國 立 交 通 大 學

電信工程學系

碩 士 論 文

無線隨意網路多重擇路協定

Multicast Routing Protocols for Mobile Ad Hoc Networks

研究生：溫中義

指導教授：方凱田

中 華 民 國 95 年 6 月

無線隨意網路多重擇路協定

Multicast Routing Protocols for Mobile Ad Hoc Networks

研究生：溫中義　　Student：Chung-Yi Wen

指導教授：方凱田　　Advisor：Kai-Ten Feng

國立交通大學

電信工程學系碩士班

碩士論文

A Thesis
Submitted to Department of Communication Engineering
College of Electrical and Computer Engineering
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of
Mater of Science
in Communication Engineering
June 2006
Hsinchu, Taiwan, Republic of China

中華民國 95 年 6 月

無線隨意網路多重擇路協定

學生：溫中義　　　　　　　　　　指導教授：方凱田

國立交通大學電信工程學系碩士班

摘　　要

在無線隨意網路中，對於支援多重傳輸應用的需求越來越增加，在多重傳輸裡其中一個我們關切的議題為擇路協定的設計，普遍來說多重擇路協定可以區分為樹狀結構和網狀結構，在不同的網路環境情況下，兩種類型的擇路協定分別有各自的優點和缺點。

在本論文中，兩種改善的多重擇路協定被提出。PCHMR 協定同時結合了樹狀結構以及網狀結構，同時路徑決定機制中除了路徑上的節點數之外，還把接收信號的強度一併考慮。ORODMR 協定則利用接收節點的資訊，減少了傳統 ODMRP 協定中所需傳送的額外控制封包量，ORODMR 協定保留了原始 ODMRP 協定的優點，同時去改善 ODMRP 協定為人所詬病的其一主要缺陷。透過模擬，在不同的節點移動模式和網路狀況下，評估提出協定的效用。

Multicast Routing Protocols for Mobile Ad Hoc Networks

Student：Chung-Yi Wen Advisor：Kai-Ten Feng

Department of Communication Engineering
National Chiao Tung University

Abstract

There has been an increasing demand for applications to support multicast communication in the mobile ad hoc networks. One of the primary concerns in the multicast communication is the feasible design of the multicast ad hoc routing protocols. Conventionally, the design of the multicast routing protocols can be categorized into the tree-based and the mesh-based schemes. These two types of protocols have their own strength and weakness under different networking scenarios.

In this thesis, two multicast routing protocols are proposed. A Power-Controlled Hybrid Multicast Routing (PCHMR) protocol is a hybrid scheme, which consists of both the tree-based and the mesh-based structures. The route determination scheme of the PCHMR algorithm not only relies on the hop counts but also on the received power strength of the neighborhood nodes. The proposed PCHMR algorithm is suitable for the dynamically changing network topologies, especially for the group mobility scenario. On the other hand, a Overhead-Reduced On Demand Multicast Routing (ORODMR) protocol, which reduces the control overhead in the conventional ODMRP algorithm, is proposed. The ORODMR protocol uses the information from the multicast receivers to reduce the control overheads effectively. The ORODMR algorithm keeps the advantages of the original ODMRP algorithm and improves one of its primary drawbacks. Different conditions associated with the mobility models are utilized in the simulations to evaluate the effectiveness of both the PCHMR and the ORODMR algorithms.

誌　謝

兩年的研究所生活在這本論文完成的同時，也畫上了句點。首先要感謝指導教授方凱田老師，在研究的過程中提供許多的建議，固定的討論讓自己的構思能夠更完備，也從實驗室定期的報告訓練中獲益良多。同時感謝交通大學電信系廖維國教授和資工系趙禧綠教授，撥空來參加口試並給予很多實質的建議，使得論文更趨完整。

感謝給予我無代價支持的家人，老爸、大姐、二姐和恩妹，分享生活中的喜更分享生活中的悲，家人讓我知道永遠都會有人在支持我，當然還有親密的叔叔和嬸嬸們，我愛你們。感謝陪伴我最多的麗娟，經由妳的心，讓自己更加成長；感謝從高中、大學或者是研究所開始一起努力的同學們，阿龜、阿智、雄光、雄仔、俗瑋、小馬、Oreal、冠風、小華、Q仔、阿魯咪、尼可、阿哲、Kinki、士琦，很高興認識了你們，也不會忘記你們帶給我一頁又一頁的回憶；感謝在生活中給予我不同感受的朋友們，惠純、愛恆的大家、Katy、小瑩、達西亞，有別於理工科的視野，妳們豐富了生活；感謝實驗室的學長學弟們，仲賢、澤恩、昭霖、文炫、文俊、裕彬、Tino、Walker；感謝忘了在誌謝裡提到的你(妳)們。你們的陪伴和支持讓我有勇氣繼續往人生下個階段挑戰，你們的肯定和教導讓我知道自己的無限可能，各位親愛的，我畢業了！:)

溫中義謹誌 于交通大學 2006/06

Contents

List of Figures

Chapter 1

Introduction

A Mobile Ad hoc NETwork (MANET) consists of wireless Mobile Nodes (MNs) that cooperatively communicate with each other without the existence of infrastructure networks. Fig. 1.1 and Fig. 1.2 illustrate the differences between the ad hoc network and the infrastructure network. Depending on different geographical topologies, the MNs are dynamically located and continuously changing their locations. The fast-changing characteristics in MANETs make it difficult to discover routes between the MNs. It is important to design efficient and reliable routing protocols to maintain, discover, and organize the routes in MANETs.

The proposed Power-Controlled Hybrid Multicast Routing (PCHMR) protocol constructs a hybrid network structure that combines the tree-based and the mesh-based topologies. The proposed hybrid structure effectively adjusts itself by considering the robustness and efficiency under different network scenarios. Moreover, in most of the existing multicast routing protocols, the routing decisions depend on the minimal hop counts between the MNs in consideration. It is recognizable that the route with the smallest hop counts does not guarantee the robustness of the route [1]. In the proposed PCHMR algorithm, not only the hop counts but also the receiving signal power between the MNs are exploited to decide which route should be selected.The simulation results show that the proposed PCHMR protocol effectively provides better performance comparing with the existing tree-based multicast routing protocol.

In a mobile environment, any reduction in control overhead is a significant advantage for

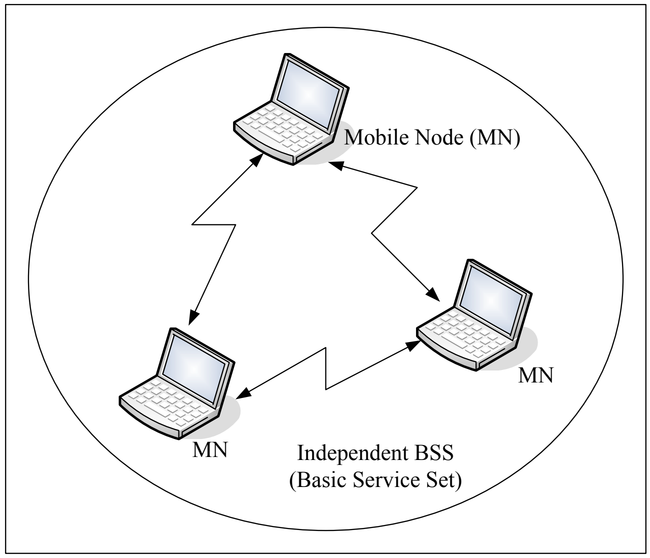


Figure 1.1: Ad Hoc Network Configuration

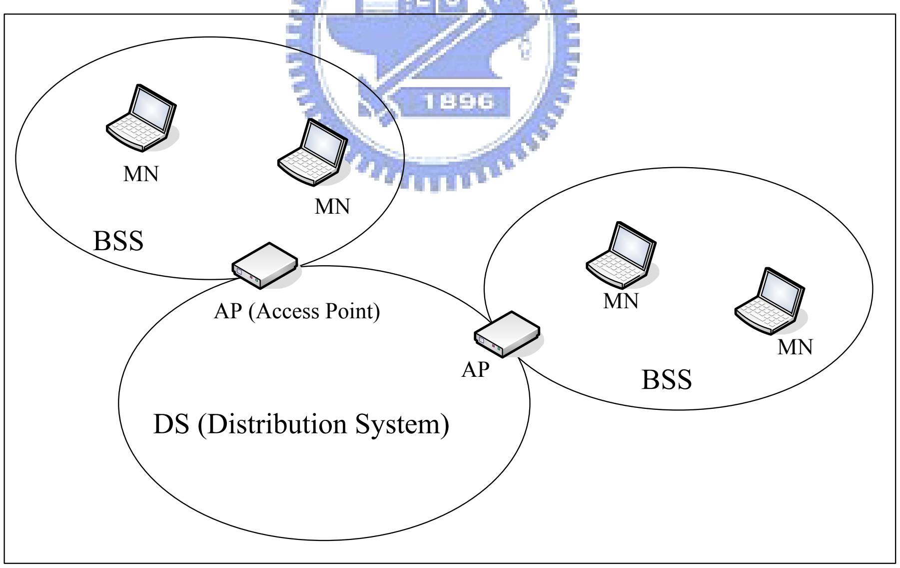


Figure 1.2: Infrastructure Network Configuration

a multicast routing protocol. In this thesis, the second proposed Overhead-Reduced On Demand Multicast Routing (ORODMR) algorithm intends to reduce the amount of the control packets that are necessary to maintain the network connectivity. Redundant data and control packets are propagated in a mesh structure. This distinguishing feature makes mesh protocols more robust but causes unnecessary bandwidth waste in the same time. In the ORODMR algorithm, the multicast receiver information is utilized to reduce the redundant packet deliveries. The receiver information is known by all forwarding group members but seldom multicast routing protocols use it. The simulation results show that the proposed ORODMR algorithm effectively reduces the control overheads and it does not sacrifice much packet delivery ratio or other connectivity performances, especially when the network environment is changed severely.

The remainder of this thesis is organized as follows. Chapter 2 shows the related works that includes the physical layer, the medium access control sub-layer, and the routing partition in the network layer. Two existing multicast routing protocols, the ODMRP and the MAODV protocols, are introduced in Chapter 3. The proposed PCHMR and ORODMR algorithms are presented in chapter 4, which includes the design concepts and the details of the proposed algorithms. Chapter 5 firstly describe the mobility models and the signal propagation models that are employed in the simulations, and then the simulation parameters and the performance evaluation are followed. Chapter 6 draws the conclusions.

Chapter 2

Backgrounds

The Open Systems Interconnection Reference Model (OSI Model) divides the functions of a system into a series of layers. Each layer has the property that it only uses the functions of the layer below, and only exports functionality to the layer above. A system that implements protocol behavior consisting of a series of these layers is known as a ”protocol stack” or a ”stack”. Protocol stacks can be implemented either in hardware or software, or a mixture of both. Typically, only the lower layers are implemented in hardware, with the higher layers being implemented in software. Fig. 2.1 shows a typical architecture in networks and it is noted that the presentation layer and the session layer are combined in the application layer. For mobile ad hoc networks, we are interested in the physical layer, the MAC (medium access control) sub-layer, and the network layer (e.g. routing and path determination). These three layers (or sub-layers) are introduced in Section 2.1, Section 2.2, and Section 2.3, respectively.

It is noted that the trends of the protocol stack configuration have changed recently [2] [3]. The protocol stack concept is convenient for the network engineers to divide the entire design into clear portions. As the network techniques has become more and more complete, the extra interconnection between protocol stacks plays a more critical role in performance improvement. The cross-layer design is a whole new concept. The idea breaks the independent layer stack method and combines the adjacent layer protocols. The cross-layer design gives us more opportunity to optimize the performance since the control overheads obviously reduced

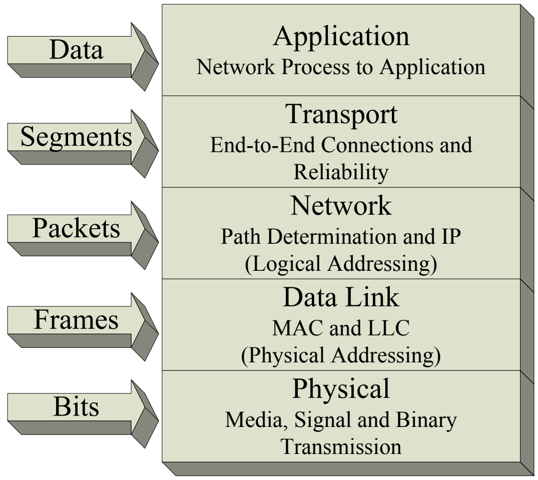


Figure 2.1: The OSI (Open Systems Interconnection) Model Architecture

comparing with the layered-type architecture.

2.1 Physical Layer

The Physical layer defines all the electrical and physical specifications for devices. This includes the layout of pins, the voltages, and the cable specifications. For example, hubs and repeaters are physical-layer devices. The major functions and services performed by the physical layer are:

- Establishment and termination of a connection to a communications medium.
- Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.
- Modulation, or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel.

The major IEEE (Institute of Electrical and Electronics Engineers, Inc.) 802.11 physical layer specifications (i.e. 802.11 legacy, 802.11b, 802.11a, and 802.11g) are illustrated in Subsection 2.1.1. In additional to that, three different radio propagation models that simulate the

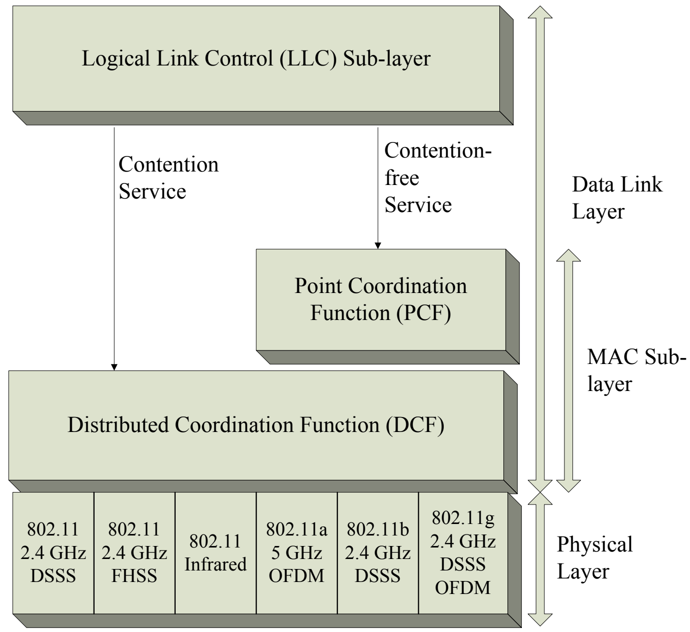


Figure 2.2: IEEE 802.11 Protocol Architecture

real signal propagation environment are followed in Subsection 2.1.2. The radio propagation model plays an important role in the simulation results.

2.1.1 IEEE 802.11

The IEEE 802.11, the Wi-Fi standard, denotes a set of Wireless Local Area Network (WLAN) standards developed by working group 11 of the IEEE LAN/MAN Standards Committee. The term also used to refer as the original 802.11, which is now called ”802.11 legacy”. After the release of the 802.11 specification in June 1997, three popular physical layer techniques in the 802.11 family defined by the 802.11a, 802.11b and 802.11g are released. Fig. 2.2 shows the 802.11 protocol architecture.

802.11 legacy

The IEEE 802.11 draft specification [4] calls for three different physical-layer implementations: the Frequency Hopping Spread Spectrum (FHSS), the Direct Sequence Spread Spectrum (DSSS), and the IR. The FHSS utilizes the 2.4 GHz Industrial, Scientific, and Medical (ISM) band (i.e. 2.4000 $\sim$ 2.4835 GHz).

For the FHSS, the basic access rate of 1 Mb/s uses the two-level Gaussian Frequency Shift Keying (GFSK), where a logical 1 and a logical 0 are encoded using different frequencies. The enhanced access rate of 2 Mb/s uses the four-level GFSK, where 2 bits are encoded at a time using four frequencies. The DSSS also uses the 2.4 GHz ISM frequency band, where the 1 Mb/s basic rate is encoded using the Differential Binary Phase Shift Keying (DBPSK), and a 2 Mb/s enhanced rate uses the Differential Quadrature Phase Shift Keying (DQPSK). The IR specification identifies a wavelength range from 850 to 950 nm. The IR band is designed for indoor use only and operates with non-directed transmissions. The IR specification was designed to enable stations to receive line-of-site and reflected transmissions. Encoding of the basic access rate of 1 Mb/s is performed using the 16-Pulse Position Modulation (PPM), where 4 data bits are mapped to 16 coded bits for transmission. The enhanced access rate (2 Mb/s) is performed using 4-PPM modulation, where 2 data bits are mapped to 4 coded bits for transmission.

802.11b

The 802.11b [5] [6] amendment to the original standard was ratified in 1999 and it is a direct extension of the DSSS modulation technique defined in the original standard. The 802.11b standard uses the Complementary Code Keying (CCK) as its modulation technique, which is a variation on CDMA (Code Division Multiple Access). 802.11b cards can operate at 11 Mbit/s, but will scale back to 5.5, then 2, then 1 Mbit/s (a.k.a Adaptive Rate Selection) if signal quality becomes an issue. Since the lower data rates use less complex and more redundant methods of encoding the data, they are less susceptible to corruption due to interference and signal attenuation. Extensions have been made to the 802.11b protocol (e.g., channel bonding and burst transmission techniques) in order to increase the speed to 22, 33, and 44 Mbit/s, but the extensions are proprietary and have not been endorsed by the IEEE. Many companies call enhanced versions "802.11b+". These extensions have been largely obviated by the development of the 802.11g, which has data rates up to 54 Mbit/s and is backwards-compatible with the 802.11b.

802.11a

The 802.11a [7] [6] amendment to the original standard was ratified in 1999. The 802.11a standard uses the same core protocol as the original standard, which operates in 5 GHz band. It uses a 52-subcarrier Orthogonal Frequency-Division Multiplexing (OFDM) with a maximum raw data rate of 54 Mbit/s, which yields realistic net achievable throughput in the mid-20 Mbit/s. The data rate is reduced to 48, 36, 24, 18, 12, 9, and then 6 Mbit/s if required. The 802.11a has 12 non-overlapping channels, 8 dedicated to indoor, and 4 to point-to-point. It is not inter-operable with 802.11b, except if using equipment that implements both standards.

Since the 2.4 GHz band is heavily used, using the 5 GHz band gives 802.11a the advantage of less interference. However, this high carrier frequency also brings disadvantages. It restricts the use of 802.11a to almost line of sight, necessitating the use of more access points; it also means that 802.11a cannot penetrate as far as 802.11b since it is absorbed more readily.

The 802.11a products started shipping in 2001, lagging the 802.11b products due to the slow availability of the 5 GHz components needed to implement products. The 802.11a was not widely adopted overall because the 802.11b was already widely adopted, because of 802.11a's disadvantages, because of poor initial product implementations which making its range even shorter, and because of regulations. Manufacturers of the 802.11a equipment responded to the lack of market success by improving the implementations (current-generation 802.11a technology has range characteristics much closer to those of 802.11b), and by making the technology that can use more than one 802.11 standard. There are dual-band, or dual-mode, or tri-mode cards that can automatically handle 802.11a and b, or a, b and g, as available. Similarly, there are mobile adapters and access points which can support all these standards simultaneously.

802.11g

In June 2003, a third modulation standard was ratified: the 802.11g [8] [6]. This flavorous works in the 2.4 GHz band (like the 802.11b) but operates at a maximum raw data rate of 54 Mbit/s, or about 24.7 Mbit/s net throughput like the 802.11a. The 802.11g hardware will work with the 802.11b hardware. The modulation scheme used in the 802.11g is the Orthogonal Frequency Division Multiplexing (OFDM) for the data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s. It reverts to (like the 802.11b standard) CCK for 5.5 and 11 Mbit/s and DBPSK/DQPSK+DSSS for 1 and 2 Mbit/s. Even though the 802.11g operates in the same frequency band as the 802.11b, it can achieve higher data rates because of its similarities to the 802.11a. The maximum range of 802.11g devices is slightly greater than that of 802.11b devices. But the range in which a client can achieve full (54 Mbit/s) data rate speed is much shorter than that of the 802.11b.

2.1.2 Radio Propagation Models

In this section, three radio propagation models including the free space model, the two-ray ground reflection model, and the shadowing model are described [9]. The radio propagation models are used to calculate the received signal power of each packet. At the physical layer of each Mobile Node (MN), there is a receiving threshold. When a packet is received, if its signal power is below the receiving threshold, it is marked as error and is dropped by the MAC sub-layer. On the other hand, if the received signal power is above the receiving threshold, the packet is treated normally.

Free Space Model

The free space propagation model represents the ideal propagation condition. It assumes that there is only one clear Line-Of-Sight (LOS) path between the transmitter and the receiver. Fig. 2.3 shows that the free space model basically represents the communication range as a circle around the transmitter. If a receiver is within the circle, it receives all packets. Otherwise, it loses all packets. H. T. Friis calculated the received signal power in free space

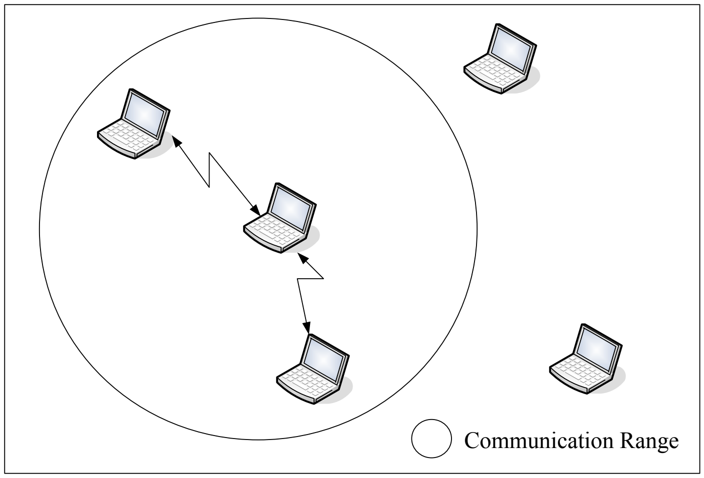


Figure 2.3: The Free Space Propagation Model

at distance d from the transmitter using the following equation [10]:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \tag{2.1}$$

where P_t is the transmitted signal power. G_t and G_r are the antenna gains of the transmitter and the receiver respectively. L ($L \geq 1$) is the system loss, and λ is the wavelength.

Two-Ray Reflection Model

A single LOS path between two MNs is seldom the only propagation path. The situation that there are two or more propagation paths between two MNs is more reasonable. The two-ray ground reflection model considers both the direct path and a ground reflection path as shown in Fig. 2.4. It is shown that this model gives more accurate prediction at a long distance than the free space model. [11] The received power at distance d is calculated as

$$P_r(d) = \frac{P_t G_t G_r {h_t}^2 {h_r}^2}{d^4 L} \tag{2.2}$$

where h_t and h_r are the heights of the transmitting and the receiving antennas respectively. The above equation shows that the two-ray reflection model has a faster power loss than the

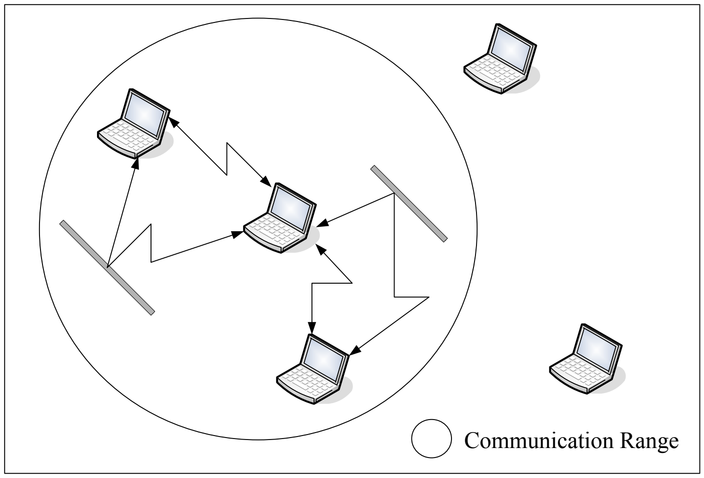


Figure 2.4: The Two-Ray Reflection Propagation Model

free space model when the distance increases.

However, the two-ray reflection model still can not simulate the real propagation environment. It does not give a good result for a short distance due to the oscillation caused by the constructive and the destructive combination of the two rays. Therefore the free space model is still used when d is small. A cross-over distance d_c is calculated as a threshold factor. When $d < d_c$, Eqn. (2.1) is used. When $d \geq d_c$, Eqn. (2.2) is used. Because Eqns. (2.1) and (2.2) give the same result at the cross-over distance, d_c can be calculated as

$$\frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d_c^2 L} = \frac{P_t G_t G_r {h_t}^2 {h_r}^2}{d_c^4 L} \Rightarrow d_c = \frac{4\pi h_t h_r}{\lambda} \tag{2.3}$$

Shadowing Model

The free space model and the two-ray reflection model predict the received power as a deterministic function of the distance. They both represent the communication range as an ideal circle. In reality, the received power at a certain distance is a random variable due to multi-path propagation effects, which is also known as fading effects. In fact, the above two models predict the mean received power at the distance d. The shadowing model extends the ideal circle model to a statistic model: MNs can only probabilistically communicate when

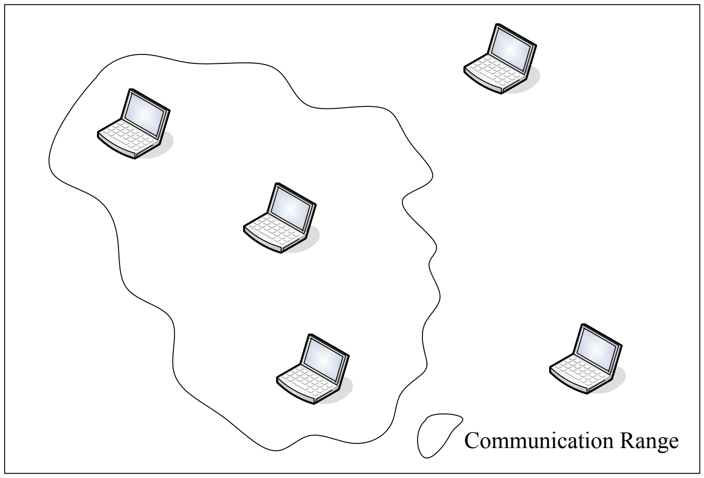


Figure 2.5: The Shadowing Propagation Model

near the edge of the communication range as Fig. 2.5.

Table 2.1 Some Typical Values of Shadowing Deviation σ_{dB}

Environment	σ_{dB}
Outdoor	4 to 12
Office, hard partition	7
Office, soft partition	9.6
Factory, line-of-sight	3 to 6
Factory, obstructed	6.8

In the shadowing model the received signal power in dB at the distance d is as follow:

$$[\frac{P_r}{P_r(d_0)}]_{dB} = -10\beta log(\frac{d}{d_0}) + X_{dB} \tag{2.4}$$

where d_0 is the close-in distance and $P_r(d_0)$ can be computed from Eqn. (2.1). X is a Gaussian random variable with zero mean and standard deviation σ_{dB}. X_{dB} reflects the variation of the received signal power at a certain distance. σ_{dB} and β is called the shadowing deviation and the path loss exponent respectively, and their value are usually empirically determined by field measurements. Table 2.1 and 2.2 give some typical values of σ_{dB} and β. Larger β values correspond to more obstructions and hence faster decrease in the average received power as the distance becomes larger.

Table 2.2 Some Typical Values of Path Loss Exponent β

Environment	β
Outdoor	
Free space	2
Shadowed urban area	2.7 to 5
In building	
Line-of-sight	1.6 to 1.8
Obstructed	4 to 6

2.2 Medium Access Control Sub-layer

The original 802.11 standard defines the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the media access method [4]. The MAC sub-layer is responsible for the channel allocation procedures, Protocol Data Unit (PDU) addressing, frame formatting, error checking, and fragmentation and reassembly. The transmission medium can operate in the contention mode exclusively, requiring all Mobile Nodes (MNs) to contend for access to the channel for each packet transmitted. The medium can also alternate between the contention mode, known as the Contention Period (CP), and a Contention-Free Period (CFP). During the CFP, the medium usage is controlled (or mediated) by the Access Point (AP), thereby eliminating the need for MNs to contend for channel access. The IEEE 802.11 supports three different types of frames: management, control, and data. The management frames are used for MN association and disassociation with the AP, timing and synchronization, and authentication and de-authentication. Control frames are used for handshaking during the CP, for positive acknowledgments during the CP, and to end the CFP. Data frames are used for the transmission of data during the CP and the CFP, and can be combined with polling and acknowledgments during the CFP.

2.2.1 Distributed Coordination Function

The Distributed Coordination Function (DCF) is the fundamental access method used to support asynchronous data transfer on a best effort basis. All MNs must support the DCF in the 802.11. The DCF operates solely in the ad hoc network, and either operates solely or coexists with the PCF in an infrastructure network. The MAC architecture is interpreted in Fig. 2.2, where it is shown that the DCF sits directly on top of the physical layer and supports contention services. Contention services promote fair access to the channel for all MNs. The DCF is based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CD (Collision Detection) is not used because a MN is unable to listen to the channel for collisions while transmitting. In the IEEE 802.11, the carrier sensing is performed at both the air interface, referred to as physical carrier sensing, and at the MAC sub-layer, referred to as virtual carrier sensing. The physical carrier sensing detects the presence of other IEEE 802.11 WLAN users by analyzing all detected packets, and also detects activity in the channel via relative signal strength from other sources.

A source MN performs the virtual carrier sensing by sending MPDU (MAC Protocol Data Unit) duration information in the header of Request To Dend (RTS), Clear To Send (CTS), and data frames. An MPDU is a complete data unit that is passed from the MAC sub-layer to the physical layer. The duration field indicates the amount of time (in microseconds) after the end of the present frame the channel will be utilized to complete the successful transmission of the data or management frame. Other MNs use the information in the duration field to adjust their Network Allocation Vector (NAV), which indicates the amount of time that must elapse until the current transmission session is complete and the channel can be idle status again. The channel is marked busy if either the physical or the virtual carrier sensing mechanism indicates the channel is busy.

Priority access to the wireless medium is controlled through the use of Inter-Frame Space (IFS) time intervals between the transmission of frames. The IFS intervals are mandatory idle time periods of the transmission medium. There are three kinds of IFS intervals : Short IFS (SIFS), Point Coordination Function IFS (PIFS), and DCF-IFS (DIFS). The SIFS interval is

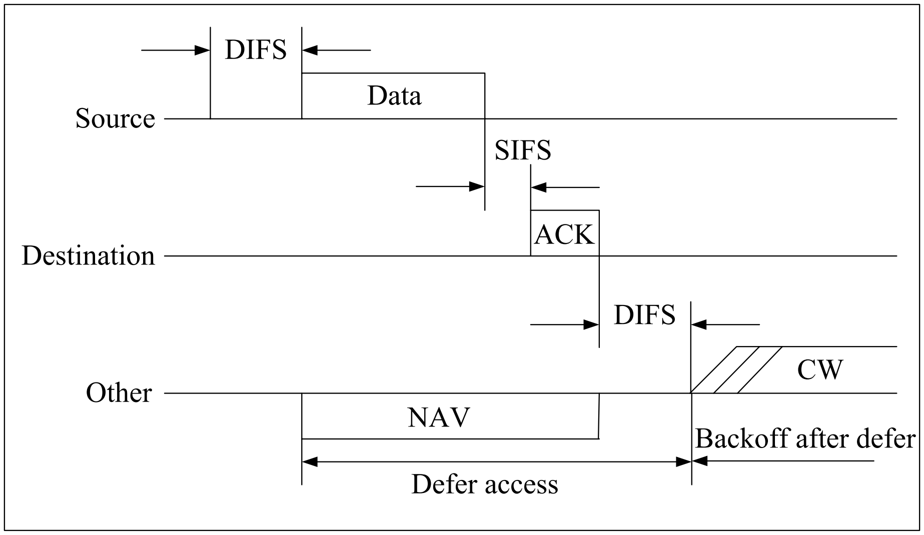


Figure 2.6: Basic Data Frame Transmission Timing Diagram

the smallest IFS, followed by the PIFS and the DIFS, respectively. MNs required to wait a shorter IFS have priority access over those MNs required to wait a longer IFS before transmitting. Fig. 2.6 is a basic data frame access method transmission timing diagram. When a MN senses the channel is idle, the MN waits for a DIFS period and experiments the channel again. If the channel is still idle, the MN transmits an MPDU. The receiving MN calculates the checksum and determines whether the packet was received correctly. Upon receipt of a correct packet, the receiving MN waits a SIFS interval and transmits a ACKnowledgment frame (ACK) back to the source MN, indicating that the transmission was successful. When the data frame is transmitted, the duration field of the frame is used to let all MNs in the Basic Service Set (BSS) know how long the medium will be busy. All MNs hearing the data frame adjust their NAV based on the duration field value, which includes the SIFS interval and the ACK following the data frame.

However a source MN in a BSS cannot hear whether a collision occurs during its own transmissions. Instead, the source continues transmitting the complete MPDU. If the MPDU is large, a lot of channel bandwidth is wasted due to a corrupt MPDU. The RTS and the CTS control frames can be used by a MN to reserve channel bandwidth prior to the an actual

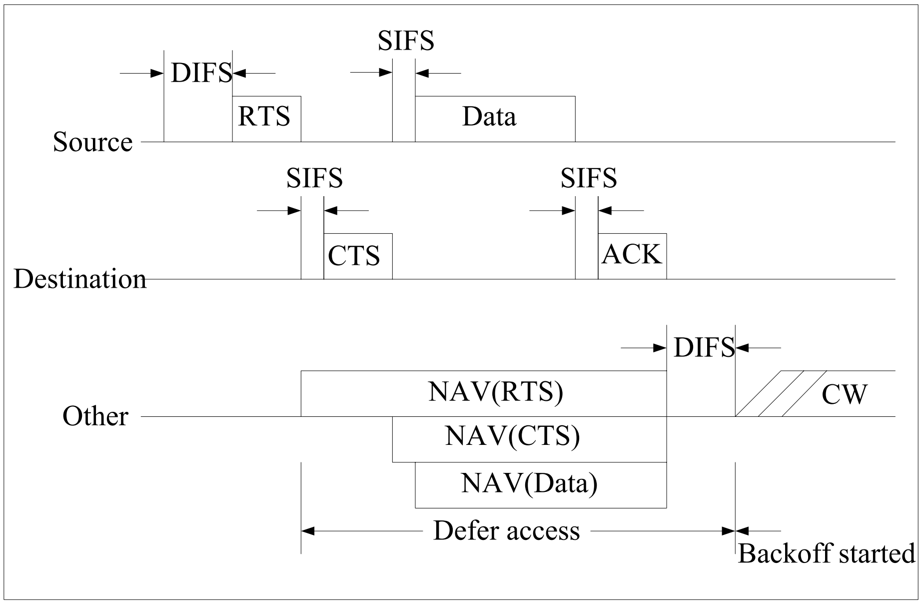


Figure 2.7: Transmission of an MPDU using RTS/CTS

MPDU transmission. The additional control overhead is acceptable because the RTS and the CTS control frames are relatively small (the RTS is 20 octets and the CTS is 14 octets) compared to the maximum data frame size (2346 octets). The source MN (after successfully contending for the channel) first transmits the RTS frame to a specified destination MN. All other MNs in the BSS, hearing the RTS packet, read the duration field and set their NAVs accordingly. The destination MN responds to the RTS packet with a CTS packet after an SIFS idle period. MNs hearing the CTS packet check the duration field and again update their NAV. Upon successful reception of the CTS, the source MN is virtually assured that the medium is stable and reserved for successful transmission of the MPDU. The use of the RTS and the CTS helps to combat the "hidden terminal" problem. Fig. 2.7 illustrates the transmission of an MPDU using the RTS/CTS mechanism.

The collision avoidance portion of CSMA/CA is performed through a random backoff procedure. The idle period after a DIFS period is referred to as the Contention Window (CW). Every MN in the CW computes a random backoff time. The random backoff time is an integer value that corresponds to a number of time slots. For the IEEE 802.11, time is slotted in time periods. Unlike slotted Aloha, where the slot time is equal to the transmission

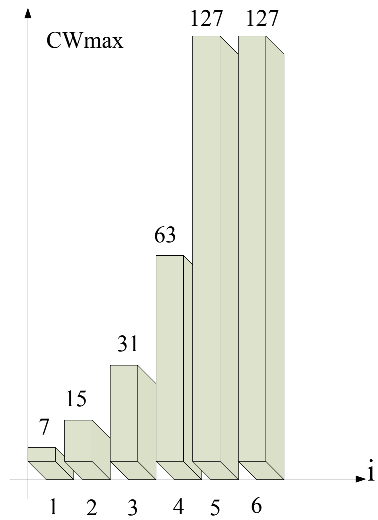


Figure 2.8: Binary Exponential Backoff Algorithm

time of one packet, the slot time used in the IEEE 802.11 is much smaller than an MPDU and is used to define the IFS intervals and determine the backoff time for MNs in the CP. Initially, the MN computes a backoff time in the range of 0 to 7. After the medium becomes idle after a DIFS period, MNs decrement their backoff timer until the medium becomes busy again or the timer reaches zero. If the timer has not reached zero and the medium becomes busy, the MN freezes its timer. When the timer is decremented to zero, the MN transmits its frame. If two or more MNs decrement to zero at the same time, a collision will occur. Each MN will have to generate a new backoff time in the range of 0 to 15. For each retransmission attempt, the backoff time grows as $\lfloor 2^{2+i} \cdot ranf() \rfloor \cdot SlotTime$, where i is the consecutive number of times a MN attempts to send an MPDU, $ranf()$ is a uniform random variate in (0,1), and $\lfloor M \rfloor$ represents the largest integer less than or equal to M. Fig. 2.8 shows the CW_{max} of the binary exponential backoff algorithm. The advantage of this channel access method is that it promotes fairness among the MNs. The fairness is maintained because each MN must recounted for the channel after every transmission of an MPDU. All MNs have equal probability of gaining access to the channel after each DIFS interval. However, there is no mechanism to guarantee minimum delay to MNs supporting time-bounded services with the DCF.

2.2.2 Point Coordination Function

The Point Coordination Function (PCF) provides the Contention-Free (CF) frame transfer and the PCF is only usable on the infrastructure network configurations. The PCF relies on the Point Coordinator (PC) to perform polling, enabling polled MNs to transmit without contending for the channel. The function of the PC is performed by the AP within each BSS. The infrastructure network configuration is not the concern in this thesis, instead the ad hoc network configurations, so there are no more descriptions about PCF.

2.3 Network Layer

In this thesis, routing (i.e. the path determination) protocols in the network layer are focused. When a Mobile Node (MN) wants to send a packet to another, this causes a packet delivery session to start. If the two MNs are in each other's transmission range, they can communicate with each other directly without other MNs' relays. Unfortunately, the sender node and the destination node are likely not close enough to communicate directly in most situations. In mobile ad hoc networks, the packet deliveries are depending on relay nodes' connectivity. The route determination is important because the relay node along the route path decide the packet delivery performances. There are three kinds of transmission categories: unicast (ont-to-one), multicast (many-to-many or one-to-many), and broadcast (one-to-all). Firstly, the unicast applications attracts researchers to be involved in the related studies. Many unicast routing protocols have been developed and these unicast routing protocols can be categorized into the proactive algorithms (such as DSDV [12] and WRP [13]), the reactive algorithms (such as TORA [14] [15], DSR [16], AODV [17], ABR [18] and SSA [19]) and the hybrid algorithms (such as ZRP [20]). Unicast routing protocol only supports the one node to one node service. Therefore, the applications are restricted.

With the fast growth in the applications that require multicast communication (i.e. one-to-many or many-to-many communication), a great amount of attention has been received in the design of the multicast ad hoc routing protocols. Protocols used in static networks, such as DVMRP [21], MOSPF [22], CBT [23], and PIM [24], are not suitable in a dynamically changing ad hoc network environment. Therefore, new multicast routing algorithms are needed to be designed. Different types of multicast routing protocols have been proposed in many research studies. Basically, these protocols can be categorized into the tree-based (such as MAODV, AMRIS, AMRoute, and GS) and the mesh-based (such as ODMRP, CAMP, and MCEDAR) algorithms. The MAODV protocol [25] is extended from the unicast AODV [17] routing algorithm for multicast communication. The on-demand routes are discovered from the originator to the multicast tree if it intends to join the tree. The AMRIS protocol [26] dynamically assigns each MN with an id-number in a multicast session. These id-numbers help the MN leave or join a multicast session and adapt rapidly to changes in the route connectivity. Core-based share trees are utilized in both the AMRoute [27] and the GS [28] algorithms to provide adaptation to the network changes. The ODMRP [29] protocol utilizes the forwarding group concept to construct its mesh topology. The CAMP [30] and the MCEDAR [31] [32] protocols generalize the idea of the core-based trees into the multicast meshes to provide richer connectivity than the tree-based structure.

The fundamental topology of the tree-based network originates from a root which spreads out its branches and the corresponding sub-branches. The benefit of using the tree-based structure is its simplicity without requiring enormous system resources for maintaining the structure. The tree-based structure, which allows reasonable amount of MNs within the network, is suitable to be applied in static network topology. For rapidly changed networks, however, the communication links between the MNs become fragile, which results in a great amount of cost for link repairing. On the other hand, there are comparably more communication linkages between the MNs in the mesh-based topology, which provides robust connectivity comparing with the tree-based networks. The mesh-based structure is suitable to be utilized in fast-changing network topologies. However, the inherent complication in the mesh-based structure makes it consumes more system resources and therefore sustains less MNs within the network topology.

Depending on different network environments, the tree-based and the mesh-based algorithms have their advantages and limitations. The hybrid multicast routing protocols, which contains both the tree and the mesh structures, have been studied in the previous work [33] [34] [35]. A hybrid multicast algorithm based on prioritized networks is proposed in [33]. The formation of either the tree or the mesh structure depends on the prioritized overlays within the MANET. The core-based hybrid structure is proposed in [34] [35], where a cluster core is responsible for maintaining the structure. it is found that excessive control overheads are induced in these algorithms by sending the control and data packets to their corresponding cores.

Chapter 3

The Existing Multicast Routing Protocols

Two basic and commonly adapted multicast routing protocols, the ODMRP and the MAODV algorithms, are introduced in Section 3.1 and Section 3.2, respectively.

3.1 On Demand Multicast Routing Protocol (ODMRP)

The On Demand Multicast Routing Protocol (ODMRP) uses the forwarding group concept [36] to construct a forwarding mesh structure. The mesh structure provides more connectivity among multicast members than the tree structure supplies. The redundant flooding packets among the forwarding group and the multicast members help get over node displacement and channel fading effects. Therefore, frequent reconfigurations or repairs are not such required than trees.

Forwarding group is a set of nodes responsible for forwarding multicast data packets. Fig. 3.1 is an example to show the forwarding group notion and the robustness of a mesh configuration. Two sources (S_1 and S_2) send multicast data packets to three receivers (R_1, R_2 and R_3) through five forwarding group nodes (M, N, O, P and Q). In the tree configuration, there is only one path from S_2 to R_2, i.e. S_2-Q-M-O-R_2. If any link between two adjacent nodes on the path breaks or fails, e.g. M-O, R_2 can't receive any data from S_2 until the tree is

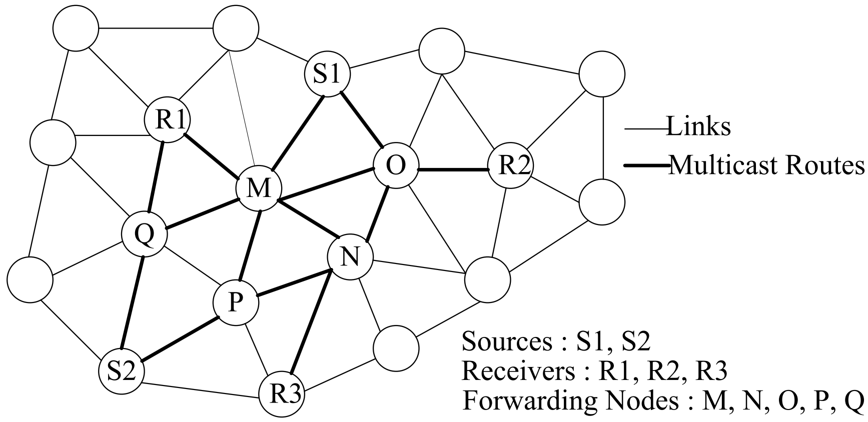


Figure 3.1: Mesh Network Topology

reconfigurable. In the mesh configuration, there are two or more than two paths between any member pairs. The redundant route (e.g. S_2-P-N-O-R_2) provides another route to delivery data without influenced by the broken link between M-O.

3.1.1 Multicast Route Establishment and Membership Maintenance

In the ODMRP algorithm, multicast route establishment and maintenances are carried out by the source on demand. On demand means that the corresponding operations are started when the demand is shown. On the other hand, the proactive routing protocols establish multicast route before the actual demand is produced. ODMRP follows a request phase and a reply phase cycle (see Fig. 3.2) that is common in on demand unicast routing protocols. The following pseudo codes describe the procedure of route establishment and membership maintenances.

while (a multicast source S wants to send a packet) {

S periodically broadcasts a *Join Request* ;

while (any node D receives non-duplicate *Join Request*) {

D store the upstream node ID (backward learning) ;

if (D is not a multicast receiver) {

D rebroadcasts *Join Request* ; }

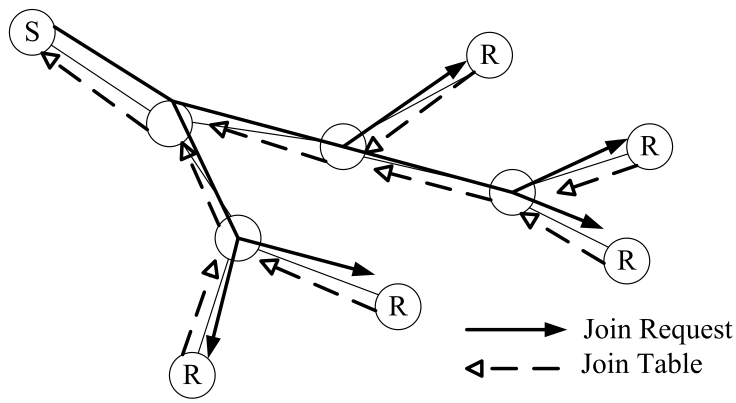


Figure 3.2: On-Demand Procedure for Membership Setup and Maintenance

else { (D is a multicast receiver)

D creates and updates the source entry in its *Member Table* ;

while (valid entries exist in the *Member Table*) {

D broadcasts *Join Table* periodically ;

while (any node T receives a *Join Table*) {

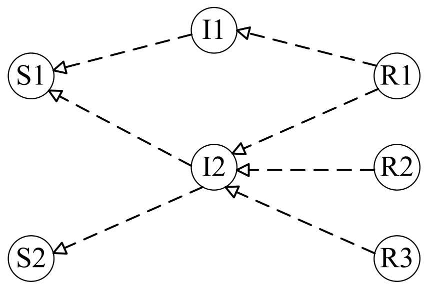
if (T 's own ID matches the next node ID of any one entry in *Join Table*) {

node T sets *FG-Flag* ;

node T broadcast its own *Join Table* built upon matched entries ; } } } } } }

The periodically control packet transmission refreshes the membership and updates the routes. The function of the next node ID field in Join Table is that node T can realize that it is on the path to the source. Therefore it is part of the forwarding group if its own ID matches the next node ID in the Join Table. The Join Table will be propagated by each forwarding group member until it arrives the multicast source. The whole process discoveries the routes from the sources to the receivers and builds a mesh-liked forwarding group.

Fig. 3.3 is an example of a Join Table forwarding flow. There are two multicast sources, S_1 and S_2, and three multicast receivers, R_1, R_2 and R_3. Nodes R_2 and R_3 send their Join



Join Table of Node R1

Source	Next Hop
S1	I1
S2	I2

Join Table of Node I1

Source	Next Hop
S1	S1

Join Table of Node R2

Source	Next Hop
S1	I2
S2	I2

Join Table of Node I2

Source	Next Hop
S1	S1
S2	S2

Join Table of Node R3

Source	Next Hop
S1	I2
S2	I2

Figure 3.3: A Join Table Forwarding Example

Tables to both S_1 and S_1 via node I_2, and node R_1 send its Join Table to S_1 via I_1. An intermediate node, I_1 or I_2, sets the FG-Flag and builds its own Join Table if its own ID matches any next node ID entry in the Join Table received from receivers. The Join Table built by node I_1 has an entry for source S_1 but no entry for source S_2 because the next node ID entry for S_2 in the Join Table received from R_1 is not I_1.

3.1.2 Soft State

In the ODMRP algorithm, no explicit control packet is necessary to join or leave the group. When a multicast source wants to leave the group (the source has no data to send to the group), it simply stops sending out Join Request packets. When a multicast receiver wants to leave the group (the receiver wants to stop receiving from a particular group) , it removes the corresponding entry in its Member Table and discontinue to broadcast the Join Table for that group. Forwarding group nodes realize that they are no more forwarding nodes if no refresh enough Join Tables are received before timeout.

3.2 Multicast Operation of the Ad-hoc Distance Vector Routing Protocol (MAODV)

In the MAODV algorithm, routes are discovered on demand, which uses a broadcast Route Request (RREQ) and a unicast Route Reply (RREP) mechanism. Broadcast packets are identified by using the source IP address and a specific field of the IP headers as a unique identifier of the packet.

3.2.1 AODV Unicast Route Discovery

The AODV algorithm is on demand and follows a route request/ route reply cycle.

Request Broadcasting and Reverse Route Establishment

When a Mobile Node (MN) requires a route to an unknown-record destination, it broadcasts a RREQ packet. A MN receiving a RREQ packet updates its Route Table to record the related route information first. The reverse route is recorded to be used to forward a RREP packet back to the source. If the MN has a fresh enough route to the requested destination, the MN generates a unicast RREP packet to the request source MN. Otherwise, it rebroadcasts the RREQ packets. Fig. 3.4(a) is a example of the broadcasting of RREQ packets.

Forward Path Setup

The responding MN unicasts the RREP packet back via the next hop to the source MN. The MN receiving the RREP packet updates its entry for the destination in its Route Table. Therefore the forward path to the destination is established. This procedure continues until the RREP packet reaches the source MN. Fig. 3.4(b) is an example of the destination MN sending back the RREP packet to the source MN. After the request and reply cycle, the source MN can use the discovered route for sending data packets to the destination.

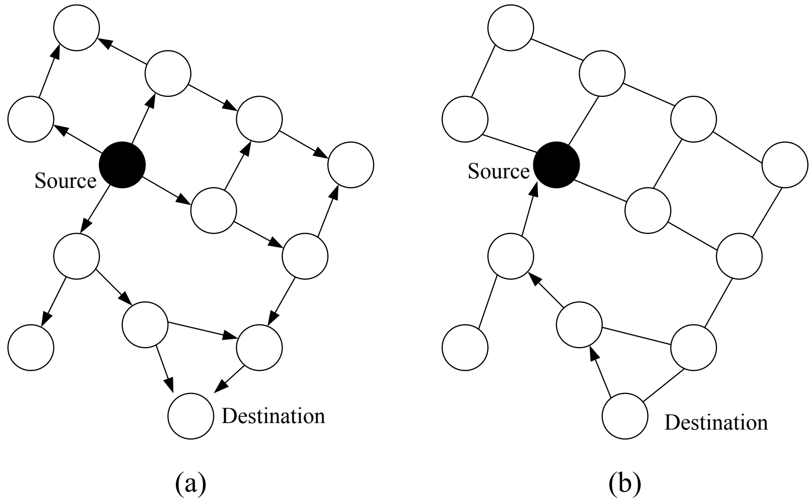


Figure 3.4: The RREQ / RREP Cycle

3.2.2 The MAODV Algorithm

The MAODV algorithm modifies the previously-described RREQ / RREP cycle by adding the Multicast Activation (MACT) packet. A multicast tree consists of the multicast group members and the routers that connecting the group members. All these MNs are called the tree members.

Route Request Message Generation

When a MN wants to join a multicast group or has multicast data to send, it sends a RREQ packet. The RREQ packet can be broadcast or unicast depending on the the information available at the source. Only a member of the multicast tree can reply a join RREQ packet and any MN that has a fresh enough route to the multicast group can respond to a non-join RREQ packet. The source will broadcast another RREQ packet if it doesn't receive any RREP packet before time out up to a default number. If all attempts are failed, the source MN becomes the group leader and manages the group information announcement. Fig. 3.5(a) shows an example for the RREQ packet propagation.

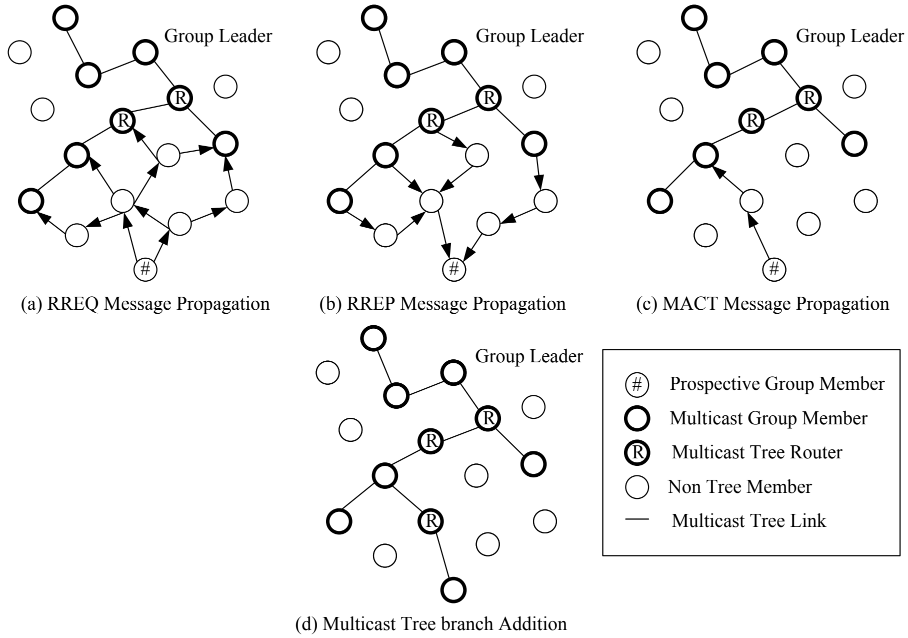


Figure 3.5: The Multicast Join Group Operation

Reverse Route Establishment

A join RREQ packet has a few processing differences. A MN receiving a join RREQ packet maintains a corresponding route information entry in its Multicast Route Table, in addition to its Route Table. There is an Enabled Flag for this entry and the flag is set to false. Whether the flag is set to true or not, it depends on the route activation process.

Route Reply Generation

With the RREP packet propagation, a MN receiving the RREP packet records the route information in both its Multicast Route Table and its Route Table, and the forward paths are established at the same time. Fig. 3.5(b) illustrates the RREP message propagation.

Multicast Route Activation

After sending the RREQ packet, the prospective MN waits for a configurable time to receive the RREP packets. Every RREP packet represents a potential addition to the multicast tree and only one of the RREP packets can be selected. The selection considers the freshness and hop count to the multicast tree (freshest and smallest hop count). At the end of the wait period, the prospective MN enables the selected route in its Multicast Route Table and then unicasts a MACT message to this selected next hop. The next hop MN repeats the same process until the MN that generated the RREP packet is reached. Fig. 3.5(c) illustrates a MACT message transmission and the addition of the multicast tree branch is completed in Fig. 3.5(d).

Multicast Tree Maintenance

Multicast tree maintenance must be done in a timely manner to optimize multicast tree connectivity. Multicast tree maintenance can be divided into three types: prune (when a node decides to leave the tree), repairing a break link and reconnecting partitioned trees.

3.3 Comparison between the ODMRP and the MAODV Protocols

A mesh-based multicast routing protocol can outperform the tree-based multicast routing protocols because of the availability of alternative routes [37].

3.3.1 Similarity between the ODMRP and the MAODV Protocols

- Both protocols discover multicast routes on demand.
- Both protocols are based on the request and reply cycles in route discovery.
- Multicast route information is kept in intermediate nodes along the multicast path.

3.3.2 Difference between the ODMRP and the MAODV Protocols

- The MAODV algorithm uses the bi-directional multicast tree while the ODMRP algorithm makes use of the mesh topology.
- A link failure causes a repair in the MAODV algorithm (hard state) while the ODMRP algorithm does not.

- A multicast tree is more efficient and avoids sending redundant packets to receivers.
- The MAODV algorithm unicasts the reply while the ODMRP algorithm broadcasts the reply.
- The MAODV algorithm doesn't activate a multicast route immediately while the ODMRP algorithm does.

Chapter 4

The Proposed Multicast Routing Protocols

4.1 The Proposed Power-Controlled Hybrid Multicast Routing (PCHMR) Protocol

This section starts form the discuss of protocol design considerations in Subsection 4.1.1, and then the practical part of the PCHMR are presented in Subsection 4.1.2 which consists of hybrid structure construction, joining process and hybrid structure maintenance.

4.1.1 Design Considerations

The design concept of the PCHMR algorithm is based on the group moving behaviors of the Mobile Nodes (MNs) in the real world. The movements of the MNs can be distinguished as one entire group or different groups within the network in consideration. The MNs within the same group tend to have similar moving behaviors, which results in a more static network topology, and comparably shorter relative distances and speeds between the MNs. On the other hand, the moving behaviors between the groups (i.e. inter-group communication) are generally diversified which cause less reliable communication linkages between the MNs.

The essence of the proposed PCHMR protocol utilizes either the tree-based or the mesh-based structure depending on whether the two MNs in communication are located within the same network group or not. The tree-based structure is adopted to establish the routes between the MNs within the same group. The communication links within the tree-based structure are easier to be maintained without sending excessive control packets. As for inter-group communication, the mesh-based structure is exploited to increase the robustness of the communication linkages. Since the numbers of group are comparably smaller than the number of the MNs within the network, the inefficiency of communication bandwidth induced by the mesh-based structure is minimized.

Fig. 4.1 shows the network topology with three groups, including Group A, B, and C. In the case that the pure tree-based structure is employed, each MN has only one upstream node that is traced back to a tree root (i.e. the MN with double circle as in Fig. 4.1). The tree structure is constructed with the MNs (i.e. the solid and the shaded circles) that are connected with the solid lines as their communication links. Due to the possible different moving behaviors between the groups, the linkages between the groups (i.e. L_1 that connects Group A and B, and L_2 that connects Group A and C) can easily be broken. The communication channels between the groups become unreliable and fragile. In the proposed PCHMR algorithm, the mesh-based topology is established with additional linkages that are constructed between different groups. As shown in Fig. 4.1, the additional linkages L_3, L_4, and L_5 are created between these three groups. Even though the linkages L_1 and L_2 are broken as mentioned before, the data packets can still be delivered between the groups via the other communication links. The proposed hybrid structure can provide more reliable linkages for inter-group communication.

4.1.2 The PCHMR Protocol

The MAODV [25] protocol is utilized as the baseline algorithm for constructing the tree aspect of the proposed hybrid structure. Each hybrid structure has a unique structure address and is composed of both the *structure members* (i.e. the solid circles in Fig. 4.1) and the *routers* (i.e. the shaded circles). It is noted that the *routers* are not the intended structure

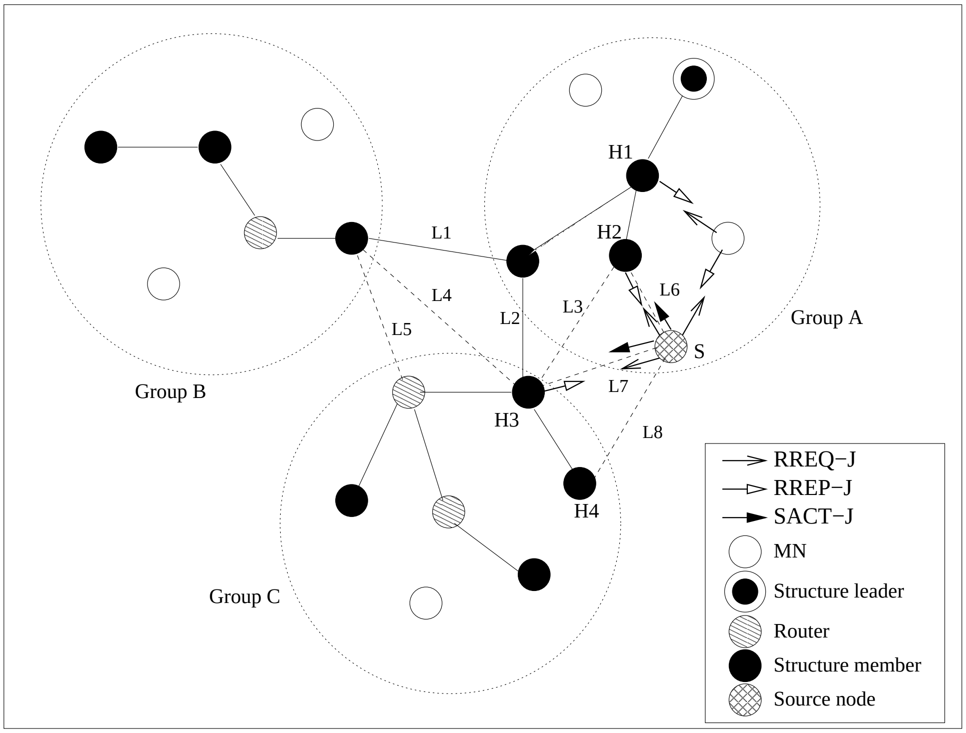


Figure 4.1: The Network Topology with the Proposed Hybrid Structure

members but only for the connection purpose within the hybrid structure.

The MN that first establishes the hybrid structure is called the *structure leader*. The *structure leader* is responsible for maintaining the hybrid structure by periodically broadcasting the *Structure-Hello* messages to all the MNs within the network. The Structure Sequence Number (SSN) is also updated to identify the freshness of the messages originated from the *structure leader* (i.e. $SSN(t_i) \geq SSN(t_j)$ for $t_i \geq t_j$). Each MN within the network maintains two tables and the contents are explained as follows:

1. Multicast Route Table (MRT): The SSN of the MN is recorded in its MRT. The MRT also lists the next hopping nodes (N_i, for $i = 1$ to n) from this MN to the hybrid structure. There are two other parameters associated with the next hopping node N_i: the Route Enabling Flag (REF_{N_i}) and the Average Power Vector ($\bar{P}_{N_i}$). REF_{N_i} is utilized to determine if the associated route is active or not; while $\bar{P}_{N_i}$ is used to record the average received signal power from this MN to the corresponding *structure member* via node N_i.

2. Structure Leader Table (SLT): The SLT records the address of the *structure leader* associated with the corresponding hybrid structure address. The periodic *Structure-Hello* messages initiated by the *structure leader* are utilized to update the contents within the SLT.

It is also noted that each MN holds a *Group Number* (GN) to identify which group it belongs to (i.e. either Group A, B, or C as in Fig. 4.1).

Hybrid Structure Construction and Joining Process

The route discovery process utilized in the AODV protocol [17] (i.e. the Route Request (RREQ) and Route Reply (RREP) cycle) is adopted as the basis in the hybrid structure construction and the corresponding joining process. As illustrated in Fig. 4.1, it is assumed that a node S intends to join the hybrid structure. After S starts broadcasting a RREQ-J (i.e. RREQ with a Join flag) packet, the MNs belonging to the hybrid structure (i.e. H_1, H_2, and H_3 as in Fig. 4.1) respond to the RREQ-J packet with a RREP-J (i.e. RREP with a Join flag) packet. Node S receives the (RREP-J)$_{H_j}$ packet, which contain the route information from S to H_j for $j = 1$ to m. It is noted that H_j represents the MN which belongs to the hybrid structure. The SSN_{H_j}, GN_{H_j}, $\bar{P}_{H_j}(t_c)$, and the hop counts (HC_{H_j}) information are also recorded in the (RREP-J)$_{H_j}$ packet, where t_c represents the current time instant.

After receiving the (RREP-J)$_{H_j}$, a Structure Activation message with a Join flag (SACT-J) is utilized by S to determine the next hop (i.e. N_i) in its MRT in order to join the hybrid structure. Node S will calculate the average power between $\bar{P}_{H_j}(t_c)$ and the receiving power ($P^r_{N_i}(t_c)$) obtained from its neighborhood node N_i. It is noted that $\bar{P}_{H_j}(t_c)$ is the average power carried by the (RREP-J)$_{H_j}$ packet, which does not include the receiving power information of the node N_i. The resulting power information will be recorded in one of the $\bar{\mathbf{P}}_{N_i}$ entry in its MRT as

$$\bar{P}_{N_i}(t_c) = \frac{(HC_{H_j} - 1)\bar{P}_{H_j}(t_c) + P^r_{N_i}(t_c)}{HC_{H_j}} \tag{4.1}$$

The power information ($\bar{P}_{N_i}(t_c)$) along with the number of hop counts (HC_{H_j}) are ex-

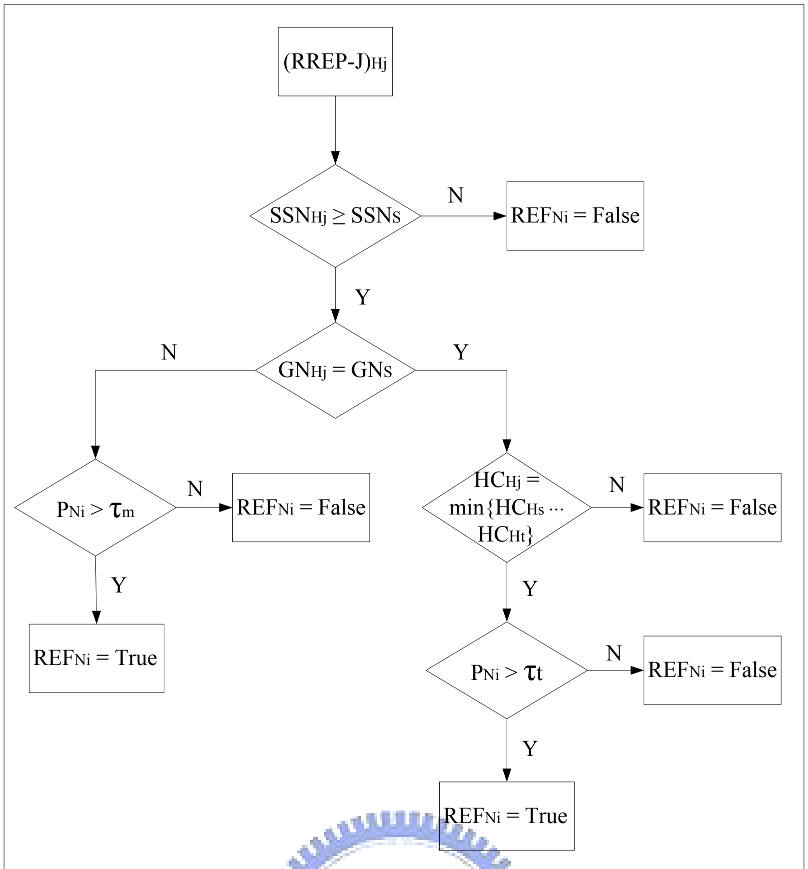


Figure 4.2: The Flow Diagrams for the Route Determination of the Proposed PCHMR Algorithm

ploited as the criterions for route determination. The REF_{N_i} associated with the selected next hopping node N_i will be enabled within the MRT of S. It is noted that H_j will be equal to N_i if H_j happens to be the next hopping node to S. As shown in Fig. 4.1, the routes (i.e. L_6 and L_7) to H_2 and H_3 might be established after the route determination algorithm. The route to H_1 may not been chosen due to the larger hopping counts between S and H_1. On the other hand, since S and H_3 possess different group numbers, the mesh aspect of the hybrid structure is constructed with the selection of the additional link L_7. The detail of the route determination algorithm is described as follows.

As illustrated by the flow diagram in Fig. 4.2, the proposed PCHMR algorithm employs several criterions for route determination. Only if all these conditions are satisfied, the SACT-

J will be initiated by S to establish the route to the corresponding MN (i.e. H_j) within the hybrid structure:

1. Information acquired from the (RREP-J)$_{H_j}$ packet is fed into the criterion checking for route establishment. If the SSN of H_j is greater or equal to the SSN of S (i.e. $SSN_{H_j} \geq SSN_S$), it indicates that H_j in the hybrid structure has more recent updates comparing with the source node S. The criterion checking can be continued. On the other hand, if $SSN_{H_j} < SSN_S$, the REF_{N_i} that corresponds to the route to H_j is set to disable.

2. The group number (GN) is utilized to verify if S and H_j are within the same moving group. This criterion determines if the tree-based or the mesh-based structure should be applied. If $GN_{H_j} = GN_S$, both H_j and S exist in the same group and the tree-based structure is adopted. The mesh-based topology is utilized if H_j and S are determined to be in different groups (i.e. $GN_{H_j} \neq GN_S$).

3. The fewest hop counts from S to H_j is selected as a criterion for route determination. If $HC_{H_j} = min\{HC_{H_s}, \ldots, HC_{H_t}\}$,where $\{HC_{H_s}, \ldots, HC_{H_t}\}$ represent the subset of $\{HC_{H_1}, \ldots, HC_{H_m}\}$ that have the same GN with S, it indicates that the route within the (RREP)$_{H_j}$ packet contains the fewest hop counts among the others. If $HC_{H_j} > min\{HC_s, \ldots, HC_t\}$, the corresponding REF_{N_i} is disabled.

4. The transmission signal strength between the MNs is considered to determine if the route should be activated. The criterion verifies if the average received signal power ($\bar{P}_{N_i}(t_c)$) from the neighborhood node is larger than a power threshold. For the tree aspect of the hybrid structure, the route to H_j is selected if the power strength of its corresponding neighborhood node N_i is greater than an adaptive threshold τ_t (i.e. $\bar{P}_{N_i}(t_c) > \tau_t$). The flag SRS_S within the MRT of S is verified to determine if there is already a route to the hybrid structure. If SRS_S = True, the REF_{N_i} is set to disable. For the mesh-based aspect of the hybrid structure, the power level of N_i is compared with another adaptive threshold τ_m. If $\bar{P}_{N_i}(t_c) > \tau_m$, the flag REF_{N_i} is set to True,

which indicates that the signal strength from N_i is large enough based on the criterion. It results in the activation of the route from S to H_j.

The selections of the two adaptive power thresholds (i.e. τ_t and τ_m) are dependent to both the mean value and the variation of the average received signal powers as

$$\tau_\gamma = \frac{1}{n}\sum_{i=1}^{n}\left(K_{1\gamma}\cdot M_{\bar{P}_{N_i}} + \frac{K_{2\gamma}}{\sigma_{\bar{P}_{N_i}}} + K_{3\gamma}\right) \tag{4.2}$$

for $\gamma = t$ and m. The parameter n represents the total number of the neighborhood MNs; $K_{1\gamma}$, $K_{2\gamma}$, and $K_{3\gamma}$, are the tunable parameters based on the system requirements; $M_{\bar{\mathbf{P}}_{N_i}}$ and $\sigma_{\bar{\mathbf{P}}_{N_i}}$ indicate the mean value and the standard deviation, which are computed online based on the time history within the average power vector $\bar{\mathbf{P}}_{N_i}$. The two power thresholds τ_t and τ_m are therefore adaptive to the mean value and the variation of the receiving power. As $M_{\bar{\mathbf{P}}_{N_i}}$ is increased, the power thresholds should be enlarged in order to reduce the possibility of selecting excessive linkages. The thresholds should be decreased if the variation $\sigma_{\bar{\mathbf{P}}_{N_i}}$ is amplified, which can results in more communication links to be chosen under severe signal propagation environments. It is also noted that the threshold τ_m is determined to consider the tradeoffs between the reliability and the overheads induced by the mesh-based structure. The additional linkages between the groups provide robustness between the MNs in communication; while the cost results from the excessive transmission of packets should be considered. With proper selection of K_{1m}, K_{2m}, and K_{3m}, the communication links between the groups can be restricted.

Hybrid Structure Maintenance

In the maintenance of the hybrid structure, two types of broadcast messages are utilized within the network. The *Structure-Hello* messages are periodically sent out by the *structure leader*. Each MN within the hybrid structure updates its SLT with the most recent information obtained from the *structure leader*. In order to manage local connectivity, another message, called *Neighbor-Hello* message, is periodically broadcasted within one hop between the MNs. In the PCHMR algorithm, the *Neighbor-Hello* message is also utilized to enhance the communication robustness while the various groups are dynamically moving within the network.

As shown in Fig. 4.1, assuming that the node S newly receives a *Neighbor-Hello* message from H_4 (which belongs to a different group), it indicates that these two MNs are moving within the communication range for data transmission. In order to increase the potential connectivity between different groups, the communication linkage L_8 is considered to be established. The criterions as stated in the previous subsection are utilized for route determination. In this case, as long as the receiving signal power $\bar{P}_{H_4}(t_c)$ is larger than the threshold τ_m, the linkage L_8 between the Group A and C can be established. H_4 will be recorded as one of the next hopping nodes in the MRT of S.

4.2 Overhead-Reduced On Demand Multicast Routing (ORODMR) Protocol

The proposed Overhead-Reduced On Demand Multicast Routing (ORODMR) protocol reduces the control overhead needed to maintain robust connectivity among Mobile Nodes (MNs).

4.2.1 Routing Tables

Each MN operating the ORODMR protocol maintains two routing tables. The first of them is the Join Reply Table (JRTable). The fields of the JRTable are as follows:

- Multicast Group IP Address
- Forwarding Group Flag Refresh Time
- Replying Member
- Replying Time

New entries are added or updated in the JRTable following the receipt of route replies (i.e. Join Tables) when the MN does not have a route entry for the indicated information in the message.

The second routing table that each MN keeps is the Join Request Table (JQTable). Similar to the maintenance of JRTable, new entries are added or updated in the JQTable after a MN receives unrecorded route requests. The contents of the JQTable are as follows:

- Multicast Group IP Address
- Source IP Address
- Sequence Number
- Previous Hop

The source ip address means the source of the Join Request and the previous hop indicates the last MN that propagated Join Request. The JQTable provides the next hop (route) information during Join Table transmissions. The source ip address and the sequence number of the packet are utilized to detect duplicates.

Besides two routing tables, all multicast group receivers maintain a Member Table that stores the multicast group information. For each multicast group that the MN joins, the responding multicast group address and the time when the last Join Request is arrived from that multicast group source (or sources) are recorded. If no Join Request is received from the recorded multicast group before the refresh time expires, the related entry is deleted from the Member Table. The operation described here achieves the partial soft state property in both the ORODMR and the ODMRP algorithms. The Member Table contains the following fields:

- Multicast Group IP Address
- Membership Refresh Time

4.2.2 Multicast Route Discovery and Forwarding Group Membership Establishment

The Multicast route discovery mechanism starts from the Join Request transmission by a source MN. The fields of the Join Request consist of the multicast group address and the sequence number. As a MN receives a Join Request, it checks that whether the packet is duplicate or not by the source IP address and the sequence number field. If the Join Request is fresh, the fields in the JQTable are added or updated according to the carried information in the request packet. The previous hop field in the JQTable points out the reverse route information to the multicast source. The Join Requests are broadcasted out the whole network until they arrive in a multicast receiver.

The multicast receiver responds the Join Request with a join reply message (i.e. the Join Table). Join Tables are propagated by broadcasting like request packets. A node that receives the Join Table sent out by the multicast receiver exactly knows the IP address information of the receiver, because it can extract the multicast receiver IP address from the IP protocol header. It is found that most of the existing multicast routing protocols do not use this receiver material to do anything. The multicast receiver IP address is obvious in the receiver-sent Join Table message but as the packet is relayed by the non-receiver node the receiver IP address is lost. To record the IP address of the receiver that responds a Join Request and generates a Join Table, two extra fields (replying member and replying time) are devised. The fields of a Join Table are as follows:

- Multicast Group IP Address
- Source IP Address
- Next Hop
- Replying Member
- Replying Time

The reverse route recorded in the JQTable is utilized here. The next hop field indicates the next hop along the route to the multicast source and the value comes from the previous hop field in JQTable. The replying member means the multicast receiver which generates the current Join Table. The replying time records the sending time in second of the Join Table.

When a MN receives a first Join Table, it checks that if the next hop field matches its own IP address. If it is on the reverse route, it has to set itself as a forwarding group member.

The forwarding group flag is set by altering the forwarding group flag refresh time to the current time and adding corresponding multicast group IP address, replying member and replying time in the JRTable. After the forwarding group's recognition, the node broadcasts its own Join Table. More explicitly, the next hop in the Join Table are changed according to previous hop in its JQTable. The replying member and the replying time are propagated out the one-hop range from the multicast receiver. For those MNs not on the reverse route, they just relay Join Table messages without making any packet content changes.

In the conventional ODMRP protocol, no matter how many Join Tables are received, the responding operation is the same. The second or the following Join Table receipt causes a node to check the forwarding group membership and to broadcast its or the ordinary Join Table. If the multicast group address already exists in the JRTable, only the forwarding group flag refresh time is updated. In the proposed ORODMR protocol, the two extra fields in Join Tables records the multicast receiver that have generated the Join Table and the knowledge of the receiver can be used for reducing unnecessary control packets.

Fig. 4.3 shows a Join Request and Join Table procedure for multicast route discovery. It is noted that node F_2 will receive three Join Table packets and two of these packets are sent by node R_2. Node F_1 will receive six Join Table packets (two of them are from node R_1 and two are from node R_2). The two successive Join Table packets generated by node R_2 (or node R_1) carry the exactly same message. It is not necessary for node F_2 and node F_1 to respond the same reply packets.

In the ORODMR protocol, a MN that receives a Join Table checks the replying member and replying time in the JRTable in addition. If the replying member related to the multicast group already exists in the JRTable, the node takes the difference of the current time and the replying time into account. When the difference is larger than a predefined threshold value, it means that the receiving Join Table is fresh enough and the node will rebroadcast the original reply packet or broadcast its own reply packet depending on the next hop field in Join Table. On the other hand, if the difference is equal or smaller than the threshold value, the Join Table is simply used to update forwarding group flag refresh time in JRTable and

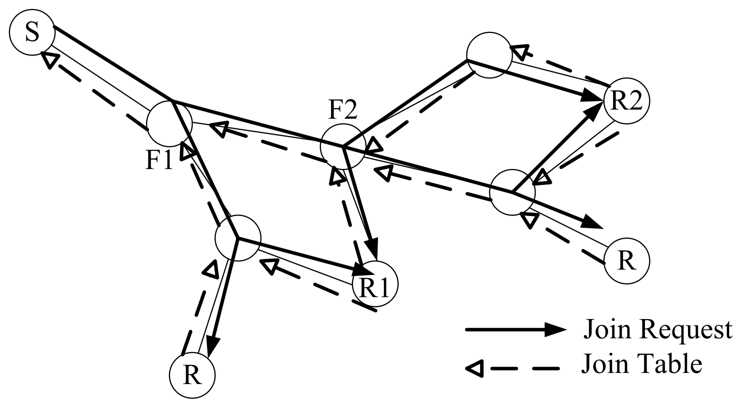


Figure 4.3: Join Request and Join Table Procedure for Multicast Route Discovery

any kind of relays are not preformed. For example, node F_2 will only broadcast its own Join Table once for the Join Tables that get node R_2 in the replying member field and so does node F_1. But the design in the conventional ODMRP algorithm guides node F_1 and node F_2 to respond every received Join Table. The ORODMR protocol reduces certain control packet flooding effectively and it is significant for any control overhead decrement in the design of the multicast routing protocols.

The proposed ORODMR protocol keeps fine mesh structures and reduces control overhead in the same time. The revoked reply packet propagation does not influence the basic data packet delivery session because the membership update of forwarding group is the same with the conventional design.

Chapter 5

Performance Evaluation

5.1 The Mobility Models

It has been studied that the moving behaviors of the MNs affect the performance of the designed ad hoc routing algorithms. In order to emulate the realistic moving environments, it is important to construct and utilize feasible mobility models for simulation purpose. The Random Waypoint Mobility (RWM) model [38] is widely used to evaluate the performance of ad hoc routing protocols. Each MN moves toward a randomly selected destination node with a chosen speed. The MN pauses for a pre-selected timeout period, and resumes its movement again. The MN's speed and timeout period are tunable parameters in order to simulate different moving scenarios.

The group mobility model fairly emulates the realistic moving behaviors of the MNs in many multicast applications. The Reference Point Group Mobility (RPGM) model [38] is utilized in the simulation to evaluate the effectiveness of the proposed PCHMR protocol. The movements of the MNs within a group depend on the traveling path of a logical Group Center (GC). By adopting the RWM model, the individual MN within a group moves randomly relative to its GC.

5.2 The Radio Propagation Model

As described in the proposed PCHMR algorithm in the previous chapter, the relative signal strength between the transmitting and the receiving MNs is considered and adopted as the major criterion for route determination. Therefore, the signal propagation model utilized in the simulations should emulate the practical transmission environment. The shadowing model [39] [40], which considers both the deterministic and the stochastic effects of the signal propagation, is employed to appropriately simulate the environment for data transmission.

5.3 Simulation Parameters

The simulations are conducted using the Network Simulator (NS-2, [41]) to compare the proposed PCHMR and ORODMR algorithms with the existing MAODV and ODMRP protocols. The RWM and RPGM model are utilized as the mobility model in the simulations. The simulation area is set to 1000×1000 m^2. The 50 MNs in the network are equally divided into five groups (i.e. 10 MNs in each group). There are 1 transmitters and 10 receivers for data packet transmission. The data distribution is designed to cross the different groups in order to show the effectiveness of the proposed PCHMR algorithm. The source node transmits its data packets with Constant Bit Rate (CBR) at the data rate of 256 Kbps. Each simulation runs for 900 seconds with the average speeds of the MNs at 0, 10, and 20 m/sec. The MNs' average pause time is set at 0 seconds. The parameters of the radio propagation model is listed as follows: $\beta = 2$, $\sigma_{dB} = 4$, $P_t = 25$ dBm, $G_t = 1$, $G_r = 1$, $L = 1$, and $\lambda = 0.125$. It is noted that these parameters are obtained from experiments to fairly emulate the realistic radio propagating environments.

5.4 Simulation Results and Discussion

The MAODV and the ODMRP protocols are implemented and compared with the proposed PCHMR and ORODMR algorithms in simulations respectively. The following four metrics are considered in the simulations for performance evaluation:

- **Data Packet Delivery Ratio**: The number of data packet delivered to multicast receivers over the number of data packet supposed to be delivered to multicast receivers.

- **Average End-to-End Delay**: The time difference between the time of a data packet transmitted and delivered.

- **Control Packet Overhead**: The number of control packets transmitted per data packet delivered.

- **Control Packet Rate**: The number of control packets transmitted over the number of control and data packets transmitted.

The changing factor is designed to be the shadowing deviations β to evaluate the performance under the environment with different signal variations. It is noted that the legend without β value indicates that β is equal to 2.

In the first part of this section, the performance comparison between two classic existing multicast routing protocols is shown in Figs. 5.1 to 5.4. The tree-based MAODV protocol shows a poor packet delivery performance than the mesh-based ODMRP protocol. In the tree structure, there is only one path between MNs. If a tree link breaks, the MAODV algorithm has to repair the link and produces more control packets. On the other hand, the ODMRP algorithm provides redundant routes with a mesh topology. The alternative paths allow data packets to be delivered even when the links fail. It is particularly noticed that the control packet overhead of the MAODV algorithm is around 20 times worse than that of the ODMRP algorithm under the high shadowing deviation ($\beta = 4$) assumption. The primary reason is that the MAODV protocol repairs the unconnected links in a timely manner even the success packet delivery is restricted by the network environment itself. On the other hand, the failed Join Request packets cause no other additional control packets in the ODMRP algorithm.

Figs. 5.5 to 5.8 illustrate the performance comparison among the MAODV, the ODMRP, the PCHMR and the ORODMR algorithms. As can be seen in Figs. 5.5 to 5.8, the mesh-based algorithms (i.e. the ORODMR and the ODMRP algorithms) obtain better performance than the tree-based algorithm (i.e. the MAODV algorithm); while the hybrid-based PCHMR

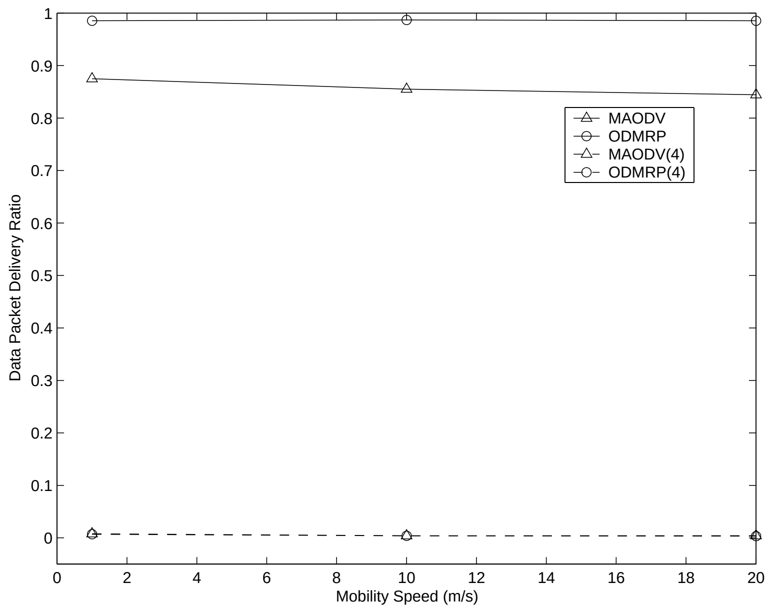


Figure 5.1: Performance Comparison: Packet Delivery Ratio vs Velocity for Different Shadowing Deviation

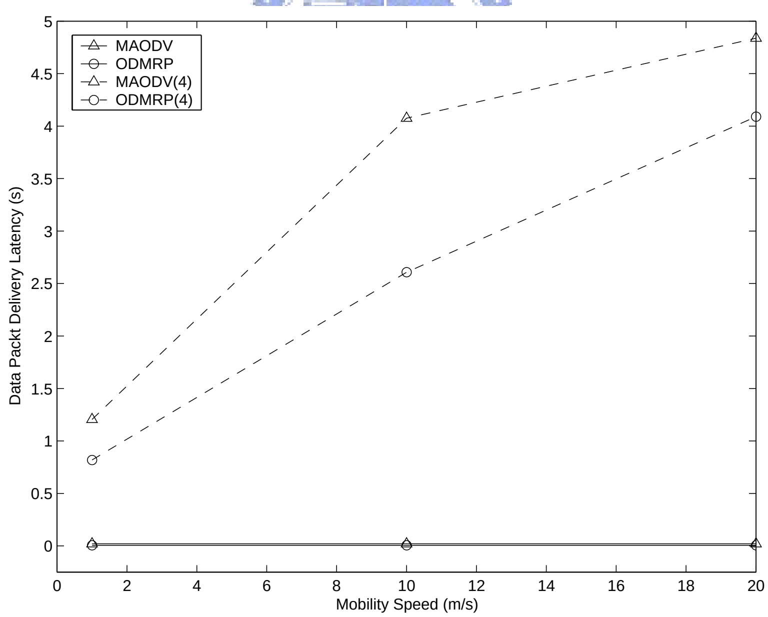


Figure 5.2: Performance Comparison: End-to-End Delay vs Velocity for Different Shadowing Deviation

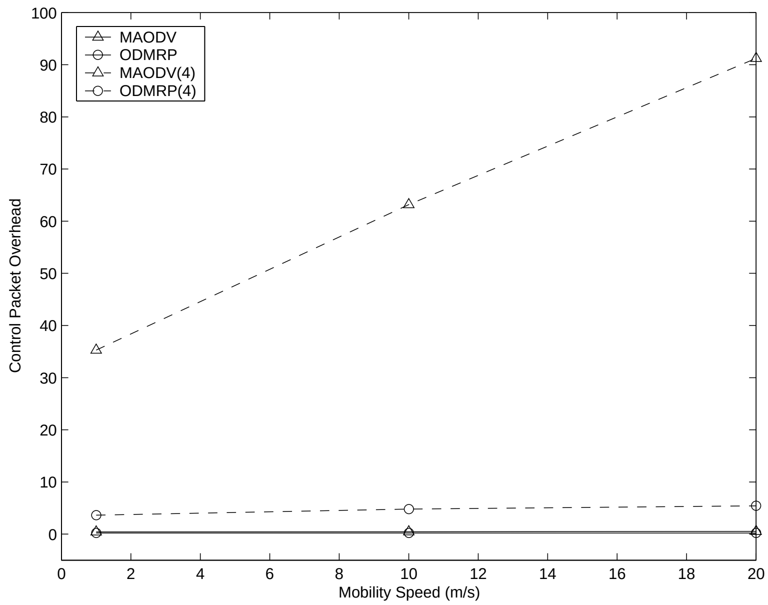


Figure 5.3: Performance Comparison: Control Packet Overhead vs Velocity for Different Shadowing Deviation

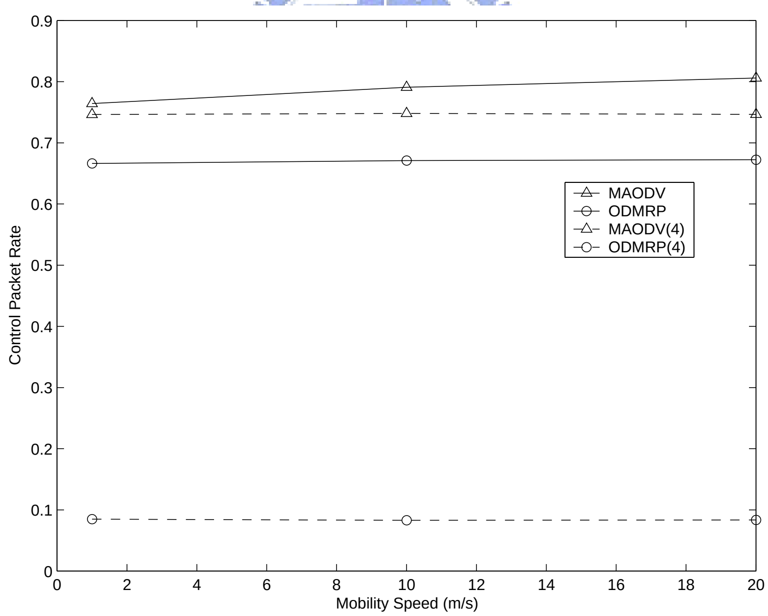


Figure 5.4: Performance Comparison: Control Packet Ratio vs Velocity for Different Shadowing Deviation

lies in between. As compared with the MAODV protocol under all mobility speeds, the proposed PCHMR scheme can increase the packet delivery ratio and also decrease the end-to-end delay, the control packet overhead, and the control packet rate. It is interesting to find that the hybrid-based PCHMR protocol consumes less control packets comparing with the tree-based MAODV scheme. The major reason is due to the excessive control packets required for repairing the broken linkages occurred from the MAODV scheme; while the PCHMR protocol utilizes comparably less control packets to maintain the mesh linkages, which offer additional reliable communication links between the MNs. With the adaptation of the power control mechanism in the PCHMR scheme, only those reliable links (that have signal powers larger than the power thresholds) are preserved; while the fragile communication links are consequently ignored.

It is noticed that the ORODMR algorithm achieves the same superior performance with the ODMRP algorithm for the packet delivery ratio and end-to-end latency, and obtain slightly decrease for the control packet overhead and the control rate in the meantime. It will be shown in the following results that the ORODMR protocol shows more distinct characteristic under a different simulation radio propagation environment

Figs. 5.9 to 5.12 illustrate the performance comparison between the tree-based MAODV and the hybrid-based PCHMR for different shadowing deviations β (i.e. 2, 2.2, and 2.5). Different shadowing deviations β are altered to test the performance difference between the PCHMR and the MAODV algorithms. The bigger the shadowing deviation parameter is, the faster the signal strength decays. It is obvious that as β value grows, the delivery ratio drops and the other three metrics considered rise. When the β value is set too stringent ($\beta = 2.5$), the packet delivery ratio and the control packet rate of both algorithms are severely degraded and it makes no difference for using power consideration and hybrid structure. In most cases, the PCHMR scheme obtains better performance than the MAODV algorithm, especially when the environment is full of interference. The received signal power and the extra mesh links make proposed PCHMR scheme achieving better performance than the MAODV algorithm in worse network connectivity.

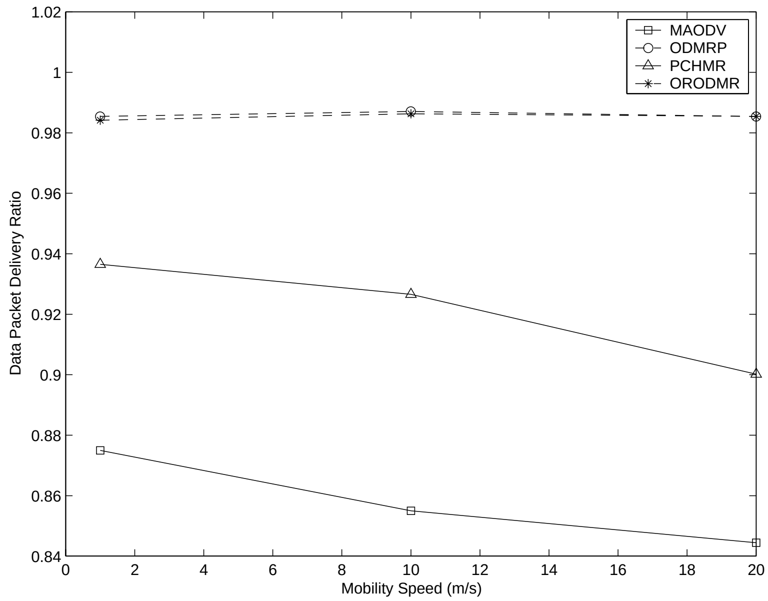


Figure 5.5: Performance Comparison: Packet Delivery Ratio vs Velocity

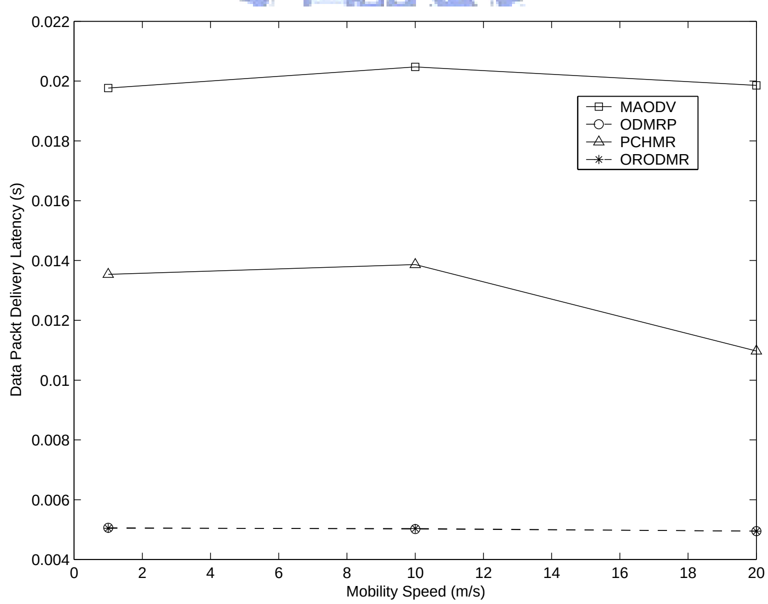


Figure 5.6: Performance Comparison: End-to-End Delay vs Velocity

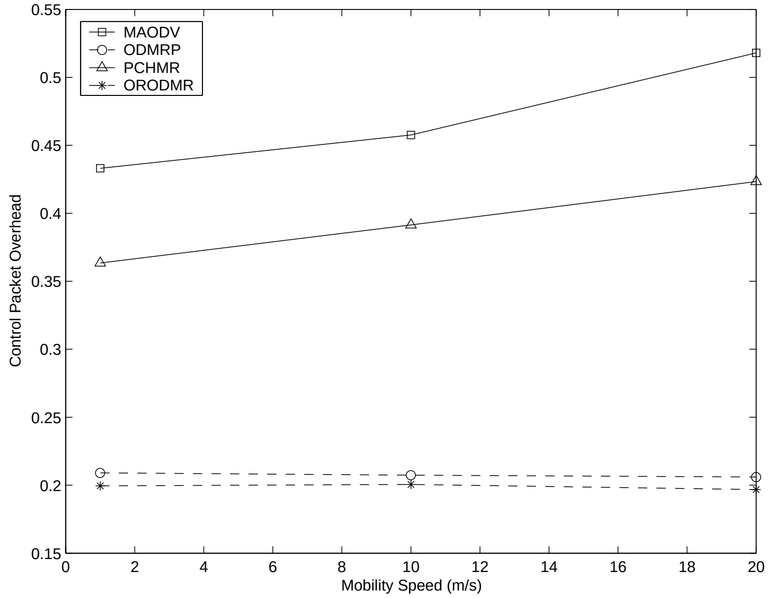


Figure 5.7: Performance Comparison: Control Packet Overhead vs Velocity

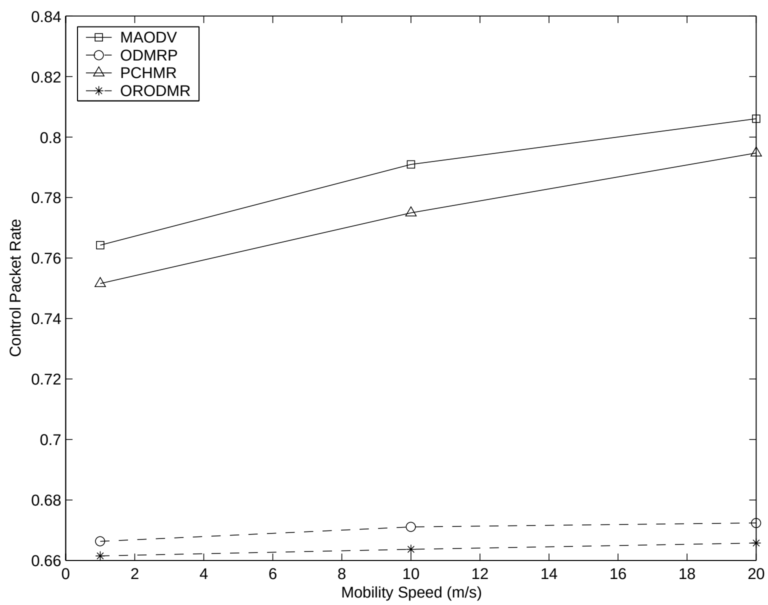


Figure 5.8: Performance Comparison: Control Packet Ratio vs Velocity

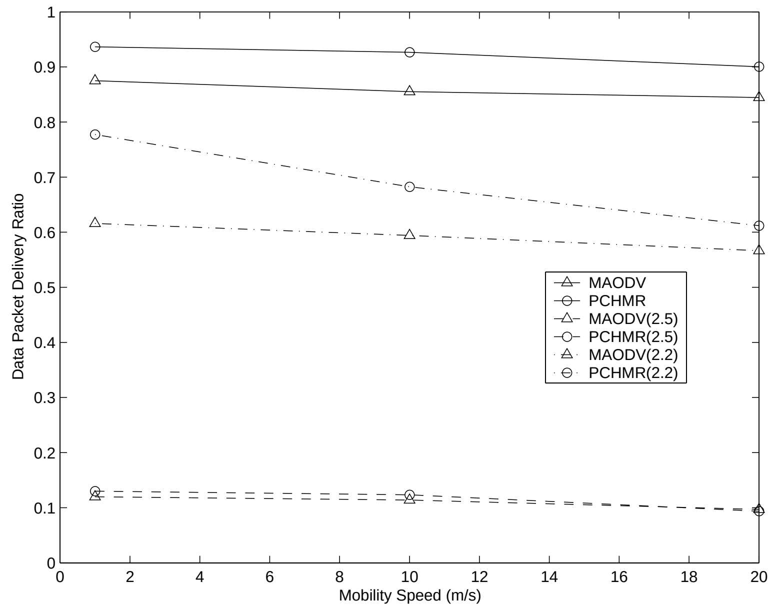


Figure 5.9: Tree Related Protocol Performance Comparison: Packet Delivery Ratio vs Velocity for Different Shadowing Deviation

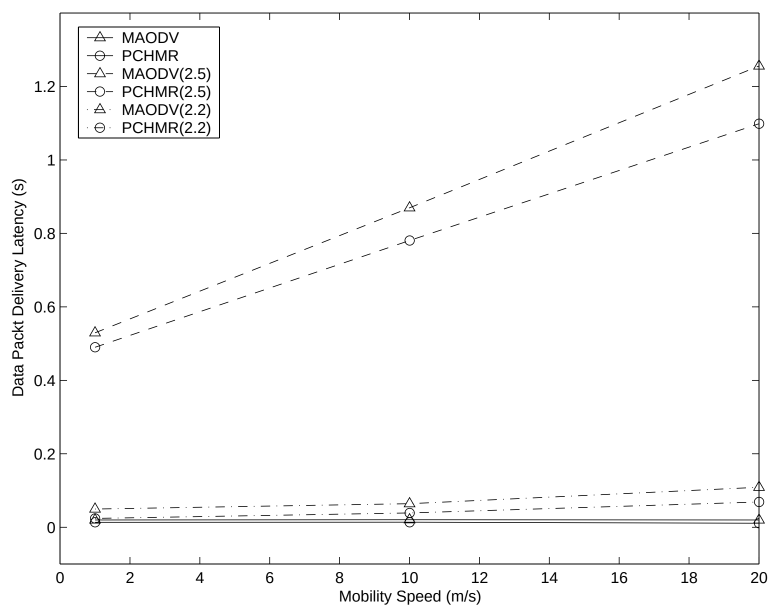


Figure 5.10: Tree Related Protocol Performance Comparison: End-to-End Delay vs Velocity for Different Shadowing Deviation

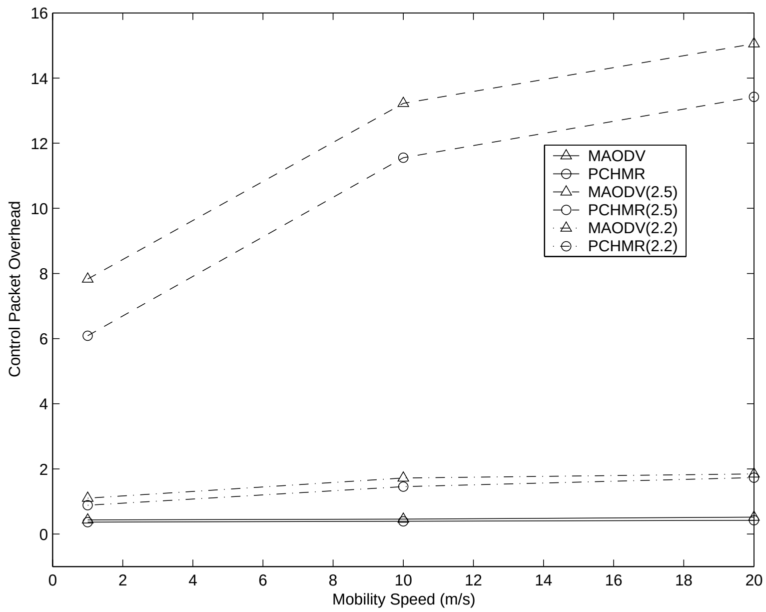


Figure 5.11: Tree Related Protocol Performance Comparison: Control Packet Overhead vs Velocity for Different Shadowing Deviation

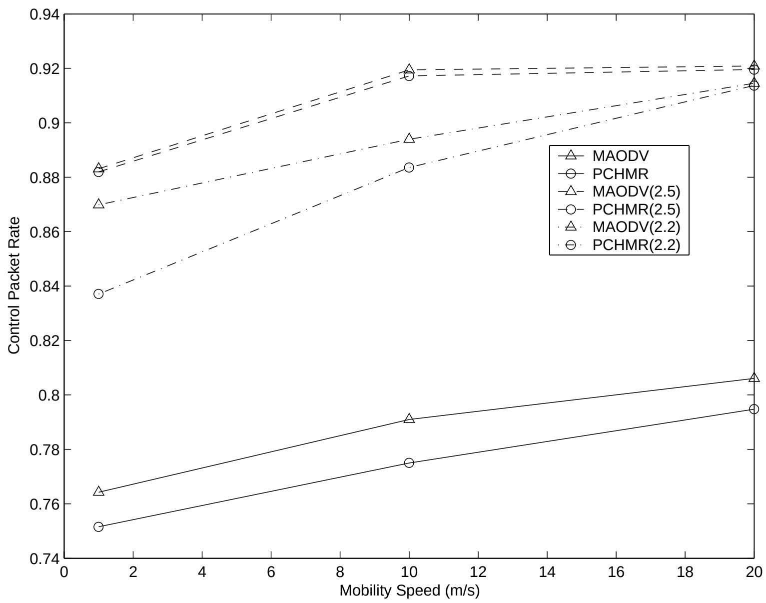


Figure 5.12: Tree Related Protocol Performance Comparison: Control Packet Ratio vs Velocity for Different Shadowing Deviation

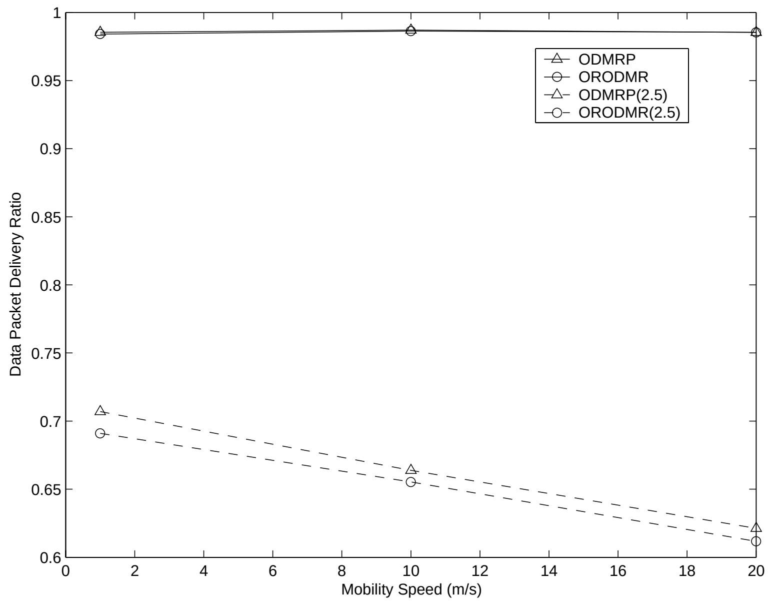


Figure 5.13: Mesh Related Protocol Performance Comparison: Packet Delivery Ratio vs Velocity for Different Shadowing Deviation

The performance comparisons between the mesh-based ORODMR and ODMRP algorithms are demonstrated in Figs. 5.13 to Figs. 5.16. The thought here is like the previous test for tree related algorithms. The proposed ORODMR protocol mainly focuses on reducing the control packet overhead. The performance under different signal propagation conditions is considered. As can be seen in Fig. 5.13 to 5.16, the ORODMR protocol keeps the high packet delivery ratio and lowered end-to-end delay. It also reduces the control packet overhead and control packet rate significantly. Even when the β equals 2.5, the delivery ratio and latency are only slightly influenced by the decreased usage of control packets that is implemented in the proposed ORODMR protocol.

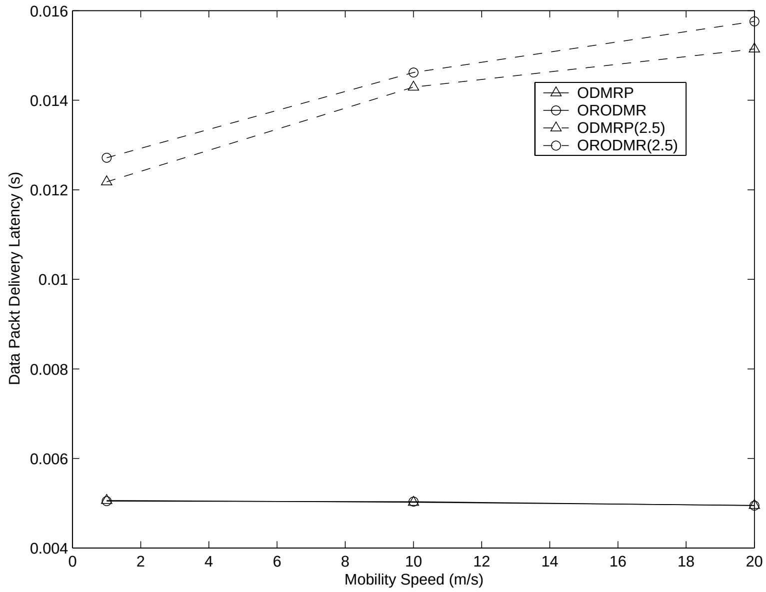


Figure 5.14: Mesh Related Protocol Performance Comparison: End-to-End Delay vs Velocity for Different Shadowing Deviation

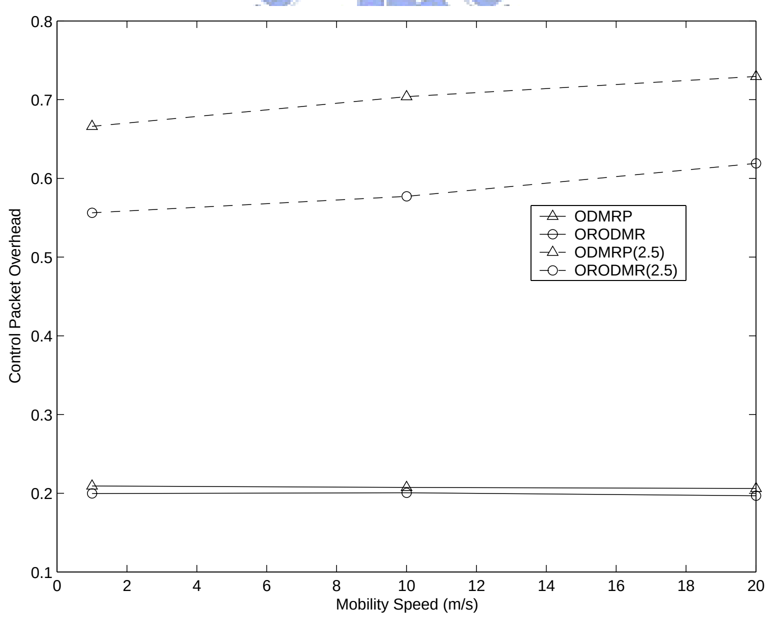


Figure 5.15: Mesh Related Protocol Performance Comparison: Control Packet Overhead vs Velocity for Different Shadowing Deviation

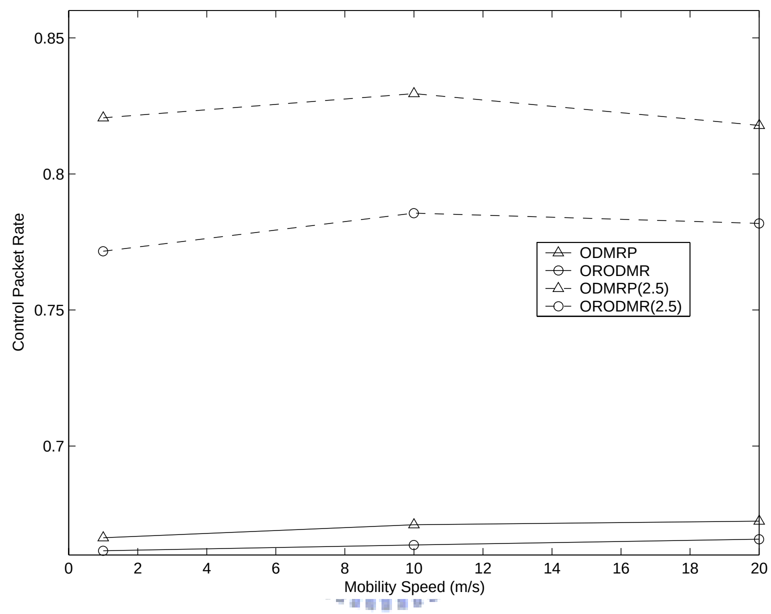


Figure 5.16: Mesh Related Protocol Performance Comparison: Control Packet Ratio vs Velocity for Different Shadowing Deviation

Chapter 6

Conclusion

A Power-Controlled Hybrid Multicast Routing (PCHMR) protocol and a Overhead-Reduced On Demand Multicast Routing (ORODMR) protocol for the mobile ad hoc network are presented in this thesis. The PCHMR algorithm combines the benefits of the tree-based and the mesh-based algorithms in order to fulfill the requirements within the dynamically changing networks, especially for group moving environment. The route determination scheme of the PCHMR algorithm considers both the hop counts within the route and the power strength between the MNs. The ORODMR protocol retains the excellent property of the ODMRP and reduces the control packets that are necessary for maintaining mobile node connectivity. The multicast receiver information are utilized to avoid redundant join reply transmission. The simulation results show that the proposed PCHMR protocol and the ORODMR algorithm outperform the existing tree-based and the mesh-based multicast routing protocols respectively, and the mesh-based multicast routing protocols achieve better performance than the tree-based multicast routing protocol under different signal variation environments.

Bibliography

[1] K. W. Chin, J. Judge, A. Williams and R. Kermode, "Implementation experience with MANET routing protocols," *ACM SIGCOMM Computer Communication Review*, Vol. 32, Issue 5, Nov. 2002, pp. 49-59.

[2] Y. Wu, P. A. Chou, Qian Zhang, K. Jain, Wenwu Zhu, Sun-Yuan Kung, "Network planning in wireless ad hoc networks: a cross-Layer approach," *Selected Areas in Communications, IEEE Journal*, Volume 23, Issue 1, Jan. 2005, pp. 136-150.

[3] S. Shakkottai, T. S. Rappaport, P. C. Karlsson, "Cross-layer design for wireless networks," *Communications Magazine, IEEE* Volume 41, Issue 10, Oct 2003, pp. 74 - 80.

[4] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications

[5] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band High-speed

[6] http://en.wikipedia.org/wiki/802.11

[7] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHZ Band

[8] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band

[9] http://www.isi.edu/nsnam/ns/ns-documentation.html

[10] H. T. Friis. A note on a simple transmission formula. *Proc. IRE,* 34, 1946.

[11] T. S. Rappaport. Wireless communications, principles and practice. Prentice Hall, 1996.

[12] C. E. Perkins, and P. Bhagwat, "Highly Dynamic Destination Sequence Distance Vector (DSDV) Routing for Mobile Computers," *Proceedings of the ACM SIGCOMM '94 Conference*, August 1994, pp.234-244.

[13] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," *ACM Mobile Networks Appl. J., Special Issue on Routing in Mobile Communication Networks,* Oct. 1996, pp. 183-197.

[14] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *Proceedings of IEEE Infocom '97*, Apr. 1997, pp. 1405-1413.

[15] V. D. Park and M. S. Corson, "Temporally-Ordered Routing Algorithm (TORA) version 1: Furrctiod specification." Internet-Draft, draft-ietf-rnanet-tora-spec-00.txt, November 1997, Working in progress.

[16] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," *Ad Hoc Networking*, edited by C. E. Perkins, Addison-Wesley, 2001.

[17] C. E. Perkins and E. M. Royer, "Ad-hoc On-demand Distance Vector Routing," *Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications*, Feb. 1999, pp. 90-100.

[18] C.-K. Toh, "A novel Distributed Routing Protocol to Support Ad-hoc Mobile Computing", *Proceedings of 15th IEEE Annual International Phoenix Conference on Computers and Communications,* March 1996, pp. 480-486.

[19] R. Dube, C. D. Rais, K.-Y. Wang, and S. K. Tripathi, "Signal Stability Based Adaptive Routing (SSA) for Ad-hoc Mobile Networks," *IEEE Personal Communications,* Feb. 1997, pp. 36-45.

[20] Z. J. Haas and M. R. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," *IEEE/ACM Trans. Networking,* vol.9, no.4, Aug. 2001, pp.427-438.

[21] S.E. Deering and D.R. Cheriton, "Multicast Routing in Datagram Internetworks and Extended LANs," *ACM Transactions on Computer Systems*, vol. 8, no. 2, May 1990, pp. 85-110.

[22] J. Moy, "Multicast Routing Extensions for OSPF," *Communications of the ACM*, vol. 37, no. 8, Aug. 1994, pp. 61-66.

[23] T. Ballardie, P. Francis, and J. Crowcroft, "Core Based Trees (CBT) - An Architecture for Scalable Inter-Domain Multicast Routing," *In Proceedings of ACM SICCOMM93*, Sail Francisco, CA, Oct. 1993, pp. 85-95.

[24] S. Deering, D.L. Estrin, D. Farinacci, V. Jacobson, C.G. Liu, and L. Wei, "The PIM Architecture for Wide-Area Multicast Routing," *IEEE/ACM Transactoins on Networking*, vol. 4, no. 2, Apr. 1996, pp. 153-162.

[25] E. M. Royer and C. E. Perkins, "Multicast Operation of the Ad-Hoc On-Demand Distance Vector Routing Protocol," *Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Aug. 1999, pp. 207-218.

[26] C. W. Wu and Y. C. Tay, "AMRIS: A Multicast Protocol for Ad Hoc Wireless Networks," *Proceedings of the IEEE Military Communications Conference*, Vol. 1, Oct. -Nov. 1999, pp. 25-29.

[27] J. Xie, R. R. Talpade, A. Mcauley, and M. Liu, "AMRoute: Ad Hoc Multicast Routing Protocol," *Mobile Networks and Applications*, Vol. 7, Iss. 6, Dec. 2002, pp. 429-439.

[28] S. K. S. Gupta and P. K. Srimani, "An Adaptive Protocol for Reliable Multicast in Mobile Multi-Hop Radio Networks," *Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications*, Feb. 1999, pp. 111-122.

[29] S. J. Lee, M. Gerla, and C. C. Chiang, "On-Demand Multicast Routing Protocol," *the IEEE Wireless Communications and Networking Conference*, Vol. 3, Sept. 1999, pp. 1298-1302.

[30] J. J. Garcia-Luna-Aceves and E. L. Madruga, "The Core-Assisted Mesh Protocol," *the IEEE Journal on Selected Areas in Communications*, Vol. 17, Iss. 8, Aug. 1999, pp. 1380-1394.

[31] P. Sinha, R. Sivakumar, and V. Bharghavan, "MCEDAR: Multicast Core-Extraction Distributed Ad Hoc Routing," *the IEEE Wireless Communications and Networking Conference*, Vol. 3, Sept. 1999, pp. 1313-1317.

[32] P. Sinha, R. Sivakumar, and V. Bharghavan, "CEDAR: a Core-Extraction Distributed Ad Hoc Routing Algorithm," *the IEEE Journal on Selected Areas in Communications*, Vol. 17, Iss. 8, Aug. 1999, pp. 1454-1465.

[33] L. Xiao, A. Patil, Y. Liu, L. M. Ni, A.-H. Esfahanian, "Prioritized overlay Multicast in Mobile Ad Hoc Environments," *IEEE Computer*, vol.37, no.2, February 2004, pp. 67-74.

[34] B. An, S. Papavassiliou, "A Mobility-Based Hybrid Multicast Routing in Mobile Ad-hoc Wireless Networks," *Military Communications Conference*, 2001.

[35] J. Biswas, M. Barai, and S. K. Nandy, "Efficient Hybrid Multicast Routing Protocol for Ad-Hoc Wireless Networks," *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04)*, 2004.

[36] C.-C. Chiang, M. Gerla and L. Zhang, "Forwarding Group Multicast Protocol (FGMP) for Multihop, Mobile Wireless Networks," *Baltzer Cluster Computig*, vol. 1, no. 2, 1998, pp. 187-196.

[37] T. Kunz, E. Cheng, "On-demand multicasting in ad-hoc networks:comparing AODV and ODMRP," *Distributed Computing Systems, Proceedings of the 22nd International Conference*, 2-5 July 2002, Page(s):453 - 454.

[38] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," *Wireless Communications and Mobile Computing: Special Issue on Mobile Ad Hoc Networking*, Vol. 2, No. 5, Dec. 2002, pp. 483-502.

[39] T. Rappaport, "Wireless Communications: Principles and Practice," *Prentice Hall PTR*, Dec. 2001.

[40] H. T. Friis, "A Note on a Simple Transmission Formula," *Proceedings of the IRE*, Vol. 41, May. 1946, pp. 254-256.

[41] J. Heidemann, N. Bulusu, J. Elson, C. Intanagonwiwak, K. Lan, Y. Xu, W. Ye, D. Estrin, and R. Govindan, "Effects of Detail in Wireless Network Simulation," *Proceedings of the SCS Multiconference on Distributed Simulation*, Jan. 2001, pp. 3-11.