity. For example, typical sensor network applications involve using devices with varying capabilities [91] or using a hierarchical architecture with devices having varying communication and computing capabilities [68]. We consider heterogeneity due to the type of antenna a node uses.

Beamforming or smart antennas improve the network performance through increased spatial reusability and provision of higher communication range. These antennas usually consist of arrays of antennas, whose signals are combined to achieve a better performance compared to omnidirectional antennas. We assume that a beamforming antenna is more expensive than an omnidirectional antenna. Hence, it may not be economically feasible to have a network in which every node uses a beamforming antenna. Therefore, it is possible to imagine a heterogeneous network in which a few nodes use beamforming antennas and the others use omnidirectional antennas.

Since smart antennas have a superior performance compared to omnidirectional antennas, we assume that a heterogeneous network of omnidirectional and smart antennas has a better performance than a homogeneous network of omnidirectional antennas. We envisage that these heterogeneous networks will be useful in applications such as disaster management or providing Internet connectivity to remote locations. In such scenarios, the edge nodes are nodes equipped with omnidirectional antennas and the intermediate nodes are equipped with smart antennas providing shorter and better links for achieving a higher throughput.

We discuss previous work on heterogeneous networks in the following.

4.1.1 Previous work

Sundaresan and Sivakumar [47] propose a MAC and routing protocol for heterogeneous networks that includes omnidirectional antennas, fixed-beam antennas, adaptive-array antennas, and Multiple-Input, Multiple-Output (MIMO) antennas. They describe a routing protocol similar to DSR for heterogeneous networks, which uses a three-tuple routing metric. The first two components capture the spatial reusability of the network and the third component captures the link rate.

Yarvis et al. [91] use a resource aware routing protocol and MAC protocol for exploiting the heterogeneity in the network. Heterogeneity is considered from an energy and link perspective. They evaluate the quantity and placement of the heterogeneous nodes in the network through analysis, simulation, and deployment. They find that using a modest amount of line-powered nodes and long-range back haul links improves the network life time. Fujii et al. [32] describe a MAC protocol for heterogeneous ad hoc networks where nodes use different transmission powers. They propose using additional handshake messages that allow lower-powered nodes to communicate effectively in the presence of higher-powered nodes.

Much of the existing work on wireless ad hoc networks assume that omnidirectional antennas are used at the physical layer. The IEEE 802.11 MAC protocol also inherently assumes that omnidirectional antennas are used. However, it is possible to use smart antennas for wireless ad hoc networks [74]. We discuss smart antennas in the next section.

4.2 Smart antennas

Smart antennas are arrays of antennas arranged in a pre-determined order, whose signals are combined to achieve a specific beam pattern. The signals can be combined in two ways, switched diversity and diversity combining. In switched diversity, a single element is chosen for the best signal and thus there is no "gain" by using this method. With diversity combining, there is an increase in the "gain". We discuss different types of smart antennas [43].

Single-beam model and multi-beam model

In the single-beam model, only one beam can be used at a time, while in the multi-beam model, more than one beam can be used at a time. The gain of a single-beam is higher than the omnidirectional mode. For the multi-beam model, the gain depends on the number of antennas used. A constant power P_w is fed to the antennas, and this power is split amongst the number of beams in use. Thus the higher the number of beams in use, the lesser the gain. Omnidirectional mode is achieved by using all the beams and hence has the least gain.

Switched-beam systems and steered-beam systems

In switched beam systems, multiple fixed-beams are formed either by shifting the phase of elements by a predetermined amount or by switching between several fixed directional antennas. In steered-beam systems, the beam can be pointed in any required direction. With steerable antennas, the direction of the main lobe can be pointed to a given direction with very fine granularity, and in switched antennas the direction of the main lobe is more discrete.

Steerable antennas can be classified as dynamic phased arrays or adaptive arrays. Dynamic phased arrays provide beam steering and adaptive arrays additionally provide adaptive beamforming. In adaptive beamforming, nulls are produced towards the interfering sources.

Details about different types of directional antennas and their gain models are discussed in [49]. We now discuss the radiation pattern of smart antennas.

4.2.1 Radiation pattern

Smart antennas have a radiation pattern that is not uniform in all directions. Thus these antennas are also called as directional antennas, and henceforth, we refer to them as directional antennas. On the other hand, isotropic antennas have a radiation pattern that is uniform in all directions. Thus for a directional antenna the gain in a particular direction $\vec{d}(\theta, \phi)$ is defined as:

$$G(\vec{d}) = \eta \frac{U(\vec{d})}{U_{ave}} \tag{4.1}$$

where η is the efficiency of the antenna, U($\vec{d}$)is the power density in $\vec{d}$ and U_{ave} is the average density over all directions. The peak gain is the highest gain over all directions. Gain is often expressed in decibels, $G_{dbi} = 10. \log_{10}(G_{abs})$. The beam-width of an antenna, usually referred as the *3 dB beam-width*, is the angle subtended by the two directions on either side of the peak gain that have a lower 3dB gain than the peak gain. Figure 4-1 shows the radiation pattern of an isotropic antenna and the simplified radiation pattern of a directional antenna.

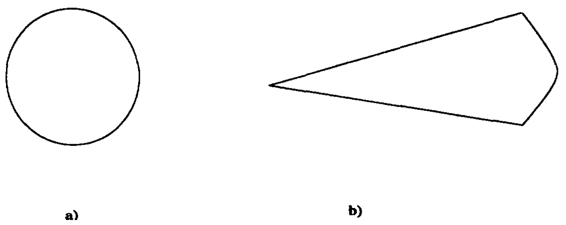


Figure 4-1: Typical radiation pattern in a) isotropic antenna and b)the simplified radiation pattern for a directional antenna

Antenna model

For our current work, we use a switched, single-beam antenna model with 8 beams. The beam-width of each beam is 45 degrees and has gain of 15 dB. Together, the 8 beams span the azimuthal range. The radiation pattern for the beams is shown in Figure 4-2. This pattern is different from the simplified radiation pattern and accounts for the side lobes and the back lobes, which contribute a non-trivial amount of radiation.

We assume that nodes have an omnidirectional and a directional mode. While transmitting, the node can either choose an omnidirectional transmission or a directional transmission. Nodes are assumed to be in the omnidirectional mode when they are idle, and upon detecting a signal switches to the best beam for receiving. Thus receiving is always directional. We use the omnidirectional mode of directional antennas for broadcasting. A similar model is used by Subramanian and Das [85].

We use the following notation. OM stands for omnidirectional mode and DM stands for directional mode. An OD node is an omnidirectional node and a D node is a directional node. We define the following communication ranges: O-O is the possible communication range when both nodes are OD nodes. We define D-O range when the sender, a D node uses directional transmission and the receiver is an OD node. Similarly the definitions of O-D range and D-D range follow. We mention the values of ranges and other relevant values in the simulations section in the following chapters.

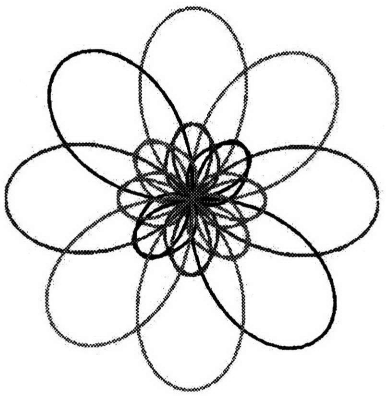


Figure 4-2: Radiation pattern of the antenna model used in this thesis

Other antenna models

Ramanathan [74] in one of his earliest papers on smart antennas assumes that the antenna can only transmit directionally and receive only in omnidirectionally. However, subsequent work by other researchers [15, 54, 18, 33] assume that there are two separate antennas and receiving is possible in both directional as well omnidirectional mode, and transmitting is possible in directional mode only. Thus for this model, the notion of a broadcast doesn't exist. A comprehensive listing of antenna models used in ad hoc networks can be found in [49]. We discuss features and issues of directional antennas in the next section.

4.3 Features and Issues

Directional antennas have a higher gain in the direction of interest and a reduced gain in other directions. These features provide a few advantages that can be leveraged in wireless ad hoc networks. These are:

1. Increased network capacity because of higher spatial reuse [49, 93]. This can be attributed to the radiation pattern of directional antennas, which allow more simultaneous conversations compared to omnidirectional antennas (Figure 4-3).

Yi et al. [93] derive the capacity of an ad hoc network with directional antennas, they show that the capacity of a network that uses directional antennas increases by a constant factor over a network that uses omnidirectional antennas.

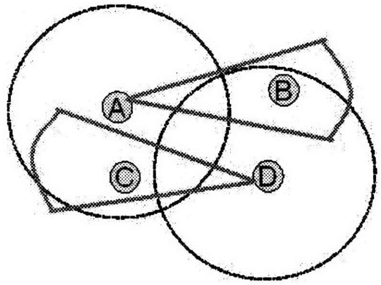


Figure 4-3: Increased spatial reusability with directional antennas [49]

2. Improved routing performance and network connectivity due to increased transmission gain (Figure 4-4). Directional antennas have a higher gain (in the direction of the main lobe) than omnidirectional antennas, and hence for the same power, directional antennas have a higher transmission/reception range than omnidirectional antennas. This also implies that it is possible to reduce the power-consumption of a node while transmitting.

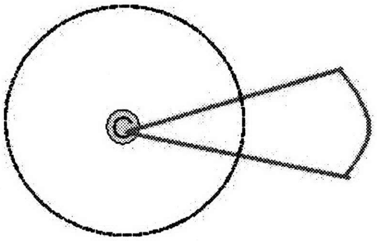


Figure 4-4: Increased transmission range of directional antennas

3. Increased signal quality and reduced interference because of directionality of the radiation pattern.

4. Reduced eve-dropping or increased security because of directionality in transmission. Directional antennas are used for reducing wormhole attacks in wireless ad hoc networks [38].

Directional antennas share some of the same problems as omnidirectional antennas such as hidden terminal problems. In addition, there are new problems introduced

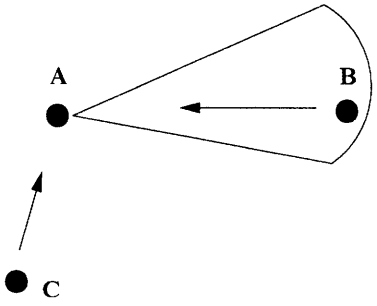


Figure 4-5: Deafness problem with directional antennas [49]

by directionality. These are the deafness and directional hidden terminal problem. Deafness occurs when a node is trying to transmit to another node, whose beam is pointing in another direction. Figure 4-5 depicts a deafness scenario. In this figure, node C is trying to transmit to node A and node A cannot hear node C's attempts as node A is engaged in a conversation with node B. The deafness scenario leads to a decrease in the throughput, and in worst case, deadlocks can happen in some networks [49]. We discuss different kinds of deafness scenarios in the next chapter.

Figure 4-6 shows a simple scenario where the directional hidden terminal problem occurs. Nodes A and B and C and D are engaged in a conversation. Node C finishes its conversation with node D and then wants to communicate with node A. However node C's communication attempts collide with the data reception at A.

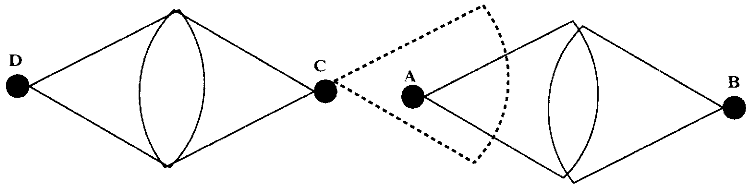


Figure 4-6: Directional hidden terminal problem

Some of the above mentioned issues with directional antennas can be alleviated by using an appropriate MAC protocol.

In heterogeneous networks that have omnidirectional as well as directional nodes, the difference in gain between the directional and omnidirectional modes creates new issues. One of these is the presence of unidirectional links. These links occur in the network because of the difference in the gain of an omnidirectional antenna and a directional antenna. We discuss the effect of these unidirectional links in Chapter 6. In the next chapter, we discuss MAC protocols for directional antennas.

Chapter 5

Medium Access Control Protocols

In this chapter we discuss medium access control (MAC) protocols for wireless networks that use directional antennas. We propose a new MAC protocol for directional antennas, request-to-pause-directional-MAC (RTP-DMAC).

5.1 Introduction

MAC protocols specify the rules for using a shared communication medium so that collision-free communication is realized. Bandwidth is scarce in wireless ad hoc networks, and hence every transmission should contribute to the overall throughput with as little control overhead as possible [59]. Thus, a MAC protocol is needed for efficient communication in wireless ad hoc networks.

Most of the work on MAC protocols for wireless networks assumes that omnidirectional antennas are used at the physical layer. In this chapter, we discuss MAC protocols for wireless networks that use smart (directional) antennas. The remainder of the chapter is organized as follows. One of the commonly used MAC protocols for wireless ad hoc networks is the 802.11b MAC protocol, which implicitly assumes that omnidirectional antennas are used at the physical layer. In Section 5.2, we discuss this protocol and in Section 5.3, we discuss modifications that have been proposed by researchers to this protocol for using directional antennas at the physical layer. These modifications improve the spatial reusability in networks. However with these modifications, the deafness problem and new variations of the hidden terminal problems arise. We discuss these problems in Section 5.4. In Section 5.5, we propose a new MAC protocol, RTP-DMAC for directional antennas, which reduces the impact of the deafness problem. We evaluate the performance of this MAC protocol in Section 5.6. In Section 5.7, we discuss previous work on MAC protocols for directional antennas. Finally, we draw relevant conclusions in Section 5.8.

5.2 802.11b DCF Protocol

The IEEE 802.11b standard specifies the MAC protocol for wireless local area networks (WLANs) using infrared (IR) waves or radio waves in the industrial, scientific, and medicine (ISM) band of the radio spectrum that operates between the 2.4GHz and 2.5GHz frequency range. Later extensions to the standard specify details of operation in other frequency ranges. More details about the standard can be found here [40].

The 802.11b MAC specifies two modes of operations, namely the independent or the ad hoc mode and the access point mode. Since we are concerned with ad hoc networks, we assume that nodes use the ad hoc mode, which is also known as the distributed coordination function (DCF). The DCF has three main components: carrier sense multiple access/collision avoidance (CSMA/CA), truncated binary exponential backoff mechanism, and the optional handshake mechanism. CSMA mechanism ensures that nodes sense the medium before transmitting any unicast data and the CA part ensures that all unicast data is acknowledged. When the acknowledgment is lost or doesn't arrive, nodes assume that data is lost and retransmit the data.

The DCF has a truncated binary exponential backoff mechanism that enables the nodes to determine a proper scheduling rate and have a fair chance to access the medium. A node when it wishes to transmit, senses (physical carrier sensing) the medium for a minimum amount of time called the distributed inter frame spacing (DIFS). If the medium is sensed to be idle for the entire DIFS period, the node waits for a random number of time slots [1]. If the medium is sensed to be busy, the node waits for the medium to be idle before starting its random wait period. If the node has already started its wait period, and it senses a transmission, it freezes its backoff counter. The backoff counter is started only after the medium is idle for the DIFS period. The node chooses the random number between 0 and its current congestion window (CW) plus 1 (i.e., between 0 and CW+1). The value of CW is chosen from a set of specified values, and these values are in the range CW_{min} to CW_{max}. CW is initially equal to CW_{min} and its value is doubled after every unsuccessful transmission ($CW_{new} + 1 = 2 * (CW_{old} + 1)$). The value of CW can go up to CW_{max} and if there is a further retransmission, the packet is dropped. After every successful transmission, the value of CW becomes CW_{min}.

We now discuss the handshake mechanism in detail.

Handshake mechanism

The DCF specifies an optional handshake mechanism, which is used for reserving the medium so as to reduce hidden terminals around the transmitter and the receiver nodes [59]. Hidden terminals cause collisions in the network and lead to wastage of the throughput. A collision due to a hidden terminal occurs when two different nodes, which are out of communication range, communicate with a common receiving node (Figure 5-1). Because of the collision, the receiving node usually cannot decode either of the messages and both the messages are lost.

The handshake mechanism (Figure 5-2) is also termed as the virtual carrier sensing mechanism as nodes use the handshake messages to gets information about the state (idle or busy) of the medium. A node S that wishes to communicate with another node R, sends a request to send message (RTS) message to R. Node R, if it is free sends a clear to send (CTS) message to node S. Node S then sends the data and once the data is successfully received at R, R sends back an ACK message acknowledging the receipt of the data. Nodes that overhear the RTS or the CTS message update their network allocation vectors (NAVs) with the total duration of the transaction, which is

[1] Each slot in 802.11b is $20\mu s$

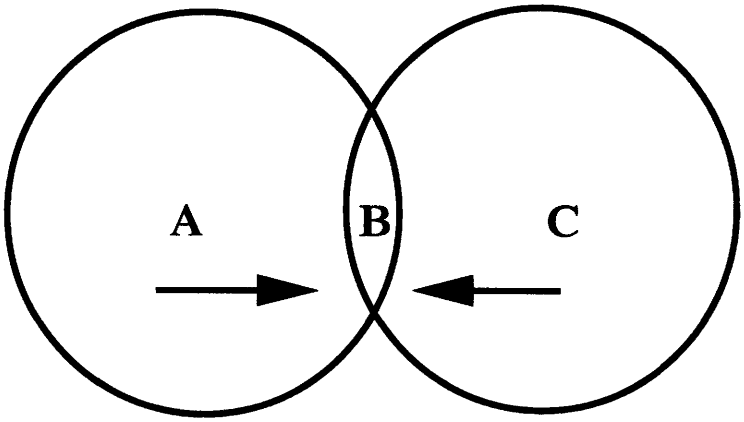


Figure 5-1: Hidden terminal problem

specified in these messages. The NAV provides the virtual carrier sensing mechanism indicating if the medium is busy or idle and if it is busy, when it is expected to be idle. In the above described handshake mechanism, a node is said to be "free" when it is not communicating with other nodes or its NAV indicates that the medium is idle [59]. The handshake mechanism solves the hidden terminal problem at an additional overhead of the RTS and CTS packets.

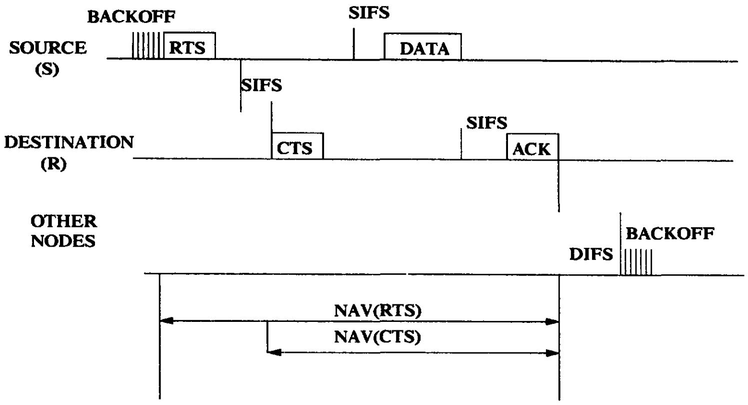


Figure 5-2: Handshake mechanism in 802.11b DCF protocol [59]

The DCF protocol has been designed assuming that omnidirectional antennas are used at the physical layer. In order to leverage the advantage of using directional antennas at the physical layer, the 802.11b MAC protocol needs some modifications. We now discuss these modifications.

5.3 Modifications to 802.11b DCF Protocol

In this section we discuss directional-NAV (DNAV) and directional handshake [86, 17] mechanisms that have been proposed to 802.11b DCF protocol for directional antennas. These mechanisms improves the spatial reusability in networks with directional antennas.

5.3.1 DNAV

The NAV component of the 802.11b DCF protocol provides the virtual carrier sensing mechanism, which reduces the occurrence of hidden terminal problems in the network. When a node receives a RTS/CTS message, the node blocks its transmissions in all directions as any transmission can cause a collision with the on-going communication. With DNAV, nodes do not transmit in the direction in which they have received the RTS/CTS message until the duration specified in the RTS/CTS message. However, nodes are free to transmit in any direction that is sufficiently different from the direction in which they heard the RTS/CTS message. The sufficiency is determined from the beam-width of the directional antennas.

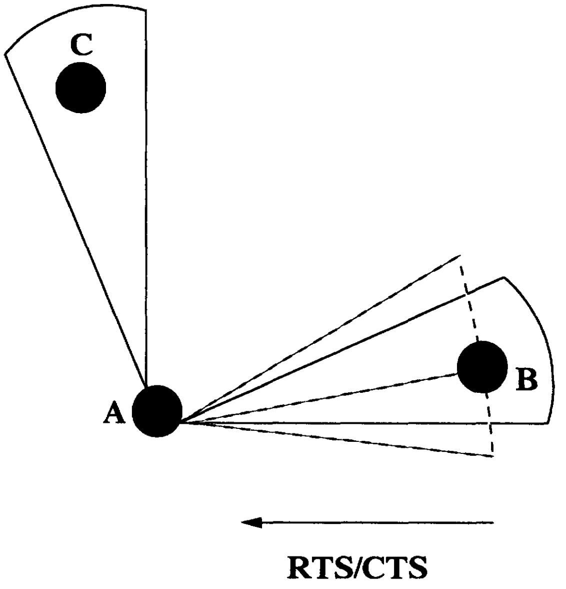


Figure 5-3: DNAV improves spatial reusability [17, 86]

Figure 5-3 explains the usage of DNAV. Node A receives an RTS/CTS from node

B and hence its DNAV in the direction of B is set. The dotted lines show the angle for which the DNAV is set. Since the DNAV is set in the direction of B, node A can communicate with node C. DNAV improves spatial reusability as now node A is able to communicate with node C. Ideally, the angle for which the DNAV is set and the beam-width should be the same, i.e. in the figure the dotted lines and the solid line should overlap [17, 15].

5.3.2 Directional Handshake scheme

The DCF employs the RTS/CTS mechanism to reduce the probability of hidden terminals in the network. Instead of transmitting RTS/CTS using the omnidirectional mode, a node that uses directional antennas can transmit these messages in the directional mode. The directional transmission/reception of these messages improves the spatial reusability as most of the radiation is along the line joining the transmitter and the receiver. In order to transmit RTS/CTS directionally, nodes should know the relative locations of the transmitters/recipients. Existing MAC protocols assume that this information is available via using GPS or via an elaborate neighbor discovery process [73]. Some MAC protocols [86] assume that when a node receives a message, it is possible to determine the angle of arrival (AOA) information. By caching this information, nodes can determine the direction information of its neighbors.

MAC protocols for directional antennas transmit data and ACK directionally. Thus when they use directional handshake mechanism, all transmissions are directional. Further is is possible to employ a directional carrier sensing which further enhances the spatial reusability.

However using directional RTS/CTS causes deafness and directional hidden terminal problems, which are discussed in the next section.

5.4 Issues with directional antennas

In this section, we discuss deafness, hidden terminal, and backoff related issues with directional antennas.

5.4.1 Deafness

Deafness refers to the situation where a sender node is trying to communicate with a receiver node and the receiver node cannot hear the sender node's attempts as the receiver node's beam is pointing in a different direction. Fig. 5-4 depicts a deafness scenario, in which node C is trying to transmit to node A, and node A cannot hear node C's attempts as node A is engaged in a conversation with node B. In this scenario when C tries to communicate with A, node C waits for a CTS from A. After certain time, node C times out and enters the backoff phase by doubling its CW. Node C now likely has to wait for a longer time than it waited previously to access the medium and try communicating with A again. Further, node A is not aware of C's communication attempts and A also has a higher chance of accessing the medium before C as A's CW is lower than that of C's CW. This worsens the situation for node C when node A again is engaged in communication with node B. Severe forms of deafness lead to wasted bandwidth and unnecessary backoff. The backoff is unnecessary because there is no real congestion at node A. Some extreme forms of deafness lead to deadlock, and in chain topologies cascading effects of deafness are seen [17].

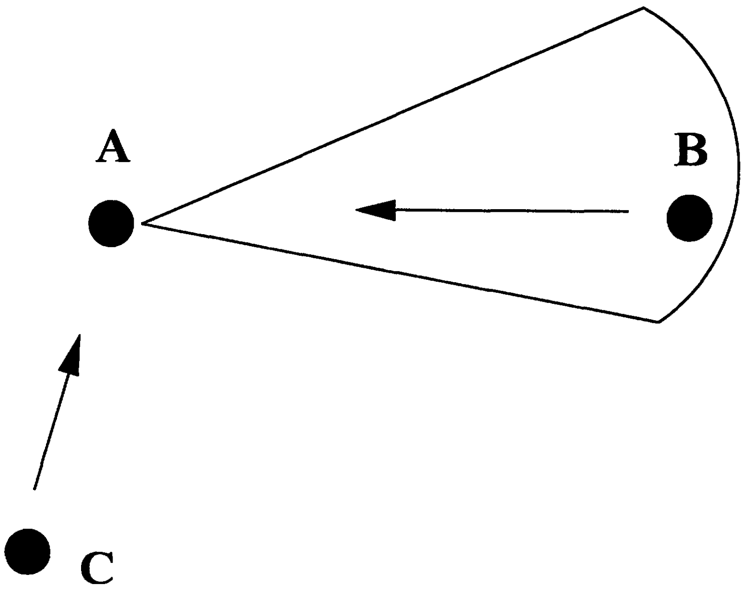


Figure 5-4: Deafness problem with directional antennas [49]

Gossain et al. [33] identify different types of deafness scenarios. These are:

- “Destination engaged in communication”. This type of deafness is similar to the scenario depicted in Fig. 5-4. This occurs usually in MAC protocols that use directional handshake schemes. This type of deafness can be avoided using an omnidirectional handshake scheme, but such a scheme reduces the spatial reusability to a great extent [33].

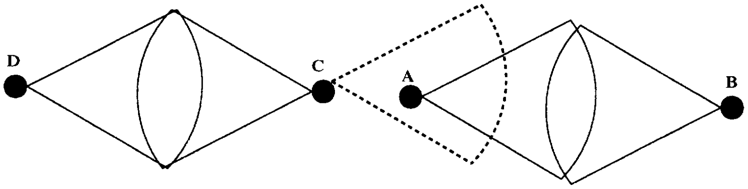


Figure 5-5: Deafness due to unheard RTS/CTS [33]

- “Unheard RTS/CTS”. Figure 5-5 depicts this type of deafness. Here node C and node D and node A and node B are having a conversation. Once node C finishes the conversation with node D, it wants to communicate with node A, and sends a directional RTS towards node A. Since node A is in conversation with node B, the RTS from C either collides with node A’s data (if A is the receiver, and hence will be a hidden terminal problem) or node A cannot respond (if it is the transmitter, because of the half-duplex nature of wireless communications) with a CTS. This type of deafness occurs with all types of MAC protocols that use directional handshake schemes [33]. Subramanian and Das [85] propose a solution to this problem using a window-based mechanism. This mechanism is similar to the solution proposed by Acharya et al. [1] for the exposed terminal problem.

- “Precautionary deafness at the receiver”. This type of deafness occurs when a receiving node does not respond with a CTS because sending a CTS would cause a collision to an ongoing communication. In Figure 5-6, node A and node C are communicating. They use their directional beams for sending the RTS (sent through node A’s beam 1) and CTS (sent through node C’s beam 3). Node D hears node A’s RTS and node B hears node C’s CTS, and hence node D sets its DNAV for its beam 3. Similarly node B sets its DNAV for its beam

2. Node D tries to communicate with node B and does not get any response because node B has set its DNAV for beam 2, and it can only respond to node D's RTS using this beam [33].

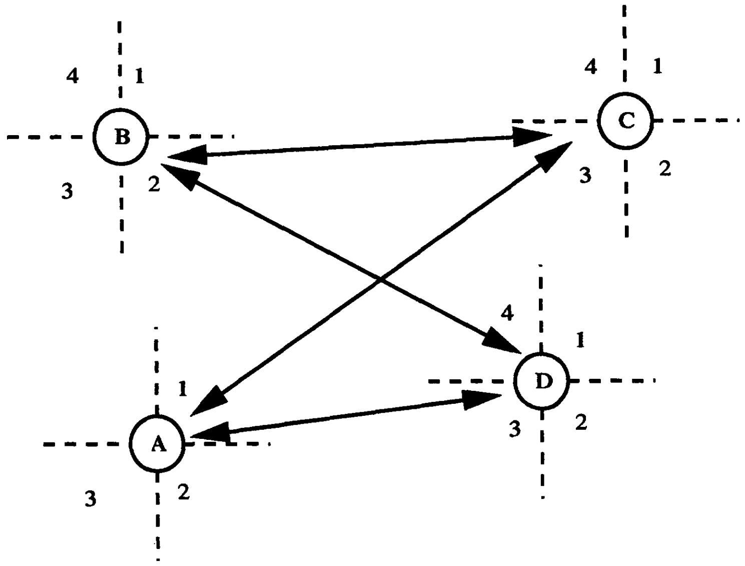


Figure 5-6: Precautionary deafness at the receiving node [33]

This type of deafness also occurs with omnidirectional antennas and is known as the blocking problem. The blocking problem can lead to false blocking scenario, which leads to reduction in throughput. Details of the false blocking problem and a solution to this problem are found in [75].

- "Persistent hearing of data". This occurs when a node is engaged in receiving data that is not intended for it. This can cause deafness as there might be other nodes trying to communicate with this node [33]. This problem is also termed as capture and a capture aware routing protocol was proposed by Choudhury [15]. This routing protocol uses multiple-beam directional antennas to mitigate the capture problem.

5.4.2 Hidden terminal problem

In the above deafness scenarios, it can happen that the message from the sender node can collide with the message reception (e.g. in the case of "Destination engaged in communication" [33]) and in such a case, the problem is a hidden terminal problem.

5.4.3 Problem with backoff scheme

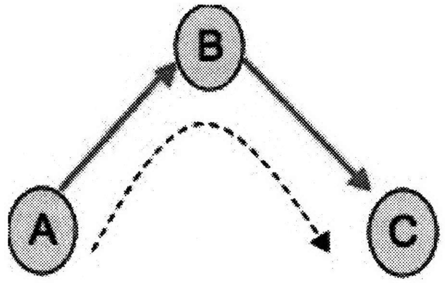


Figure 5-7: Chain topology to study the effect of deafness

The backoff scheme employed by 802.11b aggravates the deafness problem [49]. Consider a simple scenario, shown in Figure 5-7, where node A is sending data to node C via node B. Assume that nodes A, B, and C use directional antennas and use directional handshake scheme. When node A sends the packet to node B, now node A and node B have a packet to send (node A to node B and node B to node C) and both of them compete for the medium using the random backoff value. In this case both A and B choose the backoff values from [0, $cw_{min}+1$]. Consider the scenario when node B gets access to the medium before node A. In such a case, node A cannot sense node B's transmissions (because of directional transmissions) and sends a RTS message to node B. Due to the half-duplex nature of nodes in wireless communication, node B cannot hear node A's RTS message as it is transmitting its RTS message. Further nodes A and B use directional physical carrier sensing, which does not allow either of them to sense the other node's transmissions. Node A now times out and increases its congestion window and is likely to choose a higher backoff value for its next RTS transmission.

Table 5.1 shows the time taken for transmitting an RTS and a CTS message (including the short inter frame spacing), average time spent in the backoff and the DIFS, and the time taken for transmitting a message of size 1500 Bytes. The average time spent in the backoff is calculated as $\frac{CW_{min}}{2}$ times the slot duration (equal to 15*20μs for 802.11b). From this table, we can infer that by the time the RTS/CTS handshake is finished, nodes on an average would have increased their CW at least once (as average time spent in the backoff +DIFS is less than the time for RTS/CTS handshake). We also see that by the time the data transmission (between nodes B and C) is finished, node A would have backed off multiple times and in worst case, would even have dropped a packet.

Rate	**RTS + CTS**	**Backoff + DIFS**	**Data (1500B)**
1 Mbps	672 μs	350 μs	12,192 μs
11 Mbps	410 μs	350 μs	1324 μs

Table 5.1: Transmission times for different messages

To summarize the above scenarios, node A becomes deaf even before node B finishes the RTS/CTS handshake, i.e. even before the data transmission starts. Thus to reduce the impact of deafness, nodes should inform their neighbors as soon as their handshake is finished. Further even if the nodes inform the neighbors of their impending transmissions, there is a good chance that nodes would have increased their backoff window at least once. Thus, to alleviate the impact of deafness, nodes that have suffered from deafness should reset their backoff window, CW to CW_{min}. We use these observations to design the RTP-DMAC protocol, which we discuss in the following section.

5.5 RTP-DMAC protocol for directional antennas

RTP-DMAC is a cross-layer protocol that uses neighbor information and the incoming flow information from the routing layer. It also incorporates a backoff reset scheme that reduces the aggravation of nodes due to deafness. Existing solutions to solve the deafness problem either use a MAC layer approach or just use the neighbor location information from the routing layer. We describe the motivating reasons for developing a cross layer approach and then describe the protocol.

5.5.1 Motivation

Existing protocols for directional antennas consider the problem of deafness at the MAC layer. In the previous section, we saw that the underlying reason for the cause of deafness is that nodes fail to inform neighbors from which they expect an inflow. In RTP-DMAC, a node informs about an impending communication to only those neighbors from which it expects an inflow. We illustrate this with an example.

Consider the previous example (Figure 5-7), when node B is sending data to node C, node A does not know about the transmission (we are using directional handshake messages). So when node B is ready to transmit data to node C, it should inform node A about its impending data transmission. This will allow node A to set its DNAV.

The RTP-DMAC protocol is similar to a multiple-RTS-CTS MAC protocol [33], where multiple RTS/CTS messages are sent by nodes so that the deafness issue is avoided. One of the disadvantages of the multiple RTS-CTS method is the increase in the number of RTS/CTS messages. In many cases, it happens that all the RTS/CTS messages are not needed. Consider the scenario shown in Figure 5-8, which shows what nodes are informed with the RTS/CTS messages. It happens that all the nodes need not receive the RTS/CTS messages as some of them do not have any flow towards the RTS/CTS transmitting nodes.

5.5.2 Protocol Details

The RTP-DMAC protocol is an extension to the DMAC [17, 86] protocol. The DMAC protocol is an extension to the DCF, with the DNAV and directional handshake modifications. In RTP-DMAC, nodes use directional handshake, directional data transfer

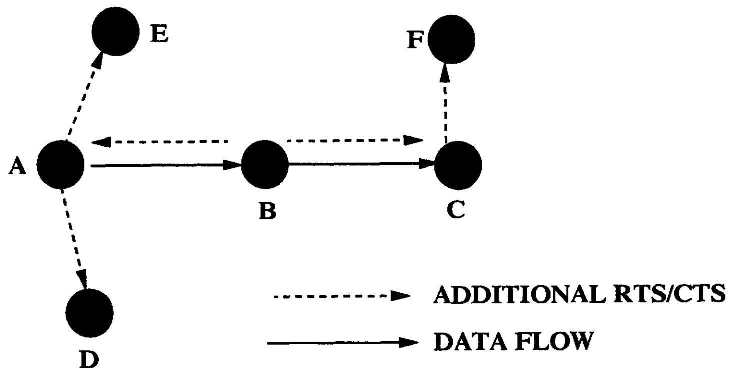


Figure 5-8: Multiple-RTS-CTS-DMAC: informing the neighbors

and directional acknowledgment. Nodes using RTP-DMAC perform the physical carrier sensing in an omnidirectional manner. A detailed discussion on the utility of omnidirectional carrier sensing over directional carrier sensing can be found in [15, 54, 18].

We define a new message frame called the request-to-pause (RTP). Nodes send RTP frames to nodes from which they expect an inflow. Nodes which hear the RTP messages set their DNAVs accordingly. Nodes that have a flow towards the node which sent the RTP frame and if they have suffered from deafness, reset their backoff window to CW_{min} so that the aggravation due to deafness is minimized. The RTP frame is sent before the handshake or after the handshake and before the data transfer. Informing the upstream neighbors before the handshake can be counter productive as the receiving node may be busy and may not respond with a CTS message. In this case, nodes which received the RTP frame would have set their DNAVs and are waiting unnecessarily. Hence, the RTP frame is only sent after a successful handshake. Figure 5-9 shows the message sequence in the RTP-DMAC protocol.

The frame format of the RTP frame is similar to that of the RTS frame. It has the same fields as that of an RTS message. In RTP-DMAC, the duration field in RTS/CTS frames include time for transmitting the RTP frames as well as data and the acknowledgment frames. The RTP frame also has a duration field, whose value includes the time taken for transmitting data and the acknowledgment frames.

We implemented the RTP-DMAC in the Qualnet simulator. We evaluate the

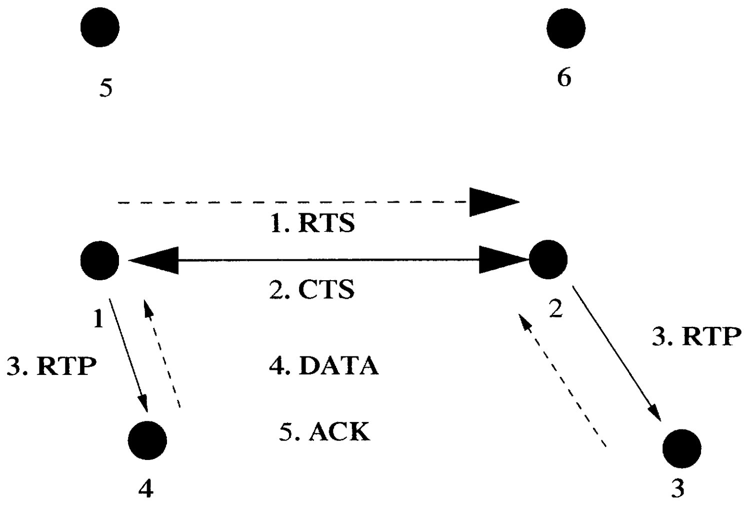


Figure 5-9: RTP-DMAC: Message sequence

performance of the RTP-DMAC protocol in the following section.

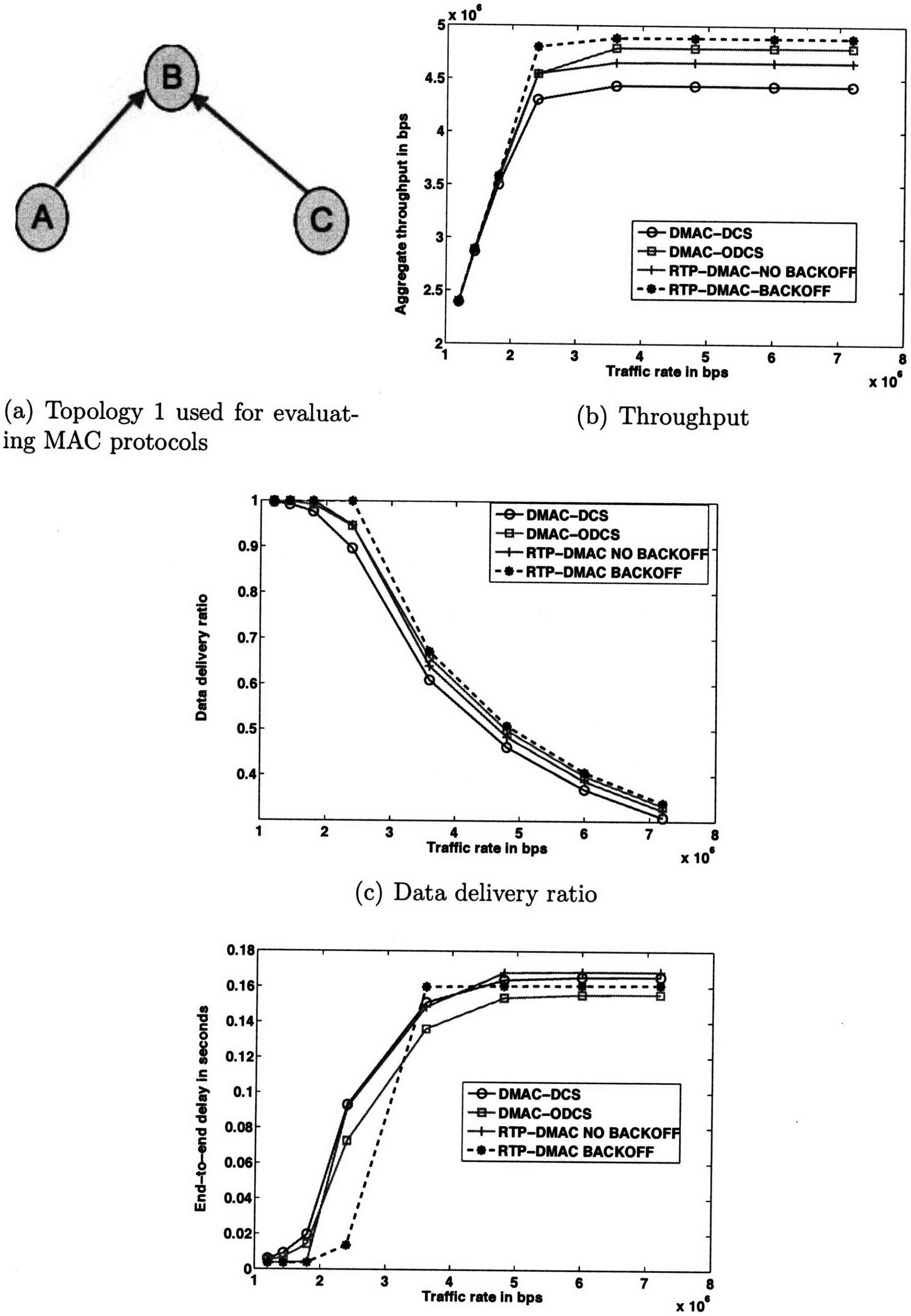
5.6 Evaluations

In this section, we evaluate the performance of different MAC protocols in three different topologies. These topologies are commonly used in evaluating the deafness scenarios in directional antennas [18, 54]. We use Qualnet (ver 3.9) [71] simulator for our simulations. Nodes use 802.11b radios with a fixed transmission rate of 11Mbps. The packet size is 1500 B and we use UDP flows. The points on the following graphs represent an average value of 20 runs. In the following three topologies, the adjacent nodes are separated by a distance of 250 m (175 m horizontally and 175 m vertically). The communication range is 290 m.

We evaluate the following MAC protocols: DMAC with directional carrier sensing (DMAC-DCS), DMAC with omnidirectional carrier sensing (DMAC-ODCS), RTP-DMAC (with and with out backoff reset mechanism). We evaluate RTP-DMAC with and with out the backoff reset mechanism so as to study how the backoff reset mechanism reduces deafness aggravation. In DMAC, nodes transmit the RTS, CTS, data, and the ACK frames directionally. For the simulations, we assume that nodes know their neighbor locations and hence, they know the beam by which they can reach them. We use throughput (from the source node to the destination node), data delivery ratio (defined as the ratio of the number of data packets received by the destination to the number of data packets sent by the source node), and end-to-end delay (defined as the average delay of the data packets that have reached the destination node) as the performance metrics for evaluating the MAC protocols. We use DMAC-DCS as the base case for comparing the performance of the MAC protocols.

Topology 1 (Figure 5-10(a)) has 3 nodes, where two nodes communicate with a single node. When node B is communicating with node A (node C), node C (node A) suffers deafness. Figures 5-10(b), 5-10(c), and 5-10(d) show the throughput, data delivery ratio, and the end-to-end delay respectively for the 4 MAC protocols. We see that RTP-DMAC improves throughput up to 11% over the base case and DMAC-ODCS improves throughput up to 8%. We see that just sending the RTP frame improves the throughput up to 6% and enabling the backoff reset mechanism further improves the throughput up to 6%. RTP-DMAC also improves the data delivery ratio. Transmitting the RTP frame incurs an additional overhead and this is seen in the end-to-end delay. RTP-DMAC without the backoff reset mechanism incurs higher delay than DMAC-ODCS. However, by enabling the backoff reset mechanism reduces the end-to-end delay. For this scenario, RTP-DMAC (with the backoff reset mechanism) has a better performance than the other MAC protocols.

In the second topology (a chain topology, Figure 5-11(a)) there are 4 nodes; node A is the source node and node D is the destination node. Node A sends data to D via nodes B and C. We use this topology to study the cascading effect of deafness. When node C is communicating with node D, nodes A and nodes B suffer deafness (cascading effect). Further, topologies of this kind (multi-hop) are commonly used in ad hoc networks. Figures 5-11(b), 5-11(c), and 5-11(d)show the throughput, data delivery ratio, and the end-to-end delay respectively for the four MAC protocols. We see that RTP-DMAC improves throughput up to 35% over the base case and DMAC-ODCS improves throughput up to 25%. We see that just sending the RTP frame improves the throughput up to 27% and enabling the backoff reset mechanism further



(a) Topology 1 used for evaluating MAC protocols

(b) Throughput

(c) Data delivery ratio

(d) End-to-end delay in seconds

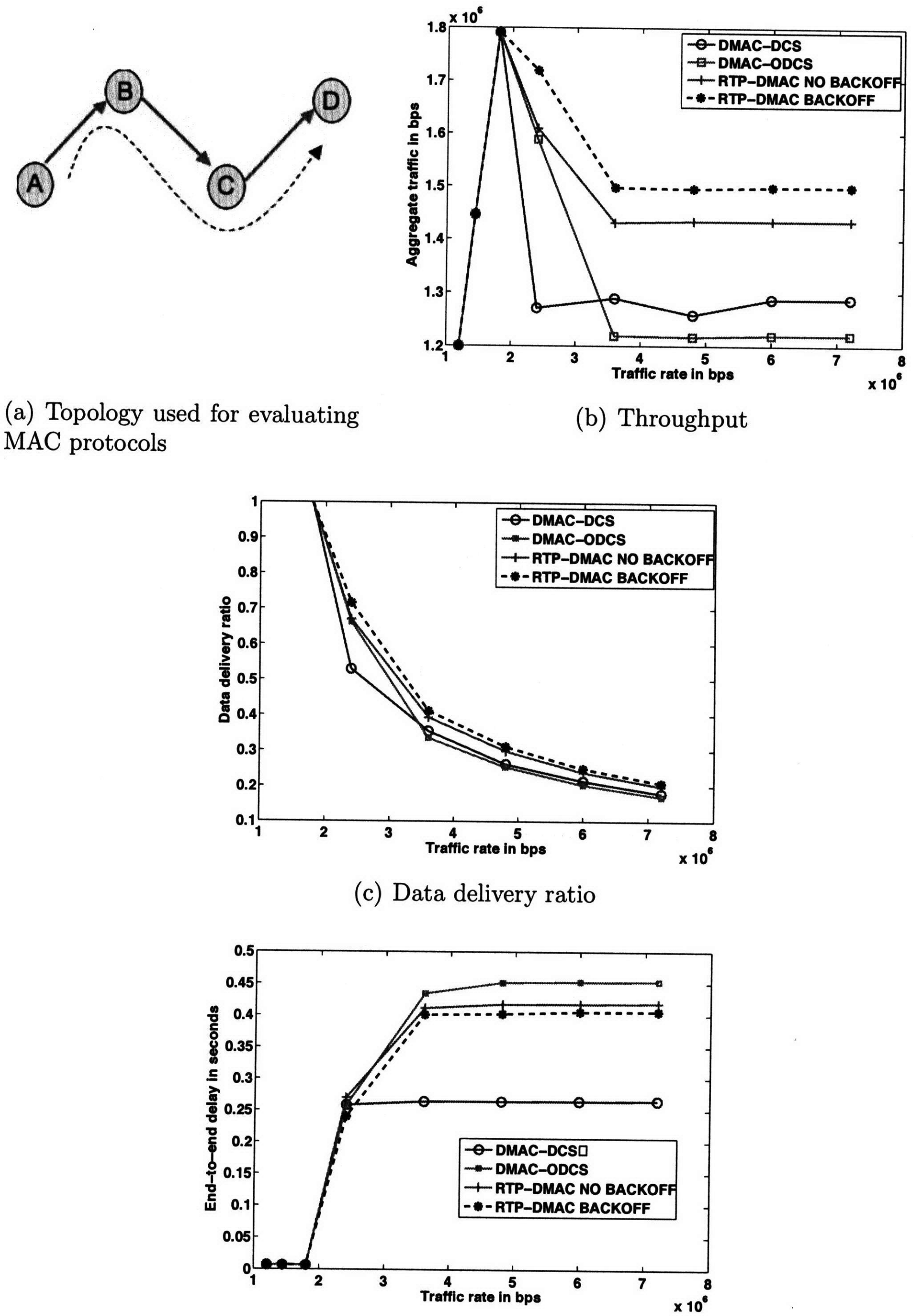
Figure 5-10: Performance of different MAC protocols in topology 1

improves the throughput up to 7%. RTP-DMAC also improves the data delivery ratio. The additional overhead incurred by transmitting the RTP frame is seen in the end-to-end delay. As in the previous case (i.e. topology 1), RTP-DMAC without the backoff reset mechanism incurs higher delay than DMAC-ODCS. However, enabling the backoff reset mechanism reduces the end-to-end delay. Again for this scenario, RTP-DMAC (with the backoff reset mechanism) has a better performance than the other MAC protocols.

In the third topology (Figure 5-12(a)), there are 3 nodes and the data flow is between nodes A and nodes C (2-hop flow). Node A suffers deafness, when node B is communicating with node C. Figures 5-12(b), 5-12(c), and 5-12(d) show the throughput, data delivery ratio, and the end-to-end delay respectively for the 4 MAC protocols. We see that RTP-DMAC improves throughput up to 22% over the base case and DMAC-ODCS improves throughput up to 8%. We see that just sending the RTP frame improves the throughput up to 17% and enabling the backoff reset mechanism further improves the throughput up to 5%. RTP-DMAC also improves the data delivery ratio. We observe a similar performance of the MAC protocols for the data-delivery ratio and the end-to-end delay metrics as in the previous topologies.

We now evaluate the performance of these MAC protocols in a random topology. The random topology consists of 30 nodes in a 1000m x 1000m grid. There are 5 flows in the topology. The routes are assigned statically. Figure 5-13(a), 5-13(b), and 5-13(c) show the throughput, data delivery ratio, and the end-to-end delay respectively for the 4 MAC protocols. We see that RTP-DMAC improves throughput up to 28% over the base case and DMAC-ODCS improves throughput up to 18%. We see that just sending the RTP frame improves the throughput up to 23% and enabling the backoff reset mechanism further improves the throughput up to 5%. RTP-DMAC also improves the data delivery ratio and the end-to-delay. The performance of the 4 MAC protocols for these metrics is similar to their performance for the throughput metric.

We see that RTP-DMAC (with the backoff reset mechanism) has a better performance than the other MAC protocols. We summarize the evaluations in the following.



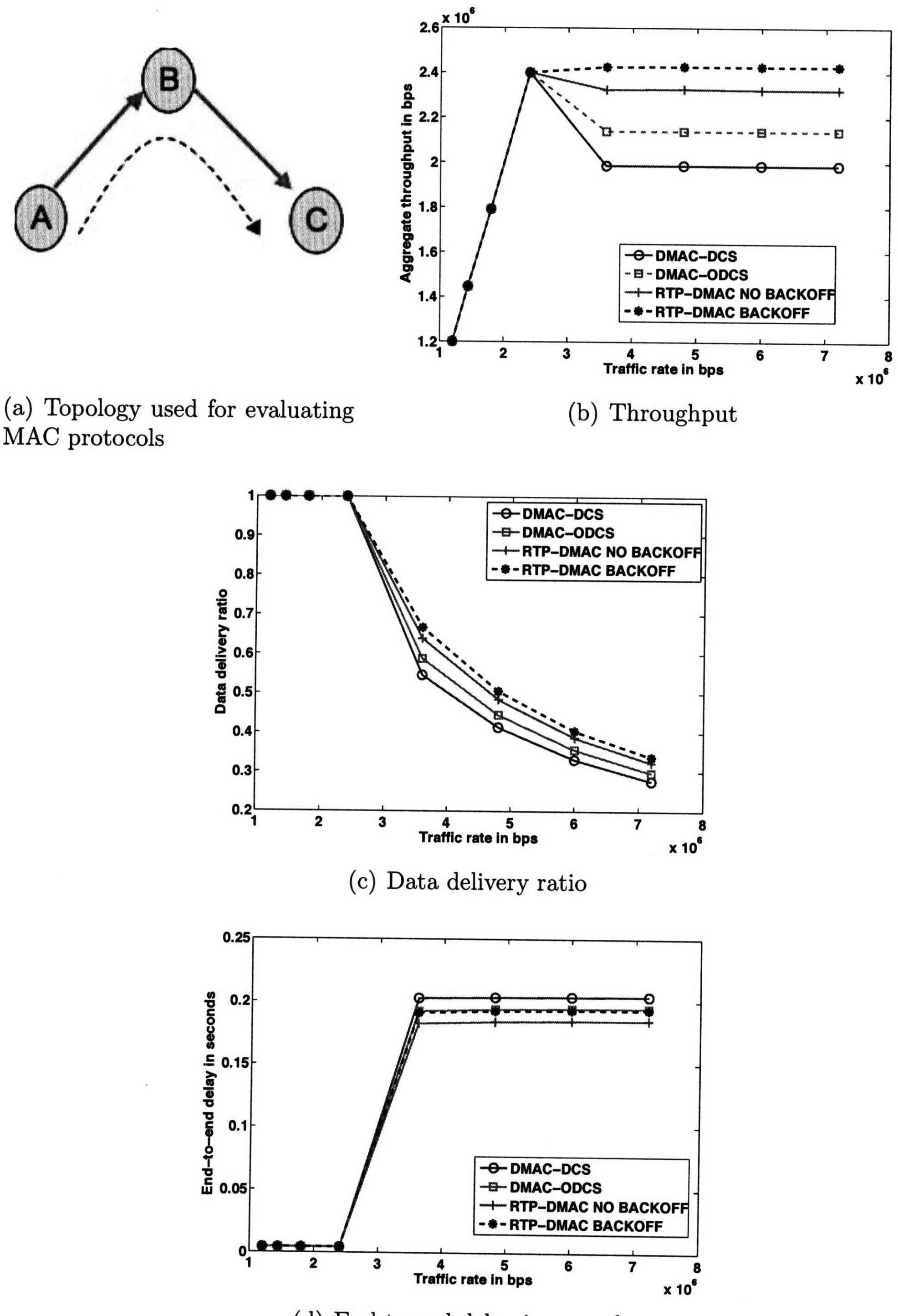
(a) Topology used for evaluating MAC protocols

(b) Throughput

(c) Data delivery ratio

(d) End-to-end delay in seconds

Figure 5-11: Performance of different MAC protocols in topology 2



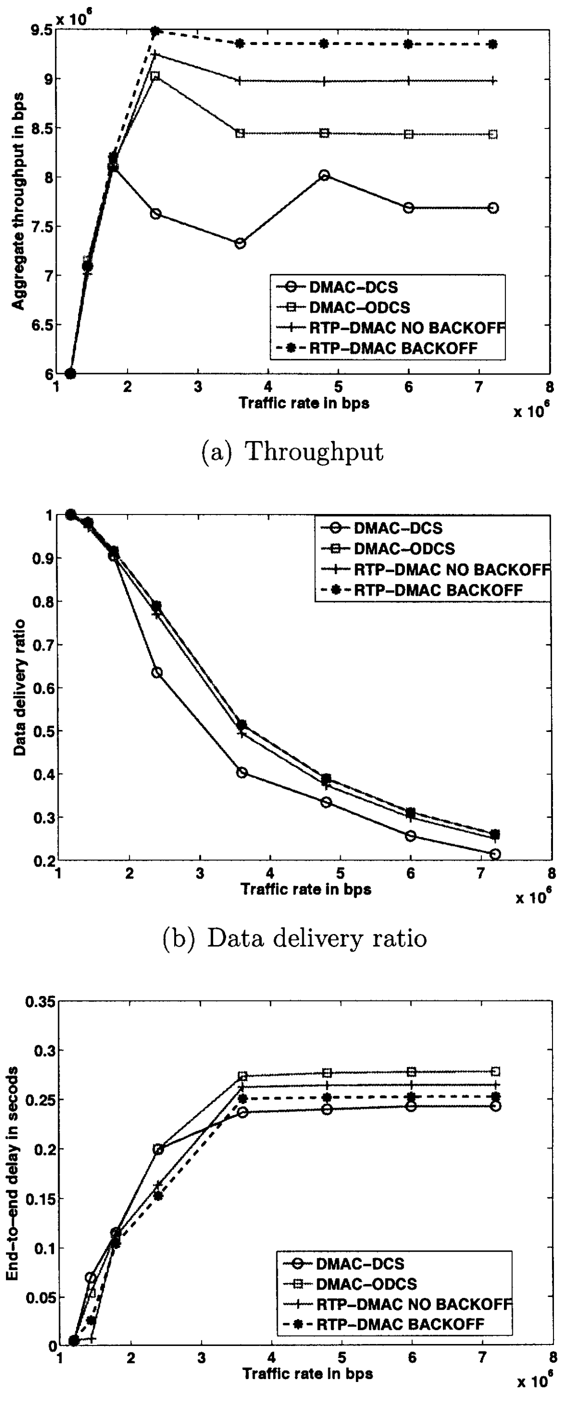
(a) Topology used for evaluating MAC protocols

(b) Throughput

(c) Data delivery ratio

(d) End-to-end delay in seconds

Figure 5-12: Performance of different MAC protocols in topology 3



(a) Throughput

(b) Data delivery ratio

(c) End-to-end delay in seconds

Figure 5-13: Performance of different MAC protocols in a Random Topology

5.6.1 Summary of evaluations

To summarize the results of evaluation, we find that RTP-DMAC with the backoff reset mechanism has a better performance (in terms of throughput) compared to the other MAC protocols. Since these topologies have been specifically designed for studying the effect of deafness and since RTP-DMAC has a better performance in these topologies, we expect that it will have a better performance in a random topology too. The results of evaluation in the random topology chosen for simulation confirm the same.

Overall (in the three topologies), RTP-DMAC with the backoff reset mechanism improves the throughput up to 35% and just by sending the RTP frame (i.e. RTP-DMAC without the backoff reset mechanism), we observe an improvement in the throughput up to 27%. We also observe that omnidirectional carrier sensing improves the throughput up to 25%. The last result agrees with the previous results in [18, 54].

In the random topology, performance of the RTP-DMAC protocol is better than the others in all the three evaluation metrics. There is an increase in the throughput up to 28% with RTP-DMAC with the backoff reset mechanism.

From the above results, we conclude that RTP-DMAC is a better MAC protocol than DMAC, omnidirectional carrier sensing is better than directional carrier sensing for reducing the impact of deafness, and the backoff reset mechanism improves the performance of RTP-DMAC in a significant manner. Having evaluated the performance of RTP-DMAC, we review some of the existing work done on MAC protocols for directional antennas in the next section.

5.7 Previous Work

In this section, we discuss 802.11b-based protocols for directional antennas. We classify these MAC protocols into two categories, MAC protocols that have been proposed for using directional antennas and MAC protocols that are designed to solve deafness and hidden terminal problems with directional antennas.

5.7.1 MAC protocols for directional antennas

Choudhury et al. [17] describe a protocol (directional-MAC, DMAC) that uses directional NAV (DNAV) for virtual carrier sensing. Their protocol is an adaptation of the 802.11b protocol for directional antennas. In their protocol, they use a directional CTS/RTS handshake for reserving the channel. They discuss the deafness and hidden terminal problem associated with directional antennas. These problems are further studied by Li et al. [49, 50], Safwat [51], and Gossain et al. [33]. Takai et al. [86] also propose a similar MAC protocol to DMAC that has the DNAV and directional handshake mechanism. However this MAC protocol uses an omnidirectional RTS when the direction of the recipient is unknown, and further they assume that at the physical layer the nodes have the capability to determine the angle of arrival (AOA).

Choudhury et al. [19] extend the DMAC protocol to the Multi-hop RTS MAC protocol (MMAC protocol). This MAC protocol exploits the extended communication range that is possible with directional antennas. The basic principle of this protocol is to use multihop for RTS transmission and use a single hop for the CTS and data transfer.

Takai et al. [87] present an adaptive range control algorithm (ARC) that is implemented at multiple layers of the communication stack. ARC uses directional reception rather than directional transmission in order to reduce the interference.

Kobyashi and Nakagawa [45] suggest using the 802.11b DCF protocol on a per antenna basis. Their system consists of sectored antennas and for each antenna, the 802.11b DCF protocol is used.

Takata et al. [88] propose a MAC protocol that reduces the location information staleness in mobile ad hoc networks. Their protocol called smart antenna based wider-range access MAC protocol (SWAMP) uses omnidirectional RTS/CTS and directional data transmission/ACK. They also investigate the optimization of parameters like beam-width, retry limit, TTL, etc. for reducing the location information staleness.

Nasipuri et al. [61] develop a power control scheme for the MAC layer. The power control scheme is used to maintain a minimum signal-to-interference-plus-noise ratio

(SINR) at the receiver. In this scheme, the RTS/CTS packets are sent with full power and are utilized to determine the minimum SINR for transmitting the data packets. The data packets are thus transmitted with a power so that the minimum SINR is maintained at the receiver.

We now discuss MAC protocols that are designed for solving deafness and hidden terminal problems.

5.7.2 MAC protocols that solve deafness and hidden terminal problems

As mentioned earlier, Li et al. [49, 50], Safwat [51], and Gossain [33] discuss various kinds of deafness problems. We discussed these different types of deafness scenarios in Section 5.4. We now discuss MAC protocols that have been proposed to solve the deafness and hidden terminal problems.

Most of the existing solutions for solving the deafness problem involve sending multiple RTS and multiple CTS packets. The idea behind sending multiple RTS/CTS packets is to avoid the deafness problems around the transmitter and the receiver nodes. Nodes that hear these messages update their DNAV and avoid transmitting in direction of the received RTS/CTS message. ElBatt et al. [25] evaluate the tradeoffs between omnidirectional and directional reservation schemes. They propose a handshake scheme in which the RTS/CTS messages are sent omnidirectionally with the beam indices indicated in the RTS/CTS messages. Neighbor nodes that hear the RTS/CTS messages avoid transmitting in the directions indicated by the beam indices in the RTS/CTS messages. Korakis et al. [46] propose a MAC protocol in which multiple RTS/CTS messages are transmitted to inform the neighbors about the impending data transmission. Gossain et al. [34] propose a multiple RTS/CTS-based MAC protocol to solve the problems of deafness and hidden terminal problems. Instead of transmitting the RTS/CTS messages in all directions, these messages are only transmitted in diametrically opposite directions so as to minimize the delay occurred in transmitting these messages. They use a deafness table in addition to

DNAV so as to differentiate between a collision and a deafness scenario.

Transmitting multiple RTS/CTS schemes solves the deafness problem to some extent. However as mentioned in Section 5.4.3, 802.11b's backoff scheme aggravates the deafness problem, which the above multiple RTS/CTS schemes do not consider.

Choudhury and Vaidya [18] propose a tone-based MAC (ToneDMAC) protocol for solving the deafness problem. In this protocol, the channel is split into two sub-channels, one for data transmission and the other for tone transmission. Once the data transmission is finished and the acknowledgment has been received, nodes transmit a tone indicating that a data transfer has just been finished. Nodes in the near vicinity of the transmitting/receiving nodes hear this transmission and will reset their backoff window to CW_{min} if they are affected by deafness. The tone frequencies are based on the node identifiers. This MAC protocol doesn't avoid deafness but only alleviates deafness of nodes. A similar tone-based MAC protocol, dual-tone DMAC to avoid deafness is proposed by Koo and Jwa [44]. In this protocol, nodes transmit a start/stop tones to indicate the start/stop of the transmission. The idea of transmitting a start tone is to avoid retransmissions to the transmitting node, so that collisions are avoided. The dual-tone DMAC has a better performance than the ToneDMAC as it prevents deafness.

Takata et al. [54] propose a novel MAC protocol in which they use a combination of receiver-initiated and sender-initiated data transfer to solve the deafness problem with directional antennas. The receiver-initiated mode is used when nodes experience deafness and the default mode is the sender-initiated mode (which is the same in 802.11 DCF protocol). They also define a ready to receive (RTR) message format to poll nodes that could have potentially been affected by deafness. They observe that RI-DMAC outperforms ToneDMAC and DMAC protocols.

Subramanian and Das [85] have proposed a MAC protocol, for solving the deafness and the directional hidden terminal problem. They assume that the omnidirectional transmission range is the same as the directional transmission range. They use omnidirectional RTS/CTS transmission to inform the neighbors about the impending data transmission/reception. They use beam indices (similar to Elbatt et al. [25]) in these messages to indicate the neighbors of the impending transmission. They extend the scheme proposed by Acharya et al. [1] and others to solve a variant of the hidden terminal problem. In this scheme, nodes wait for a short interval after they transmit the RTS so that any nearby node contemplating data transfer can start transmitting its RTS message. This way multiple transmissions can be scheduled and the throughput can be enhanced. They find that their MAC protocol outperforms the DMAC protocol.

In 802.11 MAC protocol, nodes perform physical carrier sensing. Nodes sample the channel and estimate the energy in the medium and compare it with a threshold to know if the channel is busy or idle. This is known as clear-channel-assessment (CCA). Li and Yang [50] propose a CCA threshold-based method for completely eliminating deafness without making any significant changes to the 802.11 MAC protocol. They use a channel scattering model to make the simulations more realistic. Simulations in existing research do not consider channel scattering models.

5.8 Conclusions

In this chapter, we studied MAC protocols for directional antennas. We briefly discussed the 802.11b MAC protocol and the modifications to it for using directional antennas at the physical layer. These modifications include the DNAV and directional handshake mechanism [17, 86]. We then discussed the deafness issue that occurs in networks with directional antennas because of the above modifications. We discussed how 802.11b's backoff scheme aggravates the deafness issue.

We proposed a new MAC protocol for directional antennas, RTP-DMAC, which is an extension to DMAC [17, 86] to mitigate the impact of deafness. This protocol is a cross-layer protocol that uses inflow and neighbor information from the routing layer. Further we defined a new message frame, RTP, which informs the neighboring nodes about the impending transmission so that the impact of deafness is minimized on these nodes. We also studied some of the existing MAC protocols for directional antennas.

Finally, we evaluated the performance of RTP-DMAC protocol in topologies specifically designed for studying the impact of deafness and also in a random topology. The results show that RTP-DMAC has a better performance than DMAC and the backoff reset mechanism in RTP-DMAC improves the performance in a significant manner.

In the next chapter, we discuss routing in heterogeneous networks consisting of omnidirectional and directional antennas.

Chapter 6

Routing in Heterogeneous Networks

In this chapter we discuss routing in heterogeneous wireless ad hoc networks. We discuss the design of three new routing metrics: ETX1, unidirectional-ETX(u-ETX), and unidirectional-ETX1(u-ETX1) for heterogeneous networks. The ETX1 metric is based on the work done by Cheekiralla and Engels [12] [1].

6.1 Introduction

Routing is the process of finding routes so that nodes in a network can use these routes to communicate. It consists of two main components, the routing protocol and the routing metric. The routing protocol specifies the rules for finding the routes and the metrics specify quality of the route. The goal of routing is to find a correct and an optimal route to the destination in an efficient manner.

Routing protocols for ad hoc networks can be classified as on-demand or reactive routing protocols and proactive routing protocols. In reactive routing, nodes invoke the route discovery process when they don't have the route to a destination node. Route maintenance is also done on a reactive basis, and new routes are found only

[1] Copyright ©2006 IEEE. Parts of this chapter are reprinted from: Sivaram Cheekiralla and Daniel W. Engels. Routing in Heterogeneous Wireless Ad Hoc Networks. In Proceedings of WiMAN 2007, Hawaii, USA, August 2007.

when a link is broken. However in proactive routing, nodes discover and maintain routing tables on a continuous basis.

Routing protocols for wireless ad hoc networks assume that the network is homogeneous. We are interested in the problem of routing in heterogeneous networks with nodes that either use an omnidirectional antenna or a beamforming (directional) antenna.

Since directional antennas have a superior performance compared to omnidirectional antennas, we assume that a network of omnidirectional and directional antennas has a better performance than a network of omnidirectional antennas. We study the problem of routing in such heterogeneous networks and discuss designing routing metrics for these networks.

The remainder of the chapter is organized as follows. In Section 6.2, we discuss the requirements for designing routing metrics for heterogeneous networks. In Section 6.3, we discuss the new routing metrics: ETX1, U-ETX, and U-ETX1. In Section 6.4, we discuss the routing protocol and the route discovery process. In Section 6.5, we discuss MAC layer issues that need to be considered when using the proposed routing metrics. We evaluate the proposed routing metrics in Section 6.6 and discuss previous work in Section 6.7. Finally, we draw the relevant conclusions in Section 6.8.

6.2 Requirements

Routing metric specifies quality of the route, e.g. the metric could specify the distance between the source and the destination nodes or the travel time for a data packet between the source and the destination. Commonly used routing metrics for wireless ad hoc networks include hop count, expected number of transmissions (ETX) [20], expected travel time (ETT) [24], etc. All these metrics have been proposed for homogeneous networks. We identify requirements of routing metrics for heterogeneous networks in the following.

6.2.1 Unidirectional links

Networks consisting of omnidirectional and directional antennas have unidirectional links. A unidirectional link between two nodes A and B is in which, node B is able to hear messages from node A, but not vice-versa. Unidirectional links in heterogeneous networks exist because of the difference in gain between a directional antenna and an omnidirectional antenna. Consider the scenario shown in Figure 6-1, when node A (an omnidirectional antennas) broadcasts, node B (a directional antenna) can hear, but not vice-versa.

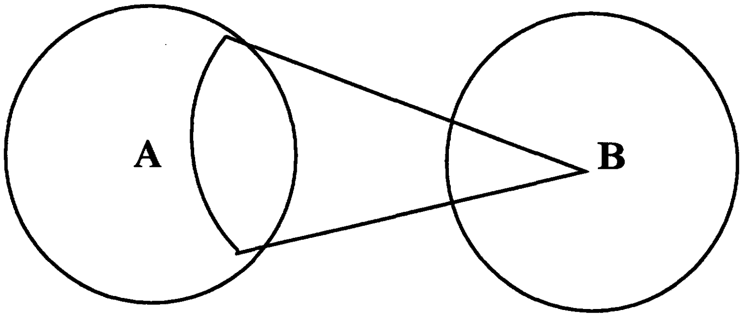


Figure 6-1: Unidirectional links in heterogeneous networks

Unidirectional links and in general asymmetric links cause complications at the MAC and the routing layers. The commonly used MAC protocol for ad hoc networks, 802.11 DCF protocol relies on bidirectional link capabilities for delivering the data.

At the routing layer, the following problems are created because of asymmetric links [69]:

1. Knowledge asymmetry; created when node B knows about node A and not vice-versa.

2. Routing asymmetry; created when the shortest path from node A to node B is different from node B to node A.

3. Sink unreachability; created when the route reply (RREP) messages from the destination node do not reach the source node.

4. Because of asymmetric links, it is possible that the routing packets (route requests, route replies, etc.) can be transmitted across a link (bidirectionally), but

> not data packets[2]. Using different transmission powers in the network can also cause asymmetric links. For example, the 802.11 DCF protocol specifies different transmission powers for broadcast and unicast packets. Because of this, it was found that gray zones could be found in the network where broadcast packets could be received and not unicast packets [53].

The routing protocol should be aware of the possibility of unidirectional links in wireless networks. For example, routing protocols like ad hoc on demand vector (AODV) [66] are designed to work only in the presence of bidirectional links. In this protocol, destinations simply use the reverse route from the source. However asymmetry or unidirectionality in the network implies such a reverse route may not exist.

Thus a routing metric for the heterogeneous networks should consider the strong possibility of unidirectional links and should choose bidirectional links while selecting the routes.

6.2.2 Neighbor Discovery

Apart from the unidirectionality aspect in heterogeneous networks, the routing metric should allow neighbor discovery. Neighbor discovery now additionally involves knowing the type of the antenna also. Since directional antennas have a superior performance compared to omnidirectional antennas, ideally the routing metric should choose routes that consist of as many directional antennas as possible.

We study these requirements with a simple scenario.

6.2.3 Example Scenario

Before describing the example scenario, we define our notation. OM stands for omnidirectional mode and DM stands for directional mode. An OD node is an omnidirectional node and a D node is a directional node. We define the following communication

[2] Data packets are usually bigger in size than the routing packets, and the probability of error increases with the increase in the size of the packet.

ranges: O-O is the communication range when both nodes are OD nodes. We define D-O range when the sender, a D node uses directional transmission and the receiver is an OD node. Similarly the definitions of O-D range and D-D range follow. For the current example scenario, O-D range is 500 m, D-O range is 265 m, D-D range is 520 m, and the O-O range is 270 m.

We consider a heterogeneous network consisting of omnidirectional and directional networks (Figure 6-2). Consider the case when node 1 has to send data to node 25. We assume that dynamic source routing (DSR) protocol is used for finding the route between these two nodes. We briefly describe some of the features of DSR here and discuss DSR in greater detail in the latter part (Section 6.4) of this chapter.

DSR is a reactive routing protocol and in order to find a route to a destination node, a source node broadcasts a route request (RREQ) message. Intermediate nodes relay this message until it reaches the destination. Nodes don't relay RREQ messages that have loops in them or duplicate RREQ messages which are not better than the original RREQ message. The route taken by a RREQ message is also embedded in i. When ever a node relays a RREQ message, it appends its address to the address path (also called as the source route). Nodes check the source route to detect loops. Nodes, when they relay the RREQ messages also increment the routing metric. Once the destination node gets the RREQ message, it sends a route reply (RREP) message. The RREP message uses the reverse route traversed by the RREQ message. The RREQ messages are broadcast messages, while the RREP messages are unicast messages.

We consider two routing metrics for this example, hop count and the expected number of transmissions (ETX). We describe ETX in detail in next section. For the current discussion, it is sufficient to know that ETX can discover unidirectional links in the network and penalizes them (i.e. gives a greater link cost than a bidirectional link).

From Figure 6-2, we see the routes taken by two RREQ messages. The route represented in the dotted line has unidirectional links, while the one in the solid line doesn't have any unidirectional links. The destination node receives both the

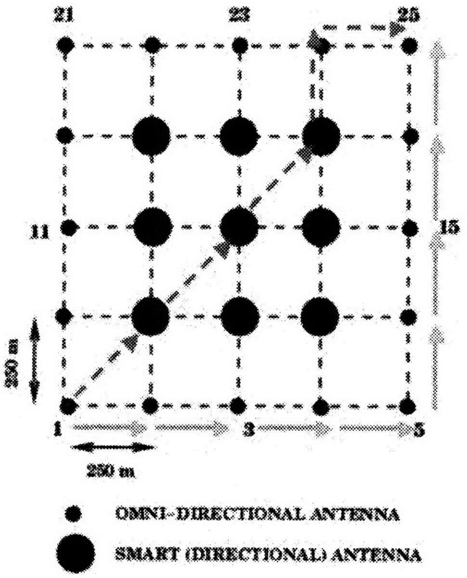


Figure 6-2: Routes chosen by hop count in a heterogeneous network

RREQ messages and it replies to the first RREQ message and the subsequent ones that are better than the best seen so far. If the RREQ message that travels via the shorter route reaches the destination first, then the RREQ message route that travels via the longer route is not replied. Thus, the RREP message that uses route with unidirectional links never reaches the source node. The RREQ message, which uses the bidirectional links is never replied. Thus with hop count, unidirectional links are not differentiated from bidirectional links. From the above scenario, we see that unidirectional links should be penalized. If unidirectional links were penalized then the RREQ message that travels the route with bidirectional links would be replied to.

Lets consider the same scenario when ETX is used as the routing metric. As mentioned previously, ETX detects unidirectional links (dotted line with arrows in Figure 6-3) and also penalizes them. We see that ETX chooses the routes that have bidirectional links (solid line with arrows in Figure 6-3) as well as routes which are shorter than the routes chosen by hop count metric. ETX also avoids routes that have unidirectional links thus reducing the impact of sending unwanted RREP messages. However, in the above scenario, ETX does not utilize directional antennas in the network to find shorter routes.

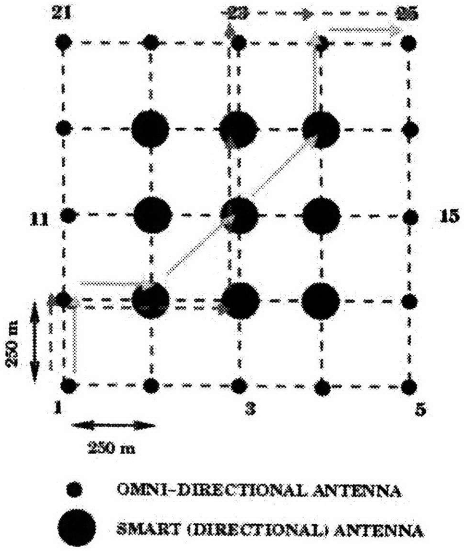


Figure 6-3: Routes chosen by ETX in a heterogeneous network

To summarize, a routing metric for heterogeneous network should have the following properties:

- Discover unidirectional links and penalize them.
- Have a good neighbor discovery scheme to improve the chance of discovering shorter routes.

Having discussed the requirements of routing metrics for heterogeneous networks, we discuss routing metrics for heterogeneous networks.

6.3 Routing metrics

The ETX metric for homogeneous wireless ad hoc networks solves the issues that we discussed in the previous section. We first discuss the details of ETX metric and then suggest modifications for improving the performance of ETX in heterogeneous networks.

6.3.1 ETX

ETX is one of the best routing metrics for homogeneous networks with OD nodes [20]. The ETX metric is calculated in the following manner. Nodes in the network periodically (every 1 second jittered up to 100 ms) broadcast specially designed probes. A node's probes contain its neighbors and the number of ETX probes that this node has heard from these neighbors in the last 10 seconds. Thus when a node 1 receives a probe from another node 2, it knows how many of its probes have reached 2 in the last 10 seconds. Further, node 1 also keeps track of the number of probes it has heard from 2. The number of probes 2 has heard from 1 and vice-versa gives an estimate of the quality of link between 1 and 2 (see Figure 6-4).

The ETX metric for a link is calculated as $\frac{100}{d_f * d_r}$, where d_f and d_r are the number of probes received in the last 10 seconds in the forward and reverse directions. If $d_f \neq d_r$, then the link is asymmetric. The value of ETX can vary from 1 to infinity. A value of 1 implies, the link is a very good link, and an ETX value of infinity implies the link is unidirectional [20]. We use 100 as an approximation to infinity.

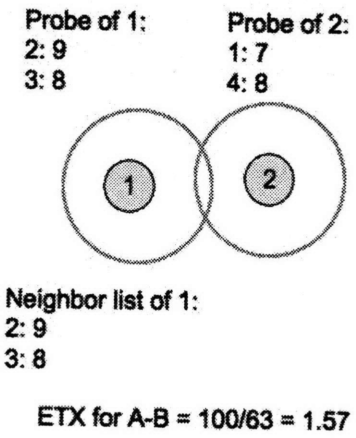


Figure 6-4: Calculation of ETX metric

To summarize, ETX [20] solves the issues mentioned in the previous section. ETX has an inherent neighbor discovery protocol and further ETX quantifies asymmetric links. However ETX needs some modifications so that it is possible to use directional antennas. Using directional antennas reduces the link length and hence improve the throughput. We propose two modifications in this thesis, the first modification is to use a higher transmission power. The other modification is to convert unidirectional links to bidirectional links. We discuss these modifications and the new routing metrics in the following section.

6.3.2 ETX1

With normal broadcast power, nodes can only discover their neighbors in the O-O communication range. In order to discover nodes beyond the O-O communication range, nodes have to increase the default broadcast power. We propose a modification to the ETX mechanism so that nodes not only discover the nodes in the O-O communication range but also some of the nodes beyond the O-O communication range. This allows an OD node to potentially reach nodes beyond its O-O communication range. This way the destination can be reached in a fewer number of hops and hence a higher throughput can be achieved. Further, we also want to to distinguish between nodes that are in the O-O communication range and those that are beyond this range so as to use transmission power in a conservative manner. We also make a minor addition to the ETX probes; nodes also indicate their type, i.e OD or D in their ETX probes. This way a node not only knows its neighbors, but also the type of the neighbor.

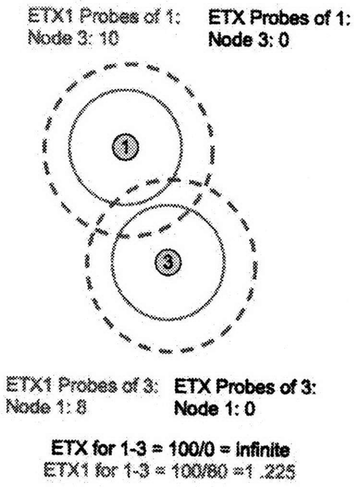


Figure 6-5: Calculation of ETX and ETX1 metric

We suggest the following mechanism for discovering nodes that are beyond the O-

O communication range and distinguish them from those in the O-O communication range. We define an additional ETX-like metric, ETX1. The combination of ETX and ETX1 is the new power-controlled ETX metric. ETX probes are transmitted at the default broadcast power, while ETX1 probes are transmitted at a higher power. Nodes alternately broadcast ETX and ETX1 probes every second, and hence an ETX or an ETX1 probe is broadcasted every 2 seconds. Nodes now additionally calculate the ETX1 metric between themselves and their neighbors in the same manner as they calculate ETX metric. Thus, a node 3 (OD node) that is beyond the O-O communication range of 1 (OD node) will have a finite ETX1 metric and an infinite ETX metric (see Figure 6-5). We evaluate the performance of this metric Section 6.6. We discuss why unidirectional links are caused in heterogeneous networks and see if it is possible to design metrics utilizing these links.

6.3.3 U-ETX and u-ETX1

In this section, we describe the design of two new routing metrics to use the unidirectional links in heterogeneous networks. In a unidirectional link, only one of the nodes that constitute the link is aware of the unidirectional link. The node that is aware of the link is able to hear from the other node but not vice-versa. In heterogeneous networks, unidirectional links exist between a directional node and an omnidirectional node, and the directional node is aware of the unidirectional link. We design metrics to exploit this fact.

Consider the example shown in Figure 6-6, where there are bidirectional links between A (OD node) and B (OD node) and between B and C (D node). There is also a unidirectional link between node A and node C, and node C is aware of this unidirectional link. Assume that node A needs a route to node E (not in Figure 6-6) and it issues a RREQ message. Nodes B and C hear the RREQ and use the ETX metric for forwarding the RREQ messages. Node C forwards the RREQ message with a route ETX metric of 100. Node B also forwards the RREQ message it received with a link ETX metric of 1. When node B forwards the RREQ message, node C also receives it. Node C forwards this RREQ message with a route ETX metric of 2 (as 2 is lower than 100). We see that node C forwards the shorter route (A-C) with a higher metric and the longer route (A-B-C) with a shorter metric.

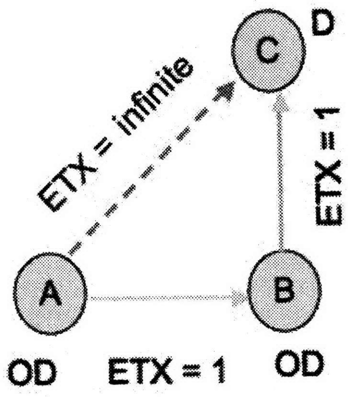


Figure 6-6: Unidirectional ETX

In the above scenario, if node C can use a higher transmission power when communicating with node A, the link can be made bidirectional. Further if the shorter route has to be selected in the route discovery process, the routing metric for the link should be less than 100. The alternate route A-B-C, has an ETX value of 2. Hence, node C should use a value less than 2 and greater than 1 (as 1 is the least possible ETX metric of a link) when relaying the RREQ. Thus node C chooses a value of 1.9 and hence node C creates a bidirectional link.

When node C forwards the RREP (a unicast message) message to node A, it is aware that the link between A and C is a unidirectional link. Hence, node C uses a higher transmission power to send the RREP message to A. Thus using a shorter ETX metric for a unidirectional link and increasing the directional transmission power, it is possible to use the unidirectional links in a better way. We call this new routing metric the unidirectional-ETX. We evaluate the performance of this metric in Section 6.6.

Even with the above modifications, the unidirectional links are not completely utilized. Consider Figure 6-7, where node C (OD node) is the destination node and node A (D node) and node B (OD node) are its neighbors. When node A broadcasts the RREQ message, node B can hear the RREQ message and not node C. However node A is aware of the unidirectional link and it is possible to use higher

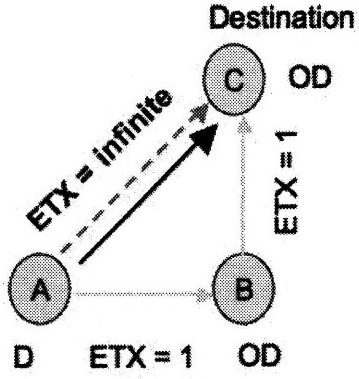


Figure 6-7: Unidirectional ETX1

directional transmission power towards node C and transmit the RREQ message. We make this change in the routing protocol so that nodes (if they are D nodes) when relaying RREQ messages, check if the destination node is in their neighbor list. If the destination node is in the list, the D node sends a directed transmission (unicast) with a higher power towards the destination (if it is a unidirectional link). The destination node uses a value of 1.9 for the unidirectional link instead of 100 (infinity). We call this metric the unidirectional-ETX1, which is an extension to U-ETX. We evaluate the performance of this metric and compare its performance with the other metrics in Section 6.6.

We discuss the routing protocol and some of the issues in the route discovery process in the following section.

6.4 Routing Protocol

DSR has a better performance than other reactive routing protocols [23], and therefore we use DSR [42] as the routing protocol. Since we are concerned with static ad hoc networks, we focus on the route discovery part . We first discuss DSR and then discuss our modifications to DSR. These modifications allow a fair comparison of routing metrics for static ad hoc networks. We also discuss some of the tradeoffs in the route relay process during the route discovery part.

6.4.1 DSR

In DSR, routes are found on a per-need basis. A source node that needs to send data to a destination node checks its routing table for a route to the destination. If a route is found, the source node uses it to transmit data to the destination. If no route to the destination exists, the source node broadcasts a route request (RREQ) message asking its neighbors if any of them has a route to the destination [42].

Intermediate nodes that hear the RREQ message relay it to others if they don't have a route to the destination. Thus, the RREQ message is relayed until it reaches the destination. The route taken by the RREQ message is included in the RREQ message, and each node adds itself to the route before relaying the RREQ message. Nodes also see if they are already in the route traversed by the RREQ message so that loops are avoided in the route. Intermediate nodes that are in the route cache the routes to the source and the destination when they relay the RREQ/RREP messages. This is done so that in the future intermediate nodes can reply from their cache instead of relaying the RREQ message to the destination [42].

RREQ messages have identifiers and an intermediate node terms a RREQ message as a duplicate if the node has seen a previous RREQ message with the same source-destination node pair and the same RREQ identifier. Nodes don't forward duplicate RREQ messages and this may lead to finding a non-optimal route. DSR also defines route maintenance and route salvaging mechanisms when links break or when nodes are mobile [42].

6.4.2 Modifications to DSR

We now discuss a few modifications to DSR. We disallow intermediate nodes to reply from their route caches so as to measure the performance of the routing metric in a fair manner. We also disallow intermediate nodes from caching the routes. Only the source and the destination nodes cache the routes. We allow an intermediate node to relay a duplicate RREQ message if the routing metric of the duplicate RREQ message is better than the routing metric of any of the RREQ messages received so far (for the same source and the destination). We disable DSR's packet salvaging and route maintenance mechanisms, as we are concerned with static ad hoc networks. Since DSR has been designed for the hop count metric, we modify the format of DSR's message to also include the ETX and the proposed metrics.

We next discuss some of the issues in the route discovery process for heterogeneous networks.

6.4.3 Route Discovery

In the route discovery phase, nodes relay the RREQ messages as long as they are not duplicate, do not contain loops, or if they are duplicate and better than the original. We discuss the specific modifications for the ETX1 metric.

In the route discovery phase, nodes broadcast the RREQ messages at a higher power (equal to the transmission power of ETX1 probes) than the default broadcast power. Intermediate nodes add the ETX and the ETX1 values (between itself and the previous hop) in the RREQ message. If the previous hop is an OD node, the ETX values are doubled so as to penalize routes that have OD nodes. Ideally, the route should have higher D nodes so as to increase the throughput. If an intermediate node receives the RREQ message for the first time, it forwards the RREQ message.

Nodes when they relay the RREQ message, they have a choice between ETX, ETX1, and any combination of ETX and ETX1 (e.g., ETX + ETX1) as the metrics to decide which RREQ messages are better. Choosing ETX1 will potentially lead to a shorter route and hence a higher throughput can be achieved. Therefore, nodes choose ETX1.

When the destination receives the RREQ message, it replies to the first RREQ message. It replies to the subsequent RREQ messages only if the metric (either ETX or ETX1 or a combination of them) is better than the metric of the previously replied RREQ messages. The destination node now does not use ETX1 metric because using ETX1 metric increases the chance of selecting a route that requires all the nodes in the path to use higher transmission power. It uses ETX + ETX1 as the metric. Using the combined metric reduces this chance and hence allows some of the intermediate nodes to use default transmission powers, and thus conserve energy. The destination node stores the routes from the RREQ messages to which it replied in its route cache.

We need modifications at the MAC layer to accommodate the routing metrics. We discuss these modifications in the following section.

6.5 MAC layer modifications

We use the following MAC protocol for all the metrics: OD nodes use the standard 802.11 MAC DCF protocol, while D nodes use a modified version of the 802.11 MAC protocol [86]. Further, D nodes use directional handshake messages and use the directional mode for data and acknowledgment frames.

6.5.1 MAC for ETX1

The power level for the messages is determined from the neighbor information from the routing layer as follows. Since some of the nodes in the route are beyond the O-O communication range, nodes should know the power levels to reach the next hop. A node determines the power level to transmit data to the next hop as follows. It checks its neighbor table and sees if there is a finite ETX value between itself and the next hop. If so, it uses the default power level to transmit data and if not the higher power is used to transmit data. Nodes use this technique for transmitting RTS/CTS, data, and the acknowledgment frames.

6.5.2 MAC for U-ETX & U-ETX1

For these metrics, the routing layer cheats and creates shorter routes. However the MAC layer is unaware of the unidirectional link and the cheating the routing layer has done. Since the MAC layer is not aware of the kind (unidirectional or bidirectional) of link the routing layer has chosen, it is necessary for the MAC layer to get the information from the routing layer. If the MAC layer finds the link to be a unidirectional link, it knows that it has to use a directional transmission with an increased gain to make this link bidirectional. The MAC layer then informs the physical layer to use the directional beam with a higher gain.

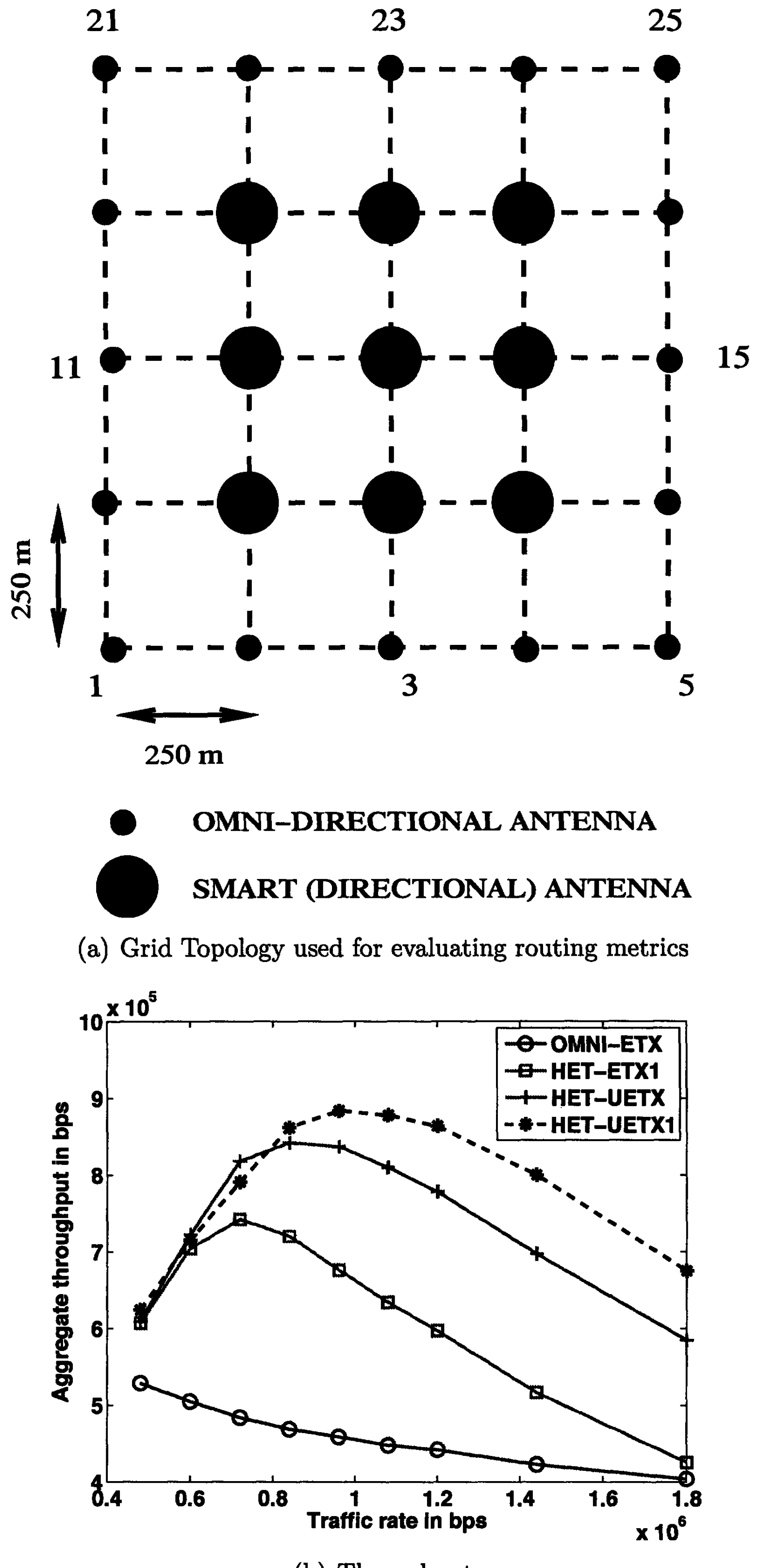
We evaluate the performance of the routing metrics in the next section.

6.6 Evaluations

We use Qualnet (ver 3.9) [71] simulator for our simulations. Nodes use 802.11b radios with a fixed transmission rate of 11Mbps. The O-O communication range is 270 m and the O-D communication range is nearly 500 fffm when using the default transmission power of 15 dB. In all our simulations, we use the first 100 seconds of simulation time for neighbor discovery using ETX probes. Once the neighbor discovery process is done, we use dummy traffic to find routes between the nodes. Once routes are found, we use those routes for simulating the actual traffic. We simulate the actual traffic for 200 s. All the points in the subsequent graphs correspond to an average of 10 runs.

The objective of the simulations is to compare and evaluate the performance of the proposed three routing metrics. We use a grid topology and a random topology to evaluate the performance of these metrics. We use aggregate throughput (from the source node to the destination node), data delivery ratio (defined as the ratio of the total number of data packets received by the destination node to the total number of data packets sent by the source node), and the average end-to-end delay (defined as the average delay of the data packets that have reached the destination node) as the performance metrics for evaluating the routing metrics.

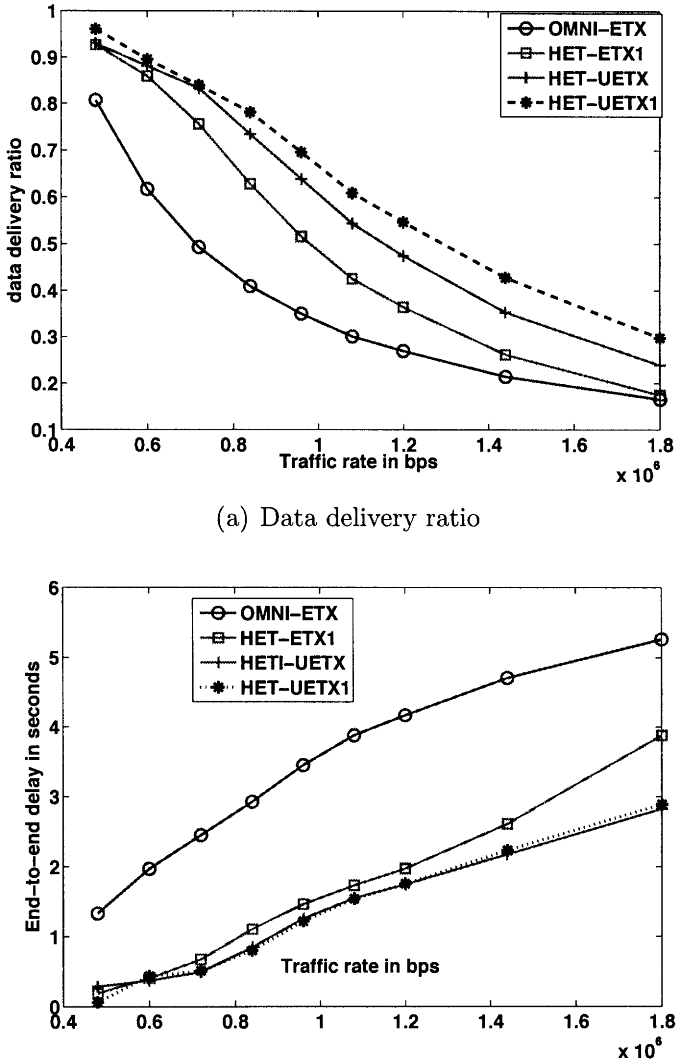
We consider the grid topology shown in Figure 6-8(a). The grid topology consists of both omnidirectional and directional antennas. We initially consider the grid with all OD nodes to find the performance of the ETX metric in the homogeneous network and use this as the base case. We then analyze the heterogeneous case. The flows in the grid are between the following nodes (source-destination): 1-25, 5-21, 3-23, and 11-15. Each flow is a CBR flow with a constant data packet size of 512 bytes. For the power-controlled ETX metric, we set the transmission power of ETX1 probes to



(a) Grid Topology used for evaluating routing metrics

(b) Throughput

Figure 6-8: Performance of routing metrics in grid topology



(a) Data delivery ratio

(b) End-to-end delay in seconds

Figure 6-9: Performance of routing metrics in grid topology

20 dB.

Figures 6-8(b), 6-9(a), and 6-9(b) show the network performance for the three metrics and the base case. As we have assumed, the homogeneous network of OD nodes gives a lower bound on the aggregate throughput. With the heterogeneous network, we see that all the routing metrics perform better than the homogeneous case. Overall, there is an improvement of 96% in the throughput with the heterogeneous case. Amongst the routing metrics, the order of performance in ascending order is ETX1, U-ETX, and U-ETX1. The poor performance of ETX1 can be attributed to the increased power used by the OD nodes, which causes interference at other receiving nodes. Both U-ETX and U-ETX1 metric have a better performance compared to the ETX1 metric. U-ETX improves the throughput up to 35% and U-ETX1 improves the throughput up to 59% over ETX1. This can be attributed to the clever usage of the increased power by directional antennas in finding shorter routes. Between U-ETX and U-ETX1, U-ETX1 has a better performance than U-ETX as U-ETX1 tries to find shorter routes than U-ETX. U-ETX1 improves the throughput up to 16% over the U-ETX metric. We see a similar trend with the data delivery ratio and the end-to-end delay, UETX1 has the best performance of the three routing metrics. U-ETX1 improves the data delivery ratio up to 71% and decreases the end-to-end delay up to 68% compared to the ETX1 metric. Also, the end-to-end delay for U-ETX and U-ETX1 metric is quite similar with marginal difference. Clearly, U-ETX1 has a better performance than the other two metrics for the grid topology.

We next consider a random topology of 50 nodes, of which 10 nodes use directional antennas. We randomly select 10 pairs of flows to evaluate the network performance. We initially evaluate the performance with the homogeneous case of OD nodes to get a lower bound on the aggregate throughput. Fig 6-10 shows the performance of the metrics in random topology. We observe that the the heterogeneous case has a superior performance than the homogeneous case.

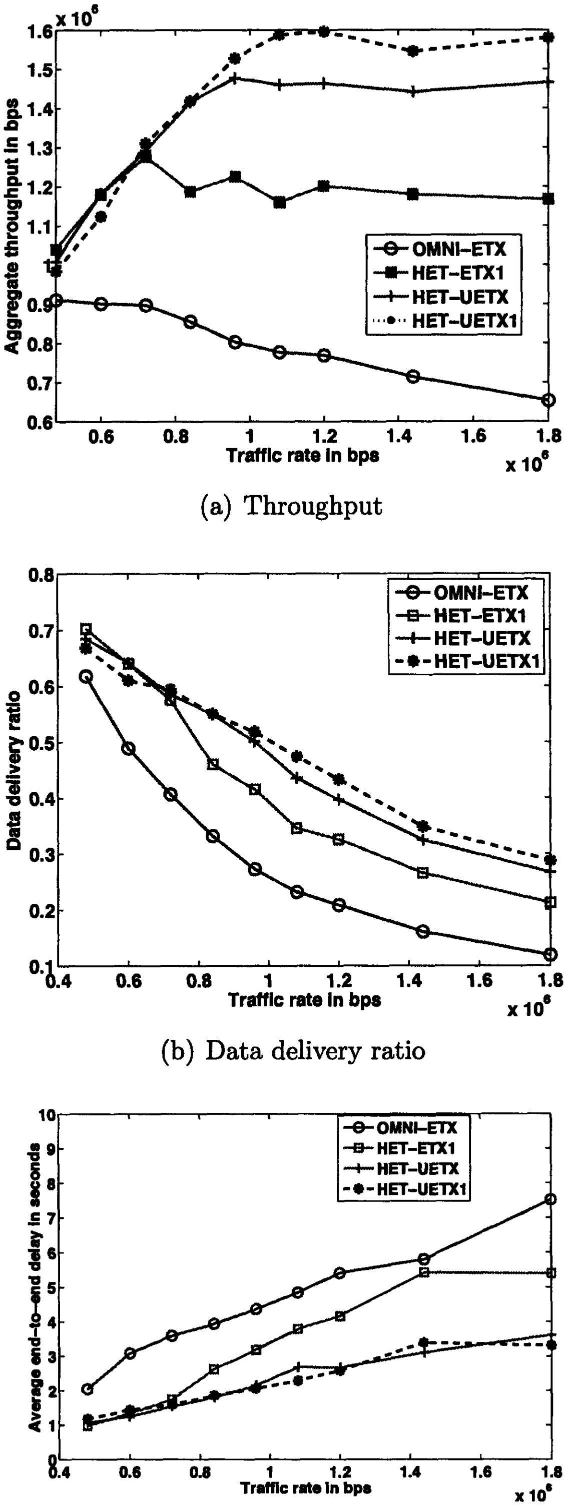
Overall, there is an improvement of 142% in the throughput with the heterogeneous case. Amongst the routing metrics, the order of performance in ascending order is ETX1, U-ETX, and U-ETX1, which is similar to their performance in the grid topology. U-ETX improves the throughput up to 37% and U-ETX1 improves the throughput up to 26% over ETX1. U-ETX1 improves the throughput up to 10% over the U-ETX metric. We see a similar trend with the data delivery ratio and the end-to-end delay, UETX1 has the best performance of the three routing metrics. U-ETX1 improves the data delivery ratio up to 38% and decreases the end-to-end delay up to 56% compared to ETX1. Also, the end-to-end delay for U-ETX and U-ETX1 metric is quite similar with marginal difference. Clearly, U-ETX1 has a better performance than the other two metrics for the random topology.

To summarize, heterogeneous networks with directional antennas and omnidirectional antennas have a better performance than a homogeneous network of omnidirectional antennas. We find that the aggregate throughput can be improved up to 142 % in a random topology and up to 96% in a grid topology. Amongst the proposed three metrics, U-ETX1 has the best performance followed by U-ETX and ETX1. U-ETX1 improves the performance over U-ETX as it is an extension to U-ETX and it tries to find shorter routes at the destination as well as while forwarding the route request messages.

We discuss the previous work on routing with directional antennas.

6.7 Relevant work

Sundaresan and Sivakumar [47] propose a MAC and routing protocol for heterogeneous networks that includes omnidirectional antennas, fixed-beam antennas, adaptive-array antennas, and Multiple-Input, Multiple-Output (MIMO) antennas. They describe a routing protocol similar to DSR for heterogeneous networks, which uses a three-tuple routing metric. The first two components capture the spatial reusability of the network and the third component captures the link rate. However, they assume the same transmission range for all the links on the network. Thus, the advantage of increased range by using a smart antennas is lost. We would like to distinguish our work from theirs as we consider a more specific case of heterogeneous network and our focus is on designing and evaluating a routing metric for this specific case. Further



(a) Throughput

(b) Data delivery ratio

(c) End-to-end delay in seconds

Figure 6-10: Performance of routing metrics in Random topology

we take advantage of the higher communication range of directional antennas.

Roy et al. [76] compare the performance of multipath routing with omnidirectional and directional antennas in homogeneous networks. They hypothesize that "route coupling" is minimized when directional antennas are used, and hence a higher throughput is achieved using directional antennas than with using omnidirectional antennas. Choudhury et al.[16] evaluate the performance of DSR using directional antennas. They suggest a "delayed route reply optimization" mechanism that allows better routes to be discovered. Choudhury [15] propose a capture aware routing protocol for multi-beam smart antennas that minimizes the effect of MAC layer capture thus improving the performance of the network. A weighted metric of hop count, capture-awareness, and node-sharing is used for choosing the routes. Cheekiralla et al. [14] compared the performance of a queue-length based routing metric with the hop count metric and found that the queue length-based metric performs better than the hop count metric.

6.8 Conclusions

In this chapter, we discussed the requirements for routing metrics for a heterogeneous network consisting of omnidirectional and directional antennas. We proposed three routing metrics, that are extensions to the ETX metric [20]. The first metric, ETX1 increases the broadcast power to find shorter routes. ETX1 is used in combination with ETX so as to conserve power as well as find shorter routes. We then proposed U-ETX and U-ETX1 to convert the unidirectional links as bidirectional links. U-ETX converts the unidirectional links as bidirectional links when relaying the RREQ messages, where as U-ETX1 does it while relaying the RREQ messages as well as when the destination is one hop away. Thus, ETX-1 has a better chance of finding shorter routes than U-ETX.

We evaluated the performance of the three routing metrics in a grid topology and in a random topology. We observed that all the three routing metrics improve the network performance (in terms of throughput, data delivery ratio, and end-to-end delay) in a heterogeneous network compared to the performance of ETX in a network of omnidirectional nodes. Amongst the proposed metrics, U-ETX1 has a better performance than the other two metrics as U-ETX1 finds shorter routes better than the other two metrics. Overall, in the random topology, U-ETX1 improves the throughput up to 37% and in the grid topology, improves the throughput up to 59% over the ETX1 metric.

The focus of this chapter was on designing routing metrics for heterogeneous networks. In the future, we plan to address the various MAC layer issues in heterogeneous networks.

We draw the relevant conclusions of this thesis in the next chapter.

Chapter 7

Conclusions

In this thesis, we discussed issues that need to be addressed for efficient communication in heterogeneous wireless ad hoc networks. Two of these issues are applicable to a broad class of heterogeneous wireless ad hoc networks and the other issues are applicable to networks that consist of omnidirectional and directional antennas. We proposed solutions for these issues and evaluated some of the solutions.

The issues and solutions are summarized below:

1. Device classification. As devices with different capabilities are used in wireless ad hoc networks, unambiguous classification of the devices is necessary. To solve this issue, we developed a taxonomical approach for unambiguously classifying devices based on their functionality. Functionality is defined on the basis of communication capability of the devices. Once a device is classified, it is characterized on the basis of different attributes. The classification scheme can be used for classifying a wide spectrum of devices ranging from RFID tags to laptops.

2. Device identification. It is necessary to have unique identifiers for efficient communication in networks. We developed an IPv6 identification scheme that can be used for identifying all kinds of physical objects. Based on this scheme, we developed routing schemes that allow generic object-to-object communication using the existing Internet infrastructure. The first scheme is a naming system

that relies on the DNS for the routing, and the other scheme uses routers as distributed databases.

We extended the IPv6 identification system to a multi-addressing scheme for wireless ad hoc networks. The multi-addressing scheme provides multiple routes in wireless networks and thus improving the redundancy of wireless networks.

3. Medium access control. We developed a new MAC protocol for ad hoc networks with directional antennas, RTP-DMAC for solving the deafness problem. We briefly discussed the 802.11b MAC protocol and the modifications to it so that directional antennas can be used at the physical layer. We discussed how 802.11b's backoff scheme aggravates the deafness problem. We used this as a motivation for designing the RTP-DMAC protocol, which is an extension to the multiple RTS-CTS-based MAC protocols. We evaluated the performance of this MAC protocol and compared its performance with that of the DMAC protocol. We found that RTP-DMAC protocol has a better performance (in terms of throughput) than DMAC.

4. Routing metrics for heterogeneous networks that consist of omnidirectional and directional antennas. We argued that the requirements of routing metrics for heterogeneous networks that consist of omnidirectional and directional antennas are detecting unidirectional links and penalizing them and neighbor discovery. We found that ETX satisfies these properties, but needs further modifications so that the routing performance can be improved in heterogeneous networks. We proposed three new routing metrics that are extensions to ETX: ETX1, U-ETX, and U-ETX1.

   The first metric, ETX1 is a power controlled routing metric that finds shorter routes by increasing the transmission power. The other two routing metrics U-ETX and U-ETX1 use higher directional transmission power with directional antennas so that the unidirectional links appear as bidirectional links. We discussed some of the changes that are required at the MAC layer to accommodate these metrics.

We evaluated the performance of these metrics in a grid topology and a random topology. We found the order of performance of the metrics in descending order as U-ETX1, U-ETX, and ETX1. We found that U-ETX1 improves the throughput up to 37% in the grid topology and improves the throughput up to 59% in the random topology over the ETX1 metric. Finally, we evaluated how having directional antennas improve the throughput performance compared to omnidirectional antennas.

Having discussed the contributions of this thesis, we now discuss how this work can be extended.

7.1 Future Work

We discuss directions for future work on the basis of our contributions in this thesis. They are below:

1. There is an increasing convergence of different technologies with standards such as 3G [59]. The proposed taxonomy can be extended to a wider range of devices such as actuators and devices used in robotics. We anticipate that these technologies would be part of applications that involve sensor networks and mesh networks. If such technologies were to be included in the taxonomy, the basis for classification and characterization would need to change. However, the general framework of taxonomy would be still applicable.

2. The proposed IPv6 identification scheme needs further work in terms of security and evaluation. We anticipate that are issues related to routing table sizes and DNS issues when using the proposed IPv6 identification scheme and the routing methodologies. Regarding the multi-addressing scheme, a proper scheme to assign addresses based on the identifier and a mechanism to detect duplicate addresses are needed.

3. The proposed MAC protocol improves the performance of directional antennas. An interesting future direction is to design a MAC protocol for heterogeneous

networks consisting of omnidirectional and directional antennas. We studied some of the routing layer issues in heterogeneous networks, but MAC layer issues in heterogeneous networks is relatively an unexplored area.

One of the important problems in ad hoc networks with directional antennas is the aggravation of deafness issue caused by 802.11b' s backoff scheme. It may be possible to design a MAC protocol with minimum modifications to 802.11b's backoff scheme so that the deafness issue isn't aggravated. Further, extending this backoff scheme to heterogeneous networks is another interesting problem

4. We proposed routing metrics that solve the issue of unidirectional links in heterogeneous networks so that the MAC layer can function smoothly. One of the important areas that need further investigation is the interaction of MAC and routing layers in heterogeneous networks. Another important area is the issue of connectivity/power control in heterogeneous networks consisting of omnidirectional and directional antennas.

There is a lot of active research in the field of smart environments where different sensing and communicating technologies (both wired and wireless) are used. For example smart home project at University of Texas Arlington [22]. In future, we anticipate applications similar to the smart home application use different types of heterogeneous networks. We expect that the research presented in this thesis would be useful in such applications.

Bibliography

[1] A. Acharya, A. Misra, and S. Bansal. MACA-P: a MAC for concurrent transmissions in multi-hop wireless networks. In *Pervasive Computing and Communications, 2003. (PerCom 2003). Proceedings of the First IEEE International Conference on*, pages 505–508, 23-26 March 2003.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Comput. Networks*, 38(4):393–422, 2002.

[3] Tuomas Aura and Michael Roe. Designing the mobile IPv6 security protocol. *Annales des Télécommunications*, 61(3-4):332–356, 2006.

[4] Steven M. Bellovin. Using the Domain Name System for System Break-ins. In *Proceedings of the Fifth USENIX UNIX Security Symposium*, June 1995.

[5] Edoardo S. Biagioni, K.W. Bridges, and Brian J.S. Chee. *A Remote Ecological Micro-Sensor Network*. `http://www.botany.hawaii.edu/pods/overview.htm`. Accessed on May 23, 2008.

[6] John Bicket, Daniel Aguayo, Sanjit Biswas, and Robert Morris. Architecture and evaluation of an unplanned 802.11b mesh network. In *MobiCom '05: Proceedings of the 11th annual international conference on Mobile computing and networking*, pages 31–42, New York, NY, USA, 2005. ACM.

[7] David Brock. *The Networked Physical World-Proposal for Engineering the Next Generation of Computing, Commerce and Automatic-Identification*. `http:`

//www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-001.pdf, 2000. Accessed on May 23, 2008.

[8] Santashil Pal Chaudhuri, Shu Du, Amit Kumar Saha, and David B. Johnson. TreeCast - A Stateless Addressing and Routing Architecture for Sensor Networks. In *Proceedings of the 4th IPDPS International Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN 2004)*, pages 221–228, April 2004.

[9] S. Cheekiralla and D.W. Engels. A functional taxonomy of wireless sensor network devices. In *Broadband Networks, 2005 2nd International Conference on*, pages 949–956 Vol. 2, 3-7 Oct. 2005.

[10] Sivaram Cheekiralla. Development of a wireless sensor unit for tunnel monitoring. Master's thesis, Massachusetts Institute of Technology, Feb 2004.

[11] Sivaram Cheekiralla and Daniel W. Engels. An IPv6-Based Identification Scheme. In *ICC 2006*, Istanbul, Turkey, June 2006.

[12] Sivaram Cheekiralla and Daniel W. Engels. Routing in Heterogeneous Wireless Ad Hoc Networks. In *WiMAN 2007*, Hawaii, USA, August 2007.

[13] Sivaram Cheekiralla and Daniel W. Engels. Viral IP Address Assignment. In *Proceedings of IEEE LCN 2006*, pages 574–575, Nov. 2006.

[14] Sivaram Cheekiralla, Ariadna Quattoni, and Daniel Engels. Load-Sensitive Routing With Directional Antennas. In *Proceedings of The 17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communication*, 2006.

[15] Romit Roy Choudhury. *Using Beamforming Antennas for Wireless Multihop Networks.* PhD thesis, UIUC, 2006.

[16] Romit Roy Choudhury and Nitin H. Vaidya. Performance of Ad Hoc Routing using Directional Antennas. *Journal of Ad Hoc Networks*, November 2004.

[17] Romit Roy Choudhury, Xue Yang, Nitin H. Vaidya, and Ram Ramanathan. Using directional antennas for medium access control in ad hoc networks. In *MobiCom '02: Proceedings of the 8th annual international conference on Mobile computing and networking*, pages 59–70, New York, NY, USA, 2002. ACM Press.

[18] R.R. Choudhury and N.H. Vaidya. Deafness: a MAC problem in ad hoc networks when using directional antennas. In *Proceedings of ICNP 2004*, pages 283–292, 5-8 Oct. 2004.

[19] R.R. Choudhury, Xue Yang, R. Ramanathan, and N.H. Vaidya. On designing MAC protocols for wireless networks using directional antennas. *Mobile Computing, IEEE Transactions on*, 5(5):477–491, May 2006.

[20] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris. A high-throughput path metric for multi-hop wireless routing. In *MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 134–146, New York, NY, USA, 2003. ACM Press.

[21] Pete Cross. Zeroing in on zigbee (part 1): Intorduction to the standard. *Circuit Cellar*, pages 16–23, February 2005.

[22] S.K. Das and D.J. Cook. Guest Editorial - Smart Homes. *Wireless Communications*, 9(6):62–62, Dec. 2002.

[23] Richard Draves, Jitendra Padhye, and Brian Zill. Comparison of routing metrics for static multi-hop wireless networks. In *SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 133–144, New York, NY, USA, 2004. ACM Press.

[24] Richard Draves, Jitendra Padhye, and Brian Zill. Routing in multi-radio, multi-hop wireless mesh networks. In *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 114–128, New York, NY, USA, 2004. ACM Press.

[25] T. ElBatt, T. Anderson, and B. Ryu. Performance evaluation of multiple access protocols for ad hoc networks using directional antennas. In *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, volume 2, pages 982–987 vol.2, 16-20 March 2003.

[26] Daniel Engels. *On the Design of Globally Unique Identification Schemes.* `http://www.autoidlabs.org/uploads/media/MIT-AUTOID-TM-007.pdf`, September 1st 2002. Accessed on May 23, 2008.

[27] Daniel W. Engels, , and Sanjay E. Sarma. Standardization requirements within the RFID Class Structure Framework, January 2005.

[28] *EPC website.* `http://www.epcglobalinc.org`. Accessed on May 23, 2008.

[29] Jakob Eriksson, Michalis Faloutsos, and Srikanth Krishnamurthy. Scalable ad hoc routing: the case for dynamic addressing. In *Proceedings of 23rd Annual Joint Conference on the IEEE and Coomunication Socities (Infocom)*, volume 2, pages 1108 –1119, March 2004.

[30] Klaus Finkenzeller. *RFID Handbook.* John Wiley and Sons Ltd., West Sussex, England, 2nd edition, 2001.

[31] Joseph Timothy Foley. *An infrastructure for electromechanical appliances on the Internet.* Massachusetts Institute of Technology, 1999. Master's Thesis.

[32] T. Fujii, T. Takahashi, T. Bandai, T. Udagawa, and T.Sasase. An Efficient MAC protocol in Wireless Ad-Hoc Networks with Heterogeneous Power Nodes. In *Proceedings of WPMC '02*, 2002.

[33] H. Gossain, C. Cordeiro, D. Cavalcanti, and D.P. Agrawal. The deafness problems and solutions in wireless ad hoc networks using directional antennas. In *Global Telecommunications Conference Workshops, 2004. GlobeCom Workshops 2004. IEEE*, pages 108–113, 29 Nov.-3 Dec. 2004.

[34] Hrishikesh Gossain, Carlos Cordeiro, Tarun Joshi, and Dharma P. Agrawal. Cross-layer directional antenna MAC protocol for wireless aed hoc networks. *Wireless Communications and Mobile Computing*, 6(2):171–182, 2006.

[35] Joseph M. Hellerstein, Wei Hong, and Samuel Madden. The sensor spectrum: technology, trends, and requirements. *SIGMOD Record*, 32(4):22–27, 2003.

[36] Jason Hill, Mike Horton, Ralph Kling, and Lakshman Krishnamurthy. The platforms enabling wireless sensor networks. *Commun. ACM*, 47(6):41–46, 2004.

[37] H.Labiod, H.Afifi, and C.De Santis. *Wi-Fi, Bluetooth, ZigBee and WiMAX*. Springer, 2007.

[38] Lingxuan Hu and David Evans. Using Directional Antennas to Prevent Wormhole Attacks. In *Proceedings of the Network and Distributed System Security S ymposium, NDSS 2004, San Diego, California, USA*. The Internet Society, 2004.

[39] Chritian Huitema. *IPv6: The New Internet Protocol*. Prentice Hall Inc., Upper Saddle River, New Jersey, 1996.

[40] IEEE. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999.

[41] *ISO Website*. `http://www.iso.org/iso/home.htm`. Accessed on May 23, 2008.

[42] David B. Johnson, David A. Maltz, and Yih-Chun Hu. The Dynamic Source Routing protocol for mobile ad hoc networks (DSR), April 2003.

[43] Joseph C. Liberti Jr. and Theodore. S. Rappaport. *Smart antennas for wireless communications :IS-95 and third generation CDMA applications*. Prentice Hall, 1999.

[44] Sang-Bo Ko and JeongWoo Jwa. A Dual-Tone DMAC Protocol for Mobile Ad Hoc Networks. *IEICE Transactions*, 90-B(2):354–357, 2007.

[45] K. Kobyashi and M.Nakagawa. Spatially divided channel scheme using sectored antennas for CSMA/CA - directional CSMA/CA. In *Proceedings of PIMRC*, 2000.

[46] Thanasis Korakis, Gentian Jakllari, and Leandros Tassiulas. A MAC protocol for full exploitation of directional antennas in ad-hoc wireless networks. In *MobiHoc '03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 98–107, New York, NY, USA, 2003. ACM.

[47] K.Sundaresan and R. Sivakumar. Ad-hoc Networks with Heterogeneous Smart Antennas: Performance Analysis and Protocols. *Wireless Communication and Mobile Computing Journal*, 2006.

[48] Martin Leopold, Mads Bondo Dydensborg, and Philippe Bonnet. Bluetooth and sensor networks: a reality check. In *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 103–113. ACM Press, 2003.

[49] Guoqing Li, Lily Yang, W. Steven Comer, and Bahareh Sadeghi. Opportunities and Challenges for Mesh Networks Using Directional Antennas. In *Proceedings of First IEEE Workshop on Wireless Mesh Networks*, pages 106–116, September 2005.

[50] Guoqing Li and L.L. Yang. On Utilizing Directional Antenna in 802.11 Networks: Deafness Study. *Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on*, 7-12 Jan. 2007.

[51] Yihu Li and Ahmed M. Safwat. Efficient Deafness Avoidance in Wireless Ad Hoc and Sensor Networks with Directional Antennas. In *PE-WASUN*, 2005.

[52] Kris Lin, Jennifer Yu, Jason Hsu, Sadaf Zahedi, David Lee, Jonathan Friedman, Aman Kansal, Vijay Raghunathan, and Mani Srivastava. Heliomote: enabling long-lived sensor networks through solar energy harvesting. In *SenSys '05:*

Proceedings of the 3rd international conference on Embedded networked sensor systems, pages 309–309. ACM Press, 2005.

[53] Henrik Lundgren, Erik Nordstrom, and Christian Tschudin. Coping with communication gray zones in IEEE 802.11b based ad hoc networks. In *WOWMOM '02: Proceedings of the 5th ACM international workshop on Wireless mobile multimedia*, pages 49–55, New York, NY, USA, 2002. ACM Press.

[54] Takata M., Bandai M., and Watanabe T. A Receiver-Initiated Directional MAC Protocol for Handling Deafness in Ad Hoc Networks. In *Proceedings of ICC 2006*, volume 9, pages 4089–4095, June 2006.

[55] Scott Meninger, Jose Oscar Mur-Miranda, Rajeevan Amirtharajah, Anantha Chandrakasan, and Jeffrey Lang. Vibration-to-electric energy conversion. In *ISLPED '99: Proceedings of the 1999 international symposium on Low power electronics and design*, pages 48–53, New York, NY, USA, 1999. ACM Press.

[56] P. Mockapetris. *Domain Names-Implementation and Specification.* IETF, `http://www.ietf.org/rfc/rfc1035.txt`, November 1987. Accessed on May 23, 2008.

[57] R. Moskowitz and P. Nikander. *Host Identity Protocol.* IETF, `http://www.ietf.org/rfc/rfc4423.txt`, May 2006. Accessed on May 23, 2008.

[58] *Motes-definition.* `http://www.intel.com/research/exploratory/motes.htm`. Accessed on May 23, 2008.

[59] C. Siva Ram Murthy and B.S.Manoj. *Ad Hoc Wireless Networks Architectures and Protocols.* Pearson Education, 2005.

[60] Marcos Augusto M.Vieira, Claudionor N. Coelho. Jr, Diogenes Cecilio da Silva Junior, and Jose M.da Mata. Survey on wireless sensor network devices. In *Emerging Technologies and Factory Automation(ETFA03). IEEE Conference*, pages 16–19, September 2003.

[61] Asis Nasipuri, Kai Lai, and Uma Reddy Sappidi. Power Consumption and Throughput in Mobile Ad Hoc Networks using Directional Antennas. In *11th International Conference on Computer Communications and Networks*, pages 620–626, October 2002.

[62] P. Nikander, J.Laganier, and F. Dupont. *A Non-Routable IPv6 Prefix for Keyed Hash Identifiers.* IETF, `http://tools.ietf.org/wg/ipv6/draft-laganier-ipv6-khi-00.txt`, September 2005. Accessed on May 23, 2008.

[63] *EPCglobal Object Name Service (ONS) 1.0.* `http://www.epcglobalinc.org/standards/ons/ons_1_0-standard-20051004.pdf`, April 2005. Accessed on May 23, 2008.

[64] Ian Oppermann, Matti Hamalainen, and Jari Iinatii. *UWB theory and applications.* Wiley, 2004.

[65] Ian Oppermann, Lucian Stoica, Alberto Rabbachin, Zack Shelby, and Jussi Haapola. UWB Wireless Sensor Networks: UWEN- A Practical Example. *IEEE Communications Magazine*, 42(12):27–32, December 2004.

[66] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, Feb 1999.

[67] Charles E. Perkins and David B. Johnson. Mobility support in IPv6. In *MobiCom '96: Proceedings of the 2nd annual international conference on Mobile computing and networking*, pages 27–37, New York, NY, USA, 1996. ACM Press.

[68] Joseph Polastre. Design and Implementation of Wireless Sensor Networks for Habitat Monitoring. Master's thesis, University of California, Berkeley, May 2003.

[69] Ravi Prakash. A Routing Algorithm for Wireless Ad Hoc Networks with Unidirectional Links. *ACM/Baltzer Wireless Networks Journal*, 7(6):617–626, November 2001.

[70] P.Vixie, S.Thomson, Y.Rekhter, and J.Bound. *Dynamic Updates in the Domain Name System (DNS UPDATE)*. IETF, `http://www.ietf.org/rfc/rfc2136.txt`, April 1997.

[71] *Qualnet Simulator*. `http://www.scalable-networks.com`. Accessed on May 23, 2008.

[72] J.M. Rabaey, M.J. Ammer, Jr. da Silva, J.L., D. Patel, and S. Roundy. PicoRadio supports ad hoc ultra-low power wireless networking. *Computer*, 33(7):42–48, Jul 2000.

[73] R. Ramanathan, J. Redi, C. Santivanez, D. Wiggins, and S. Polit. Ad hoc networking with directional antennas: a complete system solution. *Selected Areas in Communications, IEEE Journal on*, 23(3):496–506, March 2005.

[74] Ram Ramanathan. On the performance of ad hoc networks with beamforming antennas. In *MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pages 95–105, New York, NY, USA, 2001. ACM Press.

[75] S. Ray and D. Starobinski. On False Blocking in RTS/CTS-Based Multihop Wireless Networks. *IEEE Transactions on Vehicular Technology*, 56(2):849–862, March 2007.

[76] Siuli Roy, Somprakash Bandyopadhyay, Tetsuro Ueda, and Kazuo Hasuike. Multipath Routing in Ad Hoc Wireless Networks with Omni Directional and Directional Antenna: A Comparative Study. In *IWDC '02: Proceedings of the 4th International Workshop on Distributed Computing, Mobile and Wireless Computing*, pages 184–191, London, UK, 2002. Springer-Verlag.

[77] Sanjay E. Sarma, David L. Brock, and Kevin Ashton. *EPC Generation 1 Tag Data Standards.* `http://www.epcglobalinc.org/standards/tds/tds_1_1_rev_1_27-standard-20050510.pdf`. Accessed on May 23, 2008.

[78] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. *RFID Systems, Security and Privacy Implications.* `http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-014.pdf`, November 1st 2002. Accessed on May 23, 2008.

[79] Shinji Motegi and Kiyohito Yoshihara and Hiroki Horiuchi. Implementation and evaluation of on-demand address allocation for event-driven sensor network. In *Proceedings of the 2005 Symposium on Applications and the Internet (SAINT'05)*, pages 352–360, February 2005.

[80] Alex Snoeren and Hari Balakrishnan. An End-to-End Approach to Host Mobility. In *6th ACM MOBICOM*, Boston, MA, August 2000.

[81] K. Sollins and L. Masinter. *Functional Requirements for Uniform Resource Names.* IETF, `http://www.ietf.org/rfc/rfc1737.txt`, December 1994. Accessed on May 23, 2008.

[82] I. Stark. Invited talk: Thermal energy harvesting with thermo life. In *Wearable and Implantable Body Sensor Networks, 2006. BSN 2006. International Workshop on*, pages 19–22, 3-5 April 2006.

[83] Ion Stoica, Daniel Adkins, Shelley Zhuang, Scott Shenker, and Sonesh Surana. Internet indirection infrastructure. In *SIGCOMM '02: Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 73–86, New York, NY, USA, 2002. ACM Press.

[84] Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, and Hari Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In *SIGCOMM '01: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 149–160, New York, NY, USA, 2001. ACM Press.

[85] Anand Prabhu Subramanian and Samir R. Das. Addressing Deafness and Hidden Terminal Problem in Directional Antenna based Wireless Multi-Hop Networks. In *Second International Conference on COMmunication System softWAre and MiddlewaRE (COMSWARE 2007)*, Bangalore, India, January 2007.

[86] Mineo Takai, Jay Martin, Rajive Bagrodia, and Aifeng Ren. Directional virtual carrier sensing for directional antennas in mobile ad hoc networks. In *Proceedings of MobiHoc '02*, pages 183–193, 2002.

[87] Mineo Takai, Junlan Zhou, and Rajive Bagrodia. Adaptive range control using directional antennas in mobile ad hoc net works. In *MSWIM '03: Proceedings of the 6th ACM international workshop on Mo deling analysis and simulation of wireless and mobile systems*, pages 92–99, New York, NY, USA, 2003. ACM Press.

[88] Masanori Takata, Masaki Bandai, and Takashi Watanabe. An Extended Directional MAC for Location Information Staleness in Ad Hoc Networks. In *25th IEEE International Distributed Computing Systems Workshops*, pages 899–905, June 2005.

[89] Sameer Tilak, Nael B. Abu-Ghazaleh, and Wendi Heinzelman. A taxonomy of wireless micro-sensor network models. *SIGMOBILE Mob. Comput. Commun. Rev.*, 6(2):28–36, 2002.

[90] Brett Warneke, Matt Last, Brian Liebowitz, and Kristofer S. J. Pister. Smart Dust: Communicating with a Cubic-Millimeter Computer. *IEEE Computer*, 34(1):44–51, 2001.

[91] Mark Yarvis, Nandakishore Kushalnagar, Harkirat Singh, Anand Rangarajan, York Liu, and Suresh Singh. Exploiting Heterogeneity in Sensor Networks. In *Proceedings of IEEE INFOCOM*, 2005.

[92] A. K. Yeo, A. L. Ananda, and E. K. Koh. A taxonomy of issues in name systems design and implementation. *SIGOPS Oper. Syst. Rev.*, 27(3):4–18, 1993.

[93] Su Yi, Yong Pei, and Shivkumar Kalyanaraman. On the capacity improvement of ad hoc wireless networks using directional antennas. In *MobiHoc '03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 108–116, New York, NY, USA, 2003. ACM Press.

[94] ZigBee SIG, Inc., `http://www.zigbee.org`. *ZigBee Website.* Accessed on May 23, 2008.