A LINK LAYER SCHEME FOR RELIABLE MULTICAST IN WIRELESS NETWORKS

by

Aarthi Natarajan

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

ARIZONA STATE UNIVERSITY

May 2003

A LINK LAYER SCHEME FOR RELIABLE MULTICAST IN WIRELESS NETWORKS

by

Aarthi Natarajan

has been approved

April 2003

APPROVED:

_____, Chair

_____

_____

Supervisory Committee

ACCEPTED:

_____

Department Chair

_____

Dean, Graduate College

ABSTRACT

Several applications, like search and rescue operations, disaster relief operations, and environmental monitoring, involve a group of wireless devices communicating with each other. The critical nature of these applications necessitate reliable data delivery. This has increased the demand for reliable group communication protocols in wireless networks. However, obtaining reliability in single channel multi-access wireless local area networks (LANs) can be a challenging task due to node mobility, channel characteristics and resource constraints.

Multicast is the paradigm used for delivering data from a sender to a set of receivers. This research work investigates issues involved in realizing reliable multicast in single channel multi-access wireless networks. Ensuring reliable delivery of data at the link layer facilitates local error recovery and increases the reliability of the data delivered. IEEE 802.11 Medium Access Control(MAC) and Physical layer specification for wireless LANs does not support reliable multicast. This thesis, presents two MAC layer reliable multicast extensions to IEEE 802.11 MAC layer protocol: Rts-Data-Nack Protocol (RDNP) and Multizone Rts-Data-Nack Protocol (M-RDNP), RDNP uses negative acknowledgments to prompt retransmissions of corrupted data. However, RDNP suffers from collisions due to hidden terminals in ad hoc networks. M-RDNP is a modified version of RDNP which mitigates the effect of hidden terminals in ad hoc networks.

This thesis studies the performance of the protocols in both wireless LANs as well as ad hoc networks. The performance of the protocols is defined in terms of the average packet drop ratio, which is the ratio of the average number of packets dropped per receiver to the number of packets sent by the sender. The higher the average packet drop ratio, the lower the protocol reliability. Simulation results show that reliability increases with the use of the

proposed reliable MAC layer protocols in wireless LANs and stationary ad hoc networks. In mobile ad hoc networks, when the number of neighbors are high and the channel bit error rate is low, IEEE 802.11 multicast is more reliable compared to the proposed reliable multicast protocols. Whenever the channel bit error rate is high, the proposed reliable MAC layer protocols achieve better reliability than IEEE 802.11.

To my parents

ACKNOWLEDGMENTS

I would like to thank my advisor, Dr. Sandeep Gupta, for his invaluable guidance, support and encouragement. This work would have been impossible without his advice and motivation.

I would also like to thank my committee members, Dr. Partha Dasgupta and Dr. Andrea Richa for their feedback and guidance.

Also, I would like convey my sincere thanks Ganesh Sridharan for simulating the self stabilizing routing protocols. I would like to thank Georgios Varsamopoulos for helping with my analysis. I would like to thank Valliappan Annamalai for helping me with my bug fixes. I would like to thank Vikram Shankar for sharing his thoughts about the MAC layer. I would like to thank Yashwanth Prakash for his insight into the physical layer. I would like to thank Sriram Cherukuri and Naveen Tummala for proof reading my documents.

Last but not the least I would like to thank my parents and my sister for believing in my abilities.

TABLE OF CONTENTS

Page

Page

Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

CHAPTER 1

Introduction

The field of computer networks and communication has risen from the need to facilitate data transfer between two or more computing units. Some examples of computing units are desktops, laptops, personal digital assistants (PDAs), cell phones, sensor devices, global positioning systems (GPS) and handhelds. A single computing unit is termed as a *host* or a *node*. A set of hosts trying to communicate with each other form a network. Advances in the communication technology has enabled connecting hosts through the wireless medium. Technologies like IEEE 802.11[Com99] and Bluetooth[Blu02] define standards for communication between devices in local area networks and personal area networks respectively. Communication between hosts are broadly classified as unicast, multicast and broadcast. Unicast (or one-to-one communication) deals with the transfer of information from one sender to one recipient. Multicast (or one-to-many communication) deals with the dissemination of data from one sender to multiple recipients. Broadcast (or one-to-all communication) is a special form of multicast communication which deals with delivering information to all hosts forming the network.

1. Multicast Applications

There are several applications that require communication within a group. Consider the group communication involved during search and rescue operations. The message generated by one of the team members must be delivered to all the other members of the search team. Another example of group communication is a simple chat application between a group of friends. Other examples of group communications are military applications, emergency operations, disaster relief operations and white board applications. Multicast is the popular paradigm for group communication. One performance requirement common to all the above applications is reliable data delivery.

2. Wireless Network Architecture

The multicast applications mentioned above typically involve a group of mobile or stationary hosts that need to communicate within a given area. Group-related information must be delivered to these hosts through the wireless medium. Communicating using a wireless network has several advantages. Wireless networks are ease to deploy. The deployment can be very fast and in some cases setting up a wired network can be practically impossible.

The underlying communication can be infrastructure based or ad hoc (See Fig.1). In a typical infrastructure based communication, the given area is divided into a number of cells. The cells provide complete coverage to the area. Each cell is serviced by a stationary base station. The base station is connected to the wired network through the its interface. All traffic to or from the wireless hosts always flows through the base station using the wireless interface. Such an architecture is also termed as a wireless local area network

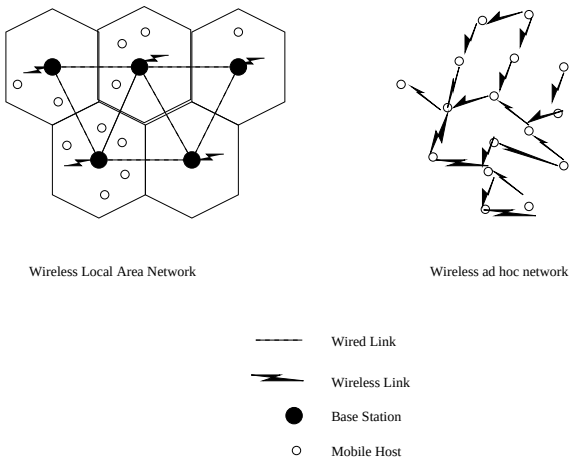


Figure 1. Wireless networks: Centralized and Distributed

(LAN). In local area networks, only the first and last hops of communication are wireless. However, in many situations, employing such an infrastructure for communication might not be feasible. In such situations, we need an ad hoc network of nodes (can also be stationary sensors) to communicate with each other. An ad hoc network is formed by a collection of autonomous mobile or stationary hosts communicating among themselves, providing the required services. In ad hoc networks all the communication hops may be wireless. In a wireless LAN, the base station propagates information to all the wireless recipients within its range. In ad hoc networks every node propagates information to its neighbors which in turn might or might not forward this information. The common feature of both architectures, is a single host propagating the group-related information to its group neighbors. We shall call this node as the sender. The sender may be different from the source of the multicast traffic. In case of wireless LANs, the sender is the base station. In case of ad hoc networks, the sender can be any host in the network which lies on the path between the source and the destination hosts. A host that can receive another host's transmission is said to be the latter's neighbor. If a neighbor is interested in the multicast data being transmitted then

it is termed as the group neighbor.

3. Importance of reliable delivery at the link layer

In a single-channel multi-access wireless medium achieving the desired performance can be quite challenging[GL00]. Reliability can be achieved end-to-end or at the link layer. Link layer reliability allows local error recovery and thereby improves throughput, conserves energy and when reliability is important it also reduces the end-to-end delay. In this work we mainly concentrate on providing link level reliability A reliable link layer must address the following three issues.

3.1. Medium Access. Firstly, the MAC layer needs to govern channel access and perform congestion control. When delivering group traffic to a set of immediate receivers, the packet can be unicast to each receiver in the set. However, owing to the broadcast nature of the medium, such retransmissions are redundant. As the number of neighbors increases, the number of unicast transmissions also increases linearly. Such repeated redundant retransmissions consume channel bandwidth and battery energy and reduce the channel throughput. A more efficient approach is to broadcast the message using the multicast address. All recipients use the multicast address information in order to filter the message. The transmission of a packet from a sender to its neighbors is termed as single hop transmission. Typically, the MAC layer is responsible for the timing and synchronization of the transmission across a single hop.

In wireless networks, the signal strength fades with the distance between the sender and the receiver. This fading property introduces several issues that need to be addressed.

- **No collision detection:** In wired networks, like the Ethernet, Carrier Sense Multi Access with Collision Detection (CSMA/CD) is used to govern medium access. The sender scans the channel before transmitting data. If the channel is idle, the sender proceeds with the data transmission. If a collision occurs at some point along the wire, the collision is visible at the sender which then halts its data transmission. In a wired networks, collisions at the receiver will be visible at the sender. However, this might not be true in a wireless medium because of its fading property. So collision detection cannot be employed in wireless networks. Also, the signal strength of transmission can be too high for the receiver to detect any other transmission. This property is called self interference. Thus collision avoidance techniques are used in wireless networks.

- **Hidden Terminals:** A hidden terminal is one which is within the range of the receiver but out of the range of the sender[TK75, FGLA97]. A hidden terminal can cause collisions at a receiver. Consider the example illustrated in Fig. 2. Node A is sending data to node B. Node C is hidden from node A. If node C wants to send data to node D, it senses the channel, finds the medium idle and begins transmitting data to node D. This causes collisions at node B.

- **Exposed Terminals:** An exposed node is one which is within the range of the sender but out of the range of the receiver. An exposed node is the inverse of a hidden node. The bandwidth of the channel is not utilized fully due to exposed terminals thereby lowering the overall throughput. Consider the example illustrated in Fig. 2. Node B is sending data to node A. Node C is hidden from node A but within the range of node B. If node C wants to send data to node D, it senses the channel, finds the medium busy and suppresses the transmission. Such a suppression is unnecessary.

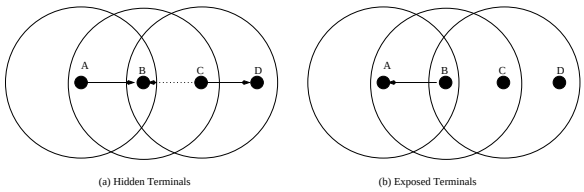


Figure 2. Hidden Terminals and Exposed Terminals

- **Capture Effect:** In the presence of two simultaneous transmissions of different signal strengths, the receiver can pick up the stronger signal if the ratio of the signal strength of the stronger signal to that of the weaker signal is greater than the capture threshold (SNR_T). This effect is known as the capture effect. This effect can be viewed as a slight mitigation of the hidden terminal problem. This effect is instrumental in the design of the proposed medium access protocols.

3.2. Local Error Recovery. Secondly, a reliable link layer must perform local error recovery. Consider a channel with a BER given by 10^{-5}. For a transmission with a payload size of 512 bytes, 4% of the packets are in error. This packet error percentage increases as the BER increases. For the same payload size, a channel with BER given by 10^{-4}, corrupts 40% of the packets. Error correction techniques and retransmissions are frequently employed to recover from such transmission errors. Both techniques consume resources in terms of both bandwidth and energy. Sender-based and receiver-based techniques have been extensively studied in order to a trigger retransmission of a corrupted packet[TKP97]. These techniques are based on the presence or absence of feedback packets from the receivers at the sender. When the feedback information flows up to the originator of the multicast traffic, the recovery is said to be end-to-end. When the feedback information is sent to the immediate sender, the recovery is said to be local. Though local error recovery does not guarantee end-to-end reliability it reduces end-to-end delay and consid-

erably improves channel throughput[IG00]. This local error recovery must be performed by the link layer.

3.3. Feedback Flow Control. Another important functionality of the MAC layer is to reduce the collision of feedback packets from multiple receivers generated during local error recovery and channel access.

3.4. Other Issues. Some more issues that need to be kept in mind when designing a reliable link layer are:

- **Bandwidth constraint:** While the bandwidth of the wire-line medium is in the order of Gbps, the bandwidth of a wireless medium is of the order of only a few Mbps. A wireless channel is severely constrained in bandwidth as opposed to its wire-line counterparts.

- **Power Anemia:** The devices participating in the transmission are constrained in energy. The battery power and size limits the operational capacity of wireless devices. Energy is consumed during computation and communication. However, it is observed that the energy consumed during communication is much higher when compared to the energy consumed during computation.

4. Overview of Thesis

In this work we propose two reliable link layer protocols for multicast in wireless networks. The first protocol, Rts-Data-Nack Protocol (RDNP), provides a Negative AC-Knowledgment (NACK) based scheme for reliable delivery of multicast[1] packets within

[1] If all nodes within the cell belong to the group to which the message has to be communicated, then the reliable multicast proposed is equivalent to reliable broadcast at the multicast address.

multi-access wireless LANs. Nodes that do not receive the data packet correctly send a NACK packet. If the sender senses a busy medium during the NACK slot, then it retransmits the packet. In wireless LANs the base station is the central arbiter and hence there are no hidden terminal problems. All communication has to go through the base station. So RDNP works well for reliable data delivery in wireless LANs. Multizone Rts-Data-Nack (M-RDNP) Protocol is a slight modification of RDNP which tries to mitigate the effect of hidden terminals in ad hoc networks by forcing the routing layer to build routes using only those nodes that do not suffer from hidden terminals. Both protocols can be easily adapted to IEEE 802.11 with slight modifications. The protocol semantics is such that multicast has higher priority compared to unicast transmissions.

Using extensive simulations in network simulator(ns-2)[FV], we show that RDNP achieves higher reliability compared to that of the LBP, PBP, DBP and the multicast protocol adopted in IEEE 802.11[Com99] in wireless LANs. We also show that in multi-hop networks, M-RDNP and RDNP show better performance than IEEE 802.11 multicast in several scenarios. We have used shortest path spanning tree (SPST) for routing packets in multi-hop networks. The reason for this choice is twofold.

- Gupta and Ganesh[SG03] have shown that SPST has better data delivery ratio compared to several routing protocols.
- We wanted to observe the behavior of self stabilizing routing protocols for reliable medium access control (MAC) layer

The rest of the document is organized as follows. Chapter 2 introduces previous work in related areas. Chapter 3 presents the functional details of the IEEE 802.11 MAC layer and the SPST routing protocol. Chapter 4 presents a detailed description of protocols

RDNP and M-RDNP. Chapter 5 presents the simulation environment used and the results obtained. Finally, chapter 6 summarizes this work.

CHAPTER 2

Related Work

The two main solutions to hidden terminals are:

- **RTS-CTS based:** A two way handshake prior to the data transmission is used to inform the hidden terminals of the upcoming data transmission. The hidden terminals then refrain from accessing the channel for the duration of transmission.
- **Busy tone based:** In the busy tone solution, the receivers transmit a busy tone on a separate control channel for the duration of reception. The hidden terminals sense the control channel before trying to access the data channel. If the hidden terminals sense a busy tone on the control channel they refrain from the data channel access.

This section presents a discussion of several MAC layer reliable unicast and multicast protocols which are based on the above schemes.

1. Unicast Protocols

1.1. RTS-CTS solutions.

Medium Access with Collision Avoidance (MACA). P. Karn proposed the MACA[Kar90] protocol to mitigate the severity of hidden terminals and exposed terminals. In MACA, when a node wants to transmit data, it broadcasts a Request-To-Send (RTS)

packet. The RTS packet contains information regarding the destination for the pending data packet and the expected duration of transmission. On receiving the RTS packet, the destination replies with a Clear-To-Send (CTS) packet if it is ready to receive the data. The CTS packet also contains information about the duration of transmission. On receiving the CTS packet, the sender transmits the data packet. If the sender does not get a CTS packet, then it backs off and contends for the channel again. All nodes that receive either the RTS packet or the CTS packet suppress their transmission for the duration specified in the corresponding packet. Thus the effect of the hidden terminals is reduced. In order to limit the effect of the exposed terminals, P. Karn suggested that if a node hears only the RTS but not the CTS, it may assume that the receiving node is out of its range. It can then go ahead and contend for the channel immediately.

Floor Acquisition Multiple Access (FAMA). The FAMA[FGLA95b, FGLA95a] protocol uses combination of Carrier Sense Multiple Access (CSMA)[JT87] and MACA in order to improve the reliability of the data delivered. In MACA, a node does not sense the channel before transmitting the RTS. If for some reason, a node does not hear both the RTS and the CTS packet, it may start transmitting packets while another data transmission is going on. To avoid this problem, the authors propose that the sender performs non-persistent[1] carrier sensing before transmitting the RTS packet. FAMA also allows the transmission of a burst of packets rather just one data packet, once the channel has been acquired. In order to avoid channel hogging, the burst size is subject to a maximum limit.

Multiple Access with Collision Avoidance for Wireless (MACAW). The MACAW [BDSZ94] protocol is an extension of the MACA protocol. MACAW differs from MACA in four aspects.

[1]Non-persistent CSMA has higher throughput when compared to p-persistent CSMA during high loads and only slightly lesser throughput under low loads

1. MACAW uses Multiplicative Increase Linear Decrease (MILD) wherein the window size be increased by 1.5 times but reduced only by one slot time. This scheme is used in order to reduce the wide fluctuation in the size of the contention window in MACA.

2. In MACA, nodes that get channel access have smaller contention windows as opposed to nodes that do not. This leads to unfair channel access. In MACAW all nodes set their contention window value to that of their neighbors which won channel access.

3. In MACA, if the RTS-CTS exchange is unsuccessful, all receivers of either the RTS or the CTS delay channel access unnecessarily. MACAW introduces the Direct Sequence (DS) packet to specifically inform the neighbors of the sending node whether the RTS/CTS dialog was successful or not.

4. When there is heavy traffic in the network and the size of the data packet is much larger than the RTS packet, the time during which the channel can be sensed to be free is very small. A node that wants to transmit will have to sense the channel during that small period and the chances of that happening are also very small. To help a node find this small period, MACAW introduces the Request RTS (RRTS) packet. This packet is sent by the receiver to the sender informing the sender that the channel around the receiver is free and that the sender may transmit an RTS if it desires.

1.2. Busy Tones.

Dual Busy Tone Multiple Access (DBTMA) -. The DBTMA proposed by Deng.et.al[DJ98] aims to reduce the effect of hidden terminals created by mobile hosts that move into a transmission zone after the RTS-CTS exchange. DBTMA uses a control channel to transmit busy tones and a data channel to transmit data packets. When a node wants to transmit, it senses for the presence of receive busy tone. When no tone is detected,

the node begins data transmission on the data channel and the transmission of transmit busy tone on the control channel. When a node starts receiving data it begins to transmit the receive busy tone on the control channel for the entire duration of the reception. This solves the hidden terminal problems created by the mobile nodes. If a node senses only the transmit busy tone and not the receive busy tone then it begins to transmit its data thereby mitigating the effect of the exposed terminals.

2. Multicast Protocols

Reliable multicast can be achieved by multiple reliable unicast transmissions to each of the receiver nodes using any of the above mentioned protocols. However, the throughput of such multicast communication falls sharply as the number of multicast receivers grows. Also, owing to the broadcast nature of the wireless medium, most of the unicast transmissions are redundant. This reason promoted research investigating broadcast oriented alternatives for reliable medium access for multicast in wireless networks. Most protocols try to address the following three problems associated with MAC layer reliable multicast.

- *Solving hidden terminal problems:* Most protocols use an exchange of RTS-CTS packets in order to solve hidden terminal problems[TK75, BDSZ94].

- *Local error recovery of packets:* Providing support for reliability at the MAC layer facilitates local error recovery. Though this does not guarantee end-to-end reliability it reduces the end-to-end delay and considerably improves the channel throughput[IG00]. Protocols have used NACK and ACK based schemes in order to recover from errors locally. The reception of a NACK packet or the absence of an ACK packet prompts

a retransmission of the packet[TKP97]. Note that delayed NACKs have also been termed as explicit retransmission request packets.

- *Eliminating collision of feedback packets:* Because the feedback information (CTS, ACK, NACK) needs to be collected from multiple receivers, protocols propose different scheduling policies for transmitting feedback packets. A robust scheme must not be affected by the collision of feedback packets.

2.1. RTS-CTS based solutions.

Delay Based Protocol (DBP). DBP [KK99, KK01] uses an exchange of RTS-CTS packets in order to provide collision free channel access. As the name suggests, DBP uses a delay based scheme in order to mitigate the effect of CTS collision from multiple receiver at the multicast sender. In this scheme, the multicast sender sends an RTS packet and waits for at most T CTS slots. As soon as the receivers receive a CTS packet they select a slot from $[0, L]$ where $L > T$ and set their internal timers to this value. The timer is decremented at the end of each slot. A receiver transmits a CTS packet as soon as this timer expires. When the multicast sender receives a CTS packet it sends the DATA packet. Receivers suppress their CTS slot transmission when they start receiving the DATA packet. The effectiveness of this protocol is strongly dependent on the values of n, T and L. The RTS is successful if and only if the multicast sender receives a single CTS packet from any receiver. If the RTS is unsuccessful the multicast sender backs off and contends for the channel again. If two or more receivers transmit a CTS in the same slot, the CTS packets collide at the receiver. Also, if every receiver selects a slot beyond T, then the multicast sender does not receive any CTS thus tries again. As demonstrated by Kuri and Kasera[KK99], the performance is optimal values of T and L need to be tuned based on the value of n. As n varies, T

and L need to be modified. When receivers detect a lost packet through a gap in sequence numbers, they must explicitly request for a retransmission of the packet. Thus, there is a delay associated with initiating an error recovery. As long as any receiver is ready to receive the data packet and this willingness is communicated to the sender through a collision free CTS packet, the sender proceeds with the transmission.

Probability Based Protocol (PBP). PBP [KK99, KK01] performs medium access through carrier sensing and RTS-CTS exchange. Also, it uses a probability based scheme in order to prevent CTS collision. Unlike DBP, in this scheme, every RTS slot is followed by exactly one CTS slot. The multicast sender transmits RTS packet after sensing an idle channel. Receivers of the multicast RTS packet respond with a CTS packet probabilistically. Let us assume that p is the probability with which a receiver responds with a CTS. The sender proceeds with the DATA transmission if and only if it receives a single CTS packet. The probability of exactly one node transmitting the CTS packet is inversely proportional to n, the number of receivers. Thus p is dependent on n. Like DBP, lost packets must be recovered through explicit retransmission requests. If the sender does not receive a CTS packet after the RTS transmission it backs off and contends for the channel again. Also, as long as any receiver is ready to receive DATA and this willingness is communicated to the sender through a collision free CTS packet, the sender proceeds with the transmission.

Leader Based Protocol (LBP). In LBP[KK99, KK01] a special node called "*leader*" is responsible for providing collision free feedback information. When the sender sends an RTS packet, the leader node replies with a CTS packet. If the sender receives the CTS packet correctly, it proceeds with the DATA transmission. Otherwise it backoff and retries later. If a non-leader receiver is not willing to participate in the transmission then it transmits an NCTS which destroys the CTS at the sender. If the leader itself is not ready to receive the

packet, it does not send a CTS. Either way, the sender will not receive a CTS packet and will not proceed with the data transmission. A receiver believes that a data packet is lost if it receives a multicast RTS packet and does not receive the corresponding data packet correctly. If a data packet is lost the receivers immediately transmit a NACK packet. Thus in this protocol there is no delay associated with initiating error recovery. If the leader receives the packet successfully it transmits an ACK packet. Otherwise the leader does not send the ACK packet. The sender contends for the channel to retransmit the data packet if if does not receive the ACK from the leader. If it does receiver the ACK then it proceeds to transmit the next packet. In LBP, the sender transmits the data packet if and only if all of the recipients are ready to receive the data packet. The sender has to keep track of the movement of the leader node and also provide a good leader election mechanism. Kuri and Kasera [KK99] propose a leader election scheme in which the first node to join the group becomes the group leader. If the leader becomes unavailable at any point of time then the entire group is destroyed and recreated. However, this process can be quite expensive when the network involves high speed mobile nodes.

Simple NACK broadcast protocol. Impett, Corson and Park[MCP00] present a simple NACK based broadcast MAC protocol which can be used even to multicast data. When the sender senses an idle channel it sends a multicast RTS directed to one of the intended recipients. The recipient to whom the RTS was directed responds with a CTS packet if willing to participate in the communication. If the sender receives the CTS it proceeds with the transmission of the DATA packet. Otherwise it backs off and contends for the channel again. Receivers that do not receive the packet, explicitly request a retransmission of the packet. Thus the initiation of the error-recovery is delayed. In order to avoid long delays, the authors suggest transmitting periodic HELLO messages with the sequence number of

the last packet transmitted. If this number does not match the sequence number of the packet, the receiver send a NACK packet. Each receiver sends a randomly delayed NACK in order to avoid an implosion of NACKs at the sender. Also, sender aggregates the NACK packets before retransmitting the DATA packet in order to avoid retransmitting the same packet several times.

Crying Baby Algorithm. The NACK based approach described above has one basic problem. Since the RTS-CTS exchange is only between the sender and one multicast receiver, all the other receivers are susceptible to hidden terminal problems. In order to avoid this problem, the authors of [MCP00] present a variation of the NACK based scheme called the Crying Baby algorithm. In this protocol, the sender maintains a list of all nodes that request a retransmission of a packet. It then transmits the data packet multiple times, once for every node in the list. In other words, if there are k nodes in the list then the sends contends k times to send the same packet. The sender assumes that the receiver sent NACK because of hidden terminal problems. There are several problems with this scheme. The list of receivers needs to be updated periodically. Also, associating hidden terminal problems to every packet lost can lead to repeated transmissions of redundant data especially if packet losses are only due to channel transmission errors.

Broadcast Support Multiple Access (BSMA). The main problem with multiple recipients is to ensure that none of the receivers suffer from hidden terminals. Tang and Gerla[TG00a, TG00b] present a simple protocol, BSMA, in which all receiver send a CTS packet at the same time. The rationale behind such an approach is that, even though they might collide at the sender, the CTS packets will be received by the hidden terminals and they will suppress their transmissions. The sender sends a multicast RTS packet. All the receivers of the multicast RTS, reply with a CTS immediately. If the sender perceives a busy

channel or receives a single CTS packet it proceeds with the DATA transmission. Similarly, all receivers which lost the DATA packet, transmit a NACK packet immediately. If the sender receives a single NACK or senses a busy medium in the NACK slot, it retransmits the packet. However, a problem with this protocol is that there can be a collision of CTS packets at the hidden terminals because of close receivers. Thus the hidden terminals can still transmit at the same time as the multicast sender.

Broadcast Medium Window (BMW). In BMW[TG01], Tang and Gerla have presented a medium access protocol for reliable broadcast. This can be used even for multicast communication. Every node maintains a list of its neighbors, a list of packets transmitted and a list of sequence numbers of packets received. List of neighbors is updated on the reception of any of RTS,CTS,DATA,ACK,HELLO frames. A sender directs the RTS packet to a particular receiver similar to the crying baby algorithm. In the RTS packet, the source also specifies the the range of packets it has transmitted (least packet sequence number already sent and the sequence number of the packet currently transmitting). If the receiver of the RTS packet realizes that it is missing some previous transmission or missing only the current transmission, it sends the corresponding missing packet sequence number along with the CTS. The multicast sender then transmits the packet with the sequence number mentioned in the CTS packet. All nodes which are a part of the multicast group consume the data. However, only the node which sent the CTS packet responds with an ACK if it received the packet correctly. If the multicast sender receives the ACK it proceeds with transmitting the next packet. If the packet transmitted was the same as the one intended then, the sender, picks a new receiver to transmit the next packet. However, if the multicast sender retransmitted a packet rather than sending the packet it intended to deliver (as mentioned in the RTS packet), it sends an RTS packet to the same receiver without

performing CSMA/CA for packet that it desired to deliver in the previous transmission. In a round robin fashion every node, listening to the sender gets a chance to recover from its losses. Also, once the sender has no more packets to transmits, it goes through one extra complete cycle of the round robin in order to ensure that all the receivers have received all packets successfully. When channel contention is high BMW will revert back to the basic medium access of IEEE 802.11 for broadcast packets. This protocol requires that the sender maintains an updated list of neighbor nodes, the reliability of delivery is dependent on the correctness of the neighbor list. Also, the protocol is not very scalable because the error recovery depends on the number if nodes thats are there in the network. Some nodes may experience delays in recovering lost packets if there are a large number of nodes in the network.

Batch Mode Multicast MAC (BMMM). In BMMM[SHAL02] there is a sequence of RTS-CTS exchanges with every receiver before the sender transmits the DATA packet. In other words there are n contention phases in order to transmit one data packet to n receivers. If the sender receives a CTS from every receiver then it proceeds with the DATA transmission. Otherwise it retries after a backoff. Once the sender finishes the data transmission it initiates a sequence of RACK/ACK exchanges with every receiver to determine which receiver lost the packet. If all the receivers send an ACK packet, it proceeds to transmit the next packet. Otherwise it retransmits the same packet. Similar to BMW, the reliability of delivery is dependent on the correctness of the neighbor list. This protocol is not very scalable because as the number of nodes increase, the number of contention phases also increase. Consider the scenario where sender is in the process of RTS-CTS with receiver A and if receiver B is yet to participate then some other node around receiver B can start transmitting data. When the sender gets to receiver B, it will not receive a

CTS and thus will delay transmission. This can happen repeatedly delaying the multicast transmission indefinitely.

Location Aware Multicast MAC (LAMM). LAMM[SHAL02] is a variation to BMMM, in which the authors propose having the RTS-CTS dialog with a subset of nodes rather than all the intended recipients using the location information of the nodes. The location information used from GPS is transmitted along with the period beacon messages (need 30 bits). Neighbors use this information to get the exact location of a node. They prove that it is sufficient for the subset of nodes to acknowledge the packet rather than all the neighbor nodes. This assumption is validated using theoretical proofs. This protocol requires extra processing at the sender in order to determine the subset. This subset can keep changing and need not be static based on node mobility.

2.2. Busy Tones.

IEEE 802.11MX. In IEEE 802.11MX[GSL03, Sha02] the sender transmits the RTS packet and listens on the signaling channel for an NCTS tone. Receivers not willing to participate in the data communication send out NCTS tone in the signaling channel. If no tone is sensed it transmits the data packet. At the start of the data transmission, the sender and the receivers start transmitting a busy tone in the busy-tone channel. Nodes that want to access the channel sense the busy tone channel. Thus all nodes that do not hear the RTS can still refrain from trying to access the channel. After the data packet is sent, the sender waits for a NAK tone. Receivers that do not receive an error free data packet send out NAK tone. If no NAK tone is heard it assumes that the data transmission was successful.

2.3. FEC based techniques.

RMDP. Authors of [YC99, RV97, RV98] suggest improving the reliability of transmission by using forward error correction (FEC) codes. FEC codes help in recovering from bit errors without retransmitting the data, thereby saving a lot of wireless bandwidth. FEC can be used in combination with M-RDNP to further improve the performance of our protocol.

2.4. Problems identified with previous work. The RTS-CTS scheme adopted in IEEE 802.11 WLAN[Com99] standard was proposed in order to combat hidden terminal problems. Xu et.al.[XGB02], show that RTS-CTS does not completely eliminate all hidden terminal problems in the network. For sufficiently large distances between the sender and the receiver, they show that the receiver nodes can still lose packets due to simultaneous transmissions from hidden terminals. In view of this recent work, all the RTS-CTS based reliable multicast protocols described above still suffer from hidden terminal problems. Though the ACK based schemes do help recover from these problems, it reduces the performance of the protocols. M-RDNP uses only reliable neighbors to transmit packets and thus does not suffer from the problems identified in [XGB02]. As the node density increase, the reliability of transmission in protocols using RTS-CTS is affected. Also, the degree of reliability achieved by LBP, DBP, PBP, BSMA, LAMM and BMMM strongly depend on explicit knowledge about the identities of the nodes receiving the multicast transmission across a single hop. M-RDNP does not have any such constraints.

CHAPTER 3

Preliminaries

1. MAC in IEEE 802.11

In this section, we shall briefly describe the Distributed Coordination Function (DCF) medium access mechanism provided by IEEE 802.11[1]. DCF is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The standard avoids collisions in single channel multi-access networks through the use of virtual carrier sensing at the MAC layer and physical carrier sensing at the physical layer. Virtual carrier sensing is performed using a timer called Network Allocation Vector (NAV). The duration field in the header of all transmitted packets is used to update the NAV of the receivers. A node can access the channel only when its NAV has expired. Typically, the value of the duration field specifies the longest duration for which the communication lasts. Neighbors who successfully receive a packet from a sender use the duration information to update their NAVs. This prevents the nodes around the sender from interfering with the remainder of the communication. Physical carrier sensing is performed by listening to the channel for any signal in the medium. Only those signals which are stronger than the noise threshold of the physical interface will be detected. The channel is presumed busy as long as a signal, greater

[1]We consider only DCF because it can be used with both wireless LANs and ad hoc networks unlike Point Coordination function (PCF)

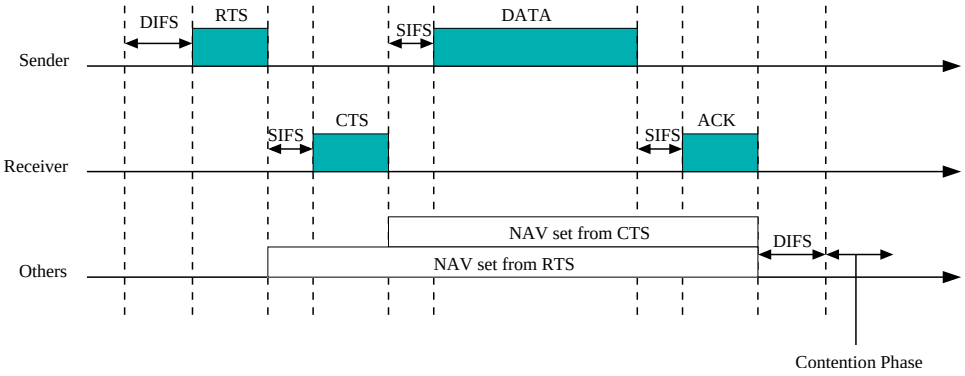


Figure 3. Timing diagram for IEEE 802.11 Unicast[Sha02]

than the noise threshold, is detected on the channel. Otherwise the channel is presumed to be idle. Time interval between frame transmissions, called InterFrame Space (IFS), provides a mechanism for prioritizing access to the shared medium. The IEEE 802.11 standard specifies three IFS intervals: short IFS (SIFS), point coordination function IFS (PIFS) and DCF-IFS (DIFS). The durations of these time intervals are such that SIFS < PIFS < DIFS. (See Table 2 for typical values)

The NAV of a node is decremented steadily. Once the NAV of a prospective sender expires, the sender waits for one DIFS duration before transmitting a packet. If the channel is presumed busy within the DIFS then the sender increments the backoff window, updates the NAV and contends for the channel again after backing off. Otherwise, it transmits the data packet. If the packet is received without errors, the recipient responds with an ACK packet after a SIFS duration. All nodes that receive the DATA packet update their NAV based on the duration field of the data packet which is the sum of one SIFS slot and transmission time for an ACK packet.

With the hope of mitigating hidden terminal problems (See Section 1), the IEEE 802.11 standard specifies a two-way handshake (RTS-CTS) prior to the data transmission. After scanning the channel for a DIFS interval, the sender sends an RTS to the receiver. The

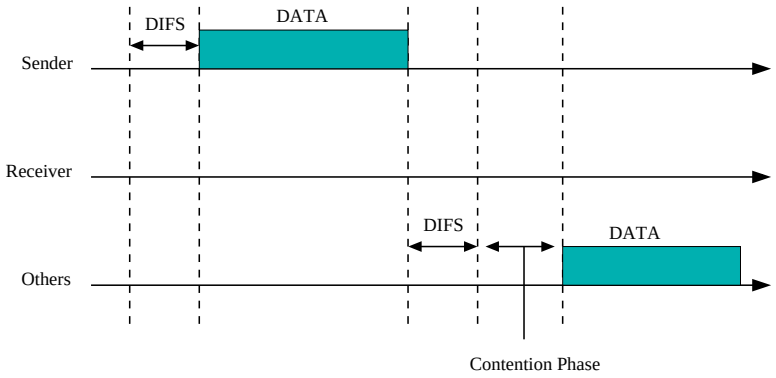


Figure 4. Timing diagram for IEEE 802.11 Multicast/Broadcast

receiver waits for a SIFS interval and then responds with a CTS expressing its willingness to participate in the communication. Following the reception of CTS packet, the sender proceeds with the DATA transmission as explained above. However, the sender starts DATA transmission after a SIFS interval instead of the DIFS time. The duration fields in the RTS and CTS packets are used to update the NAVs of the nodes surrounding the sender and receiver respectively. However, Xu et.al.,[XGB02] have shown that for sufficiently large distances between the sender and the receiver the receiver can still suffer packet loss owing to simultaneously transmission from nodes that do not hear the CTS packet. (See figure 3)

Multicast packets in IEEE 802.11 are directly transmitted without a preceding RTS-CTS handshake(Figure 4). Also, the recipients do not acknowledge the received DATA. Once the sender's NAV expires, the sender scans the channel for a DIFS duration. If the channel is idle for entire DIFS period then the sender broadcasts the multicast packet. At the end of transmission, it backs off and proceeds with the transmission of the next packet.

2. Routing Protocols

Routing protocols maintain routes to all the group members in multicast communication. Several routing protocols have been proposed. They are either proactive or reactive. In proactive protocols, routes to the group members are maintained all the time. In reactive routing protocols, the routes are built only when information must be delivered to the group members. Some protocols use a tree based approach whereas other use a mesh based approach. Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol (MAODV)[RP99] and On-Demand Multicast Routing Protocol (ODMRP)[YL02] are a two multicast routing protocols that have been commonly used for research in wireless ad hoc networks.

Gupta and Srimani[GBS00, GS99] have proposed two routing protocols, Minimum Spanning Tree (MST) and Shortest Path Spanning Tree (SPST) , which use the concept of self-stabilization in order to build routes in ad hoc networks. Self stabilization[Dij74, Dij86] uses local actions in order to reach a global legitimate state in the event of intermittent faults. Self stabilizing routing protocols treat node mobility and link failures as intermittent faults and rebuilds the tree using local actions. In both protocols, four basic modules are used to build the multicast tree:

- **Neighbor Discovery Protocol** Neighbor discovery protocol identifies the node neighbors. Each node periodically broadcasts a beacon message periodically. On receiving a broadcast message a node gets cognitive about its neighbors.

- **Link Quality Monitor** Link quality monitor monitors the link characteristics.

- **Link Cost Estimator** Each link has a unique cost associated with it. Link cost estimator estimates the link cost. The protocols use lexicographic information in order

to build unique weights as follows. Let i and j be the identities of the nodes forming the link, $LinkWght_{ij}$ is the link weight between nodes i and j and $UniqueWght_{ij}$ be the unique link weight between nodes i and j.

$$UniqueWght_{ij} = LinkWght_{ij} + (i \times 10^{-1}) + (j \times 10^{-2}) \tag{3.1}$$

- **SSMP controller** The SSMP controller incorporates fault containing strategies.

The way in which the paths a constructed are different MST and SPST. In MST, the path between two nodes is the path with the minimum α cost. α cost of the path is the maximum weight of all links along the path. In SPST, the path between any two nodes is the path with the minimum sum of individual links. We have used SPST for routing packets in multi-hop networks. The reason for this choice is twofold.

- Gupta and Ganesh[SG03] have shown that SPST has better data delivery ratio compared to MAODV, ODMRP and MST.
- We wanted to observe the behavior of self stabilizing routing protocols for reliable medium access control (MAC) layer

2.1. Shortest Path Spanning Tree Protocol (SPST). SPST builds the multicast tree in the following manner. Whenever the tree structure is perturbed owing to the mobility of nodes, the algorithm is automatically triggered in order to rebuild the tree. Every node periodically sends out beacon messages which carries information regarding the state of the nodes. Neighbor nodes use this beacon information to build a global system knowledge. Using the information provided by the beacon messages, every node computes the minimum possible weight of each and every path to the source root. It then chooses that path with the minimum weight($MinPWght_{ir}$) to connect to the root r. Assuming the edge

weights of a graph are unique, the graph has a unique shortest path spanning tree[HS84]. Once the tree has stabilized, the level of each node is determined in the tree. Any node that has one multicast node or a forwarding node as its child is considered as a forwarding node. Forwarding nodes forward the packets to its children while each multicast group member absorbs the data packets. Note that any multicast group member node can also be a forwarding node. Also, whenever the tree structure is perturbed owing to the mobility of nodes, the tree is automatically rebuilt using the information in the beacon message. For details regarding the proof of self-stabilization refer to [GBS00]. Algorithm 1 describes the working of SPST.

3. Assumptions

We have made the following assumptions:

- a single-channel multi-access wireless network consisting of a homogeneous nodes i.e., all nodes have the same processing and transceiver capabilities.
- group membership does not change at any time. Such changes should be handled by the higher layers.
- all links are symmetric i.e., if node A is the neighbor of node B then, node B is node A's neighbor.
- all nodes have infinite buffering capabilities.

Algorithm 1: SPST algorithm

At node i:

while *received beacon message from node* j **do**

if *received a beacon message from neighbor node* j **then**

update list of neighbors with node j

if *node* i *is the root* **then**

$MinPWght_{ir} \leftarrow 0$

$Parent_i \leftarrow null$

else

if $MinPWght_{ir} < (UniqueWght_{ij} + MinPWght_{jr})$ **then**

$MinPWght_{ir} \leftarrow (UniqueWght_{ij} + MinPWght_{jr})$

$Parent_i \leftarrow j$

end

end

end

end

CHAPTER 4

Protocol Description

In this chapter we give detailed description of our protocol, RDNP. We present a qualitative analysis of the behavior of RDNP in wireless LANs. We also present a modified version of RDNP, M-RDNP in order to cater to the needs of wireless ad hoc networks. Finally, we also present a summary of modifications to be made to the IEEE 802.11 standard in order to implement our protocol. Though most of the terminology used in our protocol description has been defined as a part of IEEE 802.11 MAC in chapter 3, we shall present a brief redefine some terminology before describing our protocol.

1. **Slot Time** Smallest unit of time in IEEE 802.11.

2. **Inter Frame Space (IFS)** Duration of physical carrier sensing at the end of virtual carrier sensing between frame transmissions. Helps prioritize data. IEEE 802.11 defines four inter frame spaces: DIFS, SIFS, PIFS and EIFS. Refer to table 2 for typical values of inter frame spaces.

3. **Network Allocation Vector (NAV)** All time is slotted in terms of the slot time. NAV is a timer that is used to perform virtual carrier sensing. A node can access the channel only when its NAV is 0. The duration field in every packet or a random backoff value is used to update the NAV value. The NAV is decrement once every

slot time.

4. **Contention Window (CW)** The window from which a random backoff value is chosen is called the contention window. The minimum value and maximum values for the CW are called CWMin and CWMax respectively.

5. **Exponential Backoff** If the channel access is successful then the CW is set to the CWMin value and the NAV is set to some random value from the contention window. If the channel access is unsuccessful then the CW in doubled and the NAV is set to some random value from the contention window. The node does not access the channel again until the NAV expires.

1. Detailed Description - RDNP

When a node wants to send a multicast data packet, it waits for its NAV to expire. Once its NAV expires, it senses the channel for a DIFS duration. If the channel is idle for the entire DIFS duration it transmits a multicast RTS packet. Otherwise, the sender doubles its CW, and performs an exponential backoff. Apart from the normal fields in a RTS packet, the multicast-RTS packet contains the sequence number of the data packet for which the RTS is being sent (Refer to Figure 11). All neighbors, group and non group, which receive the RTS packet, update their NAVs using the duration field of the RTS packet. In addition, group neighbors

1. use the sequence number in the RTS packet to decide if they already have the packet. If they already have the packet they do not try to recover the packet in case the packet is corrupted.

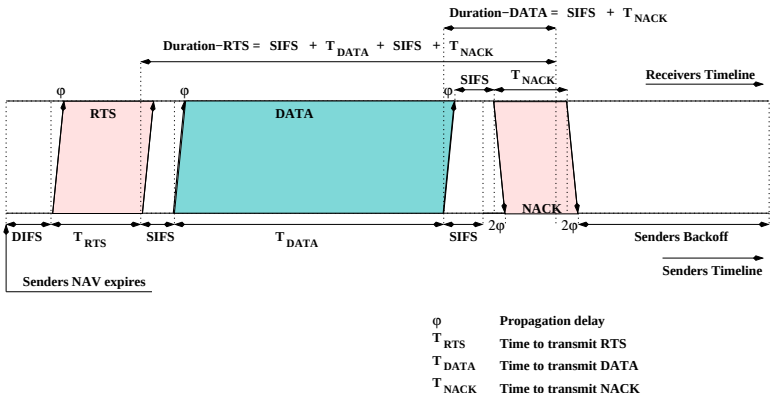


Figure 5. Timing diagram for RDNP

2. use the duration field to determine when they should send a NACK packet if the packet is not received correctly.

This is described in the steps [RTS] and [End of RTS] of algorithm 2.

After transmitting the RTS packet the sender senses the channel for a SIFS duration. If the channel is idle for the SIFS duration the sender transmits the data packet as shown in step [DATA] of algorithm 2. Otherwise it doubles its CW, and performs an exponential backoff. Non group neighbors and neighbors which already have the same data packet, ignore the data transmission. If the packet is not a retransmission and it is corrupted then group neighbors send a NACK packet as shown in step [NACK] of algorithm 2 *SIFS* units after the supposed end of the DATA transmission. If the sender receives a NACK packet or perceives a busy channel during the NACK slot it performs an exponential backoff with a doubled CW and retransmits the same packet. Otherwise it sets its CW to CWMin and backs off to transmit the next packet in the queue if any.

The main advantages of RDNP are as follows.

1. In protocols like LBP, PBP and DBP changes in the number of neighbors within a wireless LAN can affect the performance of the protocol. Our protocol performance

is unaffected by such changes.

2. Performance of RDNP is not affected by the corruption of feedback packets. There are no CTS packets and fields of the NACK packet do not carry any valuable feedback information. The absence or presence of the NACK provides the necessary feedback information. Corruption of the NACK packet does not have an adverse effect on the protocol behavior. In other words, a NACK packet and a corrupted NACK packet both produce the same effect: retransmission of the last packet transmitted. For every packet transmitted, a NACK is sent only once by a node and it is sent *SIFS* units after the DATA is received. Figure 5 shows the timing diagram for our protocol.

1.1. Problems and Solutions. RDNP does not recover from losses when

- Both RTS and DATA packets are lost at the receiver. This problem is persistent in almost all multicast protocols discussed in chapter 2.
- NACK packets are lost

The only way to recover from such errors is by requesting a retransmission of the packet when the next packet is seen. We assume that such retransmission requests are handled by the higher layers.

Algorithm 2: Protocol RDNP

[**RTS in Slot 1**] Sender $\longrightarrow$ Receivers

if *channel idle for DIFS duration* **then** send multicast-RTS

else CW $\leftarrow$ CW *2 , backoff and repeat RTS Transmission

[**End of RTS**]

Non-group neighbors: Update NAV with duration field in RTS

Group neighbors: Update NAV with duration field in RTS and wait for data

[**DATA from Slot 2 to Slot D + 2**] Sender $\longrightarrow$ Receivers

if *channel idle for SIFS duration* **then** send multicast-data

else CW $\leftarrow$ CW *2 , backoff and goto RTS Transmission

[**End of DATA**]

Sender: Wait for NACK by sensing the channel in Slot D+2

Non-group neighbors: Ignore data packet

Assume that data packets requires D slots

[**NACK in Slot D + 3**] Group Neighbor $\longrightarrow$ Sender

if *packet not corrupt or already have packet* **then** do nothing

else send NACK

[**End of NACK**]

Sender

if *got NACK or sensed a busy channel during slot D+2* **then** CW $\leftarrow$ CW * 2 , backoff and goto Step A

else CW $\leftarrow$ CWMin , backoff and goto Step A for next queued packet

2. Qualitative Analysis of RDNP in Wireless LANs

In this section we show how RDNP can be directly extended to work with IEEE 802.11 LANs. We assume that every cell communicates at a different channel. Hence there is no interference from adjacent cells. This implies that there can be no hidden terminals problems due to nodes from adjacent cells. All communication has to go through the base station. This greatly simplifies our channel access problems. Since nodes outside the cell coverage do not cause hidden terminal and all nodes within the cell can hear the base station, the need for CTS packet is eliminated. The protocol semantics is such that multicast has higher priority compared to unicast. This is demonstrated in the following section.

2.1. Co-existence with other traffic in Wireless LANs. In this section, we examine the behavior of our protocol in the presence of other traffic in wireless LANs. The base station wants to send multicast traffic and other nodes in network try to send data to the base station. If one of the contenders gains access to the channel, then the other will suppress its transmission because of physical carrier sensing. We will take a closer look at what happens if the base station and its contender try to access the channel simultaneously.

1. **Multicast and Unreliable-Unicast:** Consider the scenario when the base station starts the multicast RTS and one of the network nodes starts transmitting the unicast data(without RTS-CTS) to the base station simultaneously. The base station will not be able to receive the unicast data packet from the unicast sender because of its own multicast RTS transmission. If the size of the unicast data packet is greater than the multicast RTS packet, the unicast sender will still be transmitting the data packet even at the end of the multicast RTS packet transmission. The base station will suppress its multicast data transmission because of a busy medium caused by the

unicast data. If the size of the unicast data packet is less than the size of the multicast RTS, the base station will proceed with the multicast data transmission. In either case the multicast receivers do not lose a packet. However, the base station will not receive the unreliable unicast packet sent to it.

2. **Multicast and Reliable-Unicast:** Consider the scenario when the base station starts the multicast RTS and one of the network nodes starts transmitting unicast RTS to the base station simultaneously. The unicast transmission will not be successful because the base station will not send a CTS packet in response to the unicast RTS. Only the multicast communication will go through. Even though the unicast sender might not hear the multicast RTS it will not interfere with the multicast data transmission from the base-station because of physical carrier sensing. Thus the protocol semantics gives higher priority to multicast transmission over unicast transmissions.

3. **Multicast and Multicast/Broadcast:** These scenarios are not possible because only the base station can start a multicast/broadcast transmission and there is only one base station per cell.

3. M-RDNP for Ad Hoc Networks

In situation when there are no hidden terminals problems because of a centralized controller like a base station RDNP operates very well. However, this is not the case in wireless ad hoc networks. There is no centralized controller and there can be simultaneous transmissions, thereby leading to hidden terminal problems. Recently, Gerla et.al.,[XGB02] have shown that RTS-CTS does not always solve hidden terminal problems. Based on their observation we have classified the area around the sender into four regions. In the following

sections, we shall describe the reliability of the data delivered to nodes in each of the four regions. We also propose slight modifications to RDNP in order to overcome some of the identified problems.

3.1. Classifying the area around a transmitter. The strength of a signal fades as the distance between the sender and receiver increases. For a **two-ray ground** propagation model with the distance separating the transmitter and receiver given by d, we have reception power (P_r)[Rap96] given by,

$$P_r = P_t G_t G_r \frac{{h_t}^2 {h_r}^2}{d^4} \tag{4.1}$$

where,

P_t power with which a node transmits a packet.

G_t, G_r antenna gains of the transmitter and receiver respectively.

h_t, h_r antenna heights of the transmitter and receiver respectively.

Signal with strength lesser than the reception threshold will be perceived as noise by the transmitter. The distance at which the signal strength fades to the reception threshold is called the reception range(RX). Similarly, signals with strengths lesser than the noise threshold will be not be detected by the antenna. The distance at which the signal strength fades to the noise threshold is called the noise range(CS). A signal at a receiver will be a combination all transmissions around the receiver. Consider the scenario when a receiver is interested in signal from a particular source. We shall call all other transmissions as noise. The signal from source can be picked up only if the signal to noise ratio is greater than the signal-to-noise threshold (SNR_T). Note that since all the nodes are homogeneous, they have the same radio parameters: P_t, G_t, G_r, h_t, h_r.

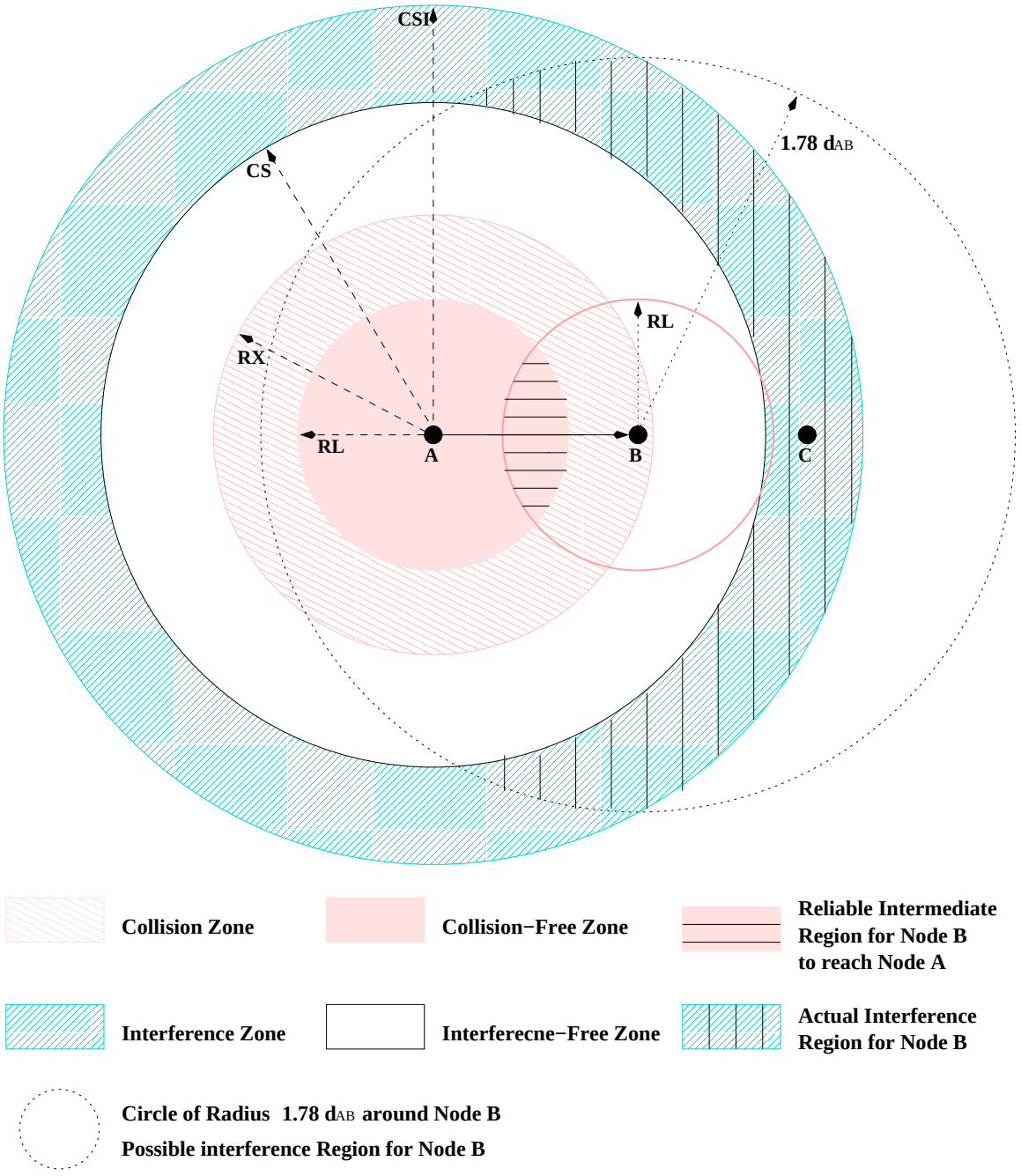


Figure 6. Reliable region and Unreliable region

Let -

$P_{r(A,B)}$ be the strength of signal at receiver B from sender A.

d_{AB} distance between node A and node B.

Consider the following scenario (See Figure 6), in which node A is transmitting data to node B. At the same time, node C is also transmitting packets to another node. If node B has to successfully receive node A's transmission,

$$\begin{aligned} \frac{P_{r(A,B)}}{P_{r(C,B)}} &\geq SNR_T \\ (\frac{d_{BC}}{d_{AB}})^4 &\geq SNR_T \\ d_{BC} &\geq d_{AB} \times \sqrt[4]{SNR_T} \end{aligned} \tag{4.2}$$

This means that, for node B to successfully receive node A's transmission, all nodes transmitting simultaneously as node A must be at least $d_{AB}\sqrt[4]{SNR_T}$ meters away from node B (Refer to [XGB02]).

Because of physical carrier sensing, in IEEE 802.11 LANs, a receiver will not try to access the channel as long as a node within its noise range is transmitting[Com99]. In other words, no node within a radius of CS from sender A will access the channel during sender A's transmission. If node C is within a distance of CS from node A then node B will not experience any collision. Thus, there is a region around sender A within which no node will experience hidden terminal problems, because of physical carrier sensing. We call this region as the **collision-free zone**. Let RL denote the radius of this region. In order to determine RL we set $d_{AC} = CS$. Thus $d_{BC} = CS - d_{AB}$ and

$$d_{AB} = \frac{CS}{\sqrt[4]{SNR_T} + 1}$$

Normally, SNR_T is set to 10[XGB02] and d_{AB} now represents RL. Thus,

$$RL = \frac{CS}{2.78} \tag{4.3}$$

A receiver (say node B) which can receive any transmission from a sender (say node A), is farthest from the sender when $d_{AB} = RX$. In order to determine the farthest distance from a sender (node A) at which an interfering node (node C) can interfere with node A's transmission at the farthest receiver (node B, $d_{AB} = RX$), we need to find the farthest distance of interfering node (node C) from the receiver (node B) for which the receiver (node B) will experience collisions. We shall call the region around a sender within which nodes can interfere with the reception at any receiver as the **interference zone**. Let CSI denote the radius of this region. Substituting for d_{BC} in equation 4.2 we get,

$$d_{AC} \quad = \quad d_{AB}(\sqrt[4]{SNR_T} + 1)$$

Substituting for SNR_T, d_{AB} and d_{AC} we get

$$CSI = 2.78 \times RX \tag{4.4}$$

From the above analysis, we can observe that the area around a transmitter can be defined in terms of four ranges. The RX, CS, RL and CSI. Using these ranges, the area around a transmitting node (say node A) can be classified into four basic zones (nodes in each zone can affect or can be affected by the transmission in a different way. See **Fig.6**).

1. **Collision-Free Zone**: This is the region around the sender within which no receiver suffers from hidden terminal problems. Nodes in this region are called **reliable neighbors** of node A. The radius defining this region is denoted as $RL = \frac{CS}{2.78}$ and the area of this region is given by

$$A_{RL} = \pi RL^2$$

2. **Collision Zone**: This is the region around the sender within which a node can receive the transmission from the sender, but might lose the packet due to collisions from hidden terminals. Nodes in this regions are called **unreliable neighbors** of node A. The radius defining this region is denoted as RX and the area of this region is given by,

$$A_{RX} = \begin{cases} 0 & : \quad RL >= RX \\ \pi \times RX^2 - A_{RL} & : \quad RL < RX \end{cases}$$

3. **Interference-Free Zone**: This is the area between the noise range and the reception range. No node in this region will transmit as long as node A is transmitting. Nodes in this region are called **non-interfering nodes** for node A. Also, nodes in this region will not be able to decipher the transmission from node A. The radius defining this region is denoted as CS and the area of this region is given by,

$$A_{CS} = \begin{cases} 0 & : \quad RX >= CS \\ \pi \times CS^2 - \pi \times RX^2 & : \quad RX < CS \end{cases}$$

4. **Interference Zone**: Nodes within this region will cause hidden terminal problems to nodes in the unreliable region. Nodes in this region are called **interfering nodes** for node A. The radius defining this region is denoted as $CSI = 2.78 \times RX$ and the area of this region is given by,

$$A_{CSI} = \begin{cases} 0 & : \quad CS >= CSI \\ \pi \times CSI^2 - \pi \times CS^2 & : \quad CS < CSI \end{cases}$$

From the above equations, it is clear that the reliable range (RL) depends solely on the noise range (CS) and the interference range (CSI) depends solely on the transmission range (RX).

3.2. Severity of hidden terminal problems with variation in the distance and CS. In paper [XGB02], Xu, et.al., analyze the effectiveness of RTS-CTS. Their analysis does not consider the effect of CS and CSI described above. In this section, we shall see how the distance between the sender and receiver, CS and CSI affect the severity of the hidden terminal problems experienced by the receiver. For a receiver at a distance of d from the sender, we identify the area within which nodes can interfere with the reception. Let node A be transmitting to node B and d_{AB} be the distance between them. Node B will experience collisions as long as a node within a radius of $1.78 \times d_{AB}$ transmits at the same time. We shall represent this region as **possible interference around B**(dotted circle around node B in Figure 6). Because of the four regions surrounding node A, the **actual interference area around B** can be a lot less than the possible interference around B. The actual interference region around node B is given by equation 4.5.

d_{AB} equal to d.

I_d actual interference area affecting by a receiver at a distance of d from the sender.

IP_d possible interference area affecting a receiver at a distance of d from the sender with radius $R_{IP}(R_{IP} = 1.78 \times d)$

$I_{B,CSI}$ possible interference area that does not intersect with the senders CSI region

$I_{B,CS}$ possible interference area that does not intersect with the senders CS region

$A_{(N1,r1)\cap(N2,r2)}$ area of intersection between two circles centered at nodes N1 and N2 having radius $r1$ and $r2$ respectively

$$I_{B,CSI} = IP_d - A_{(A,CSI)\cap(B,R_{IP})}$$

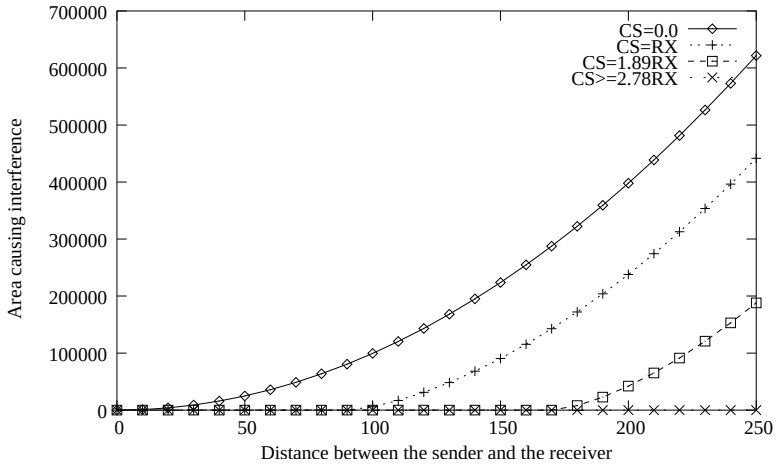
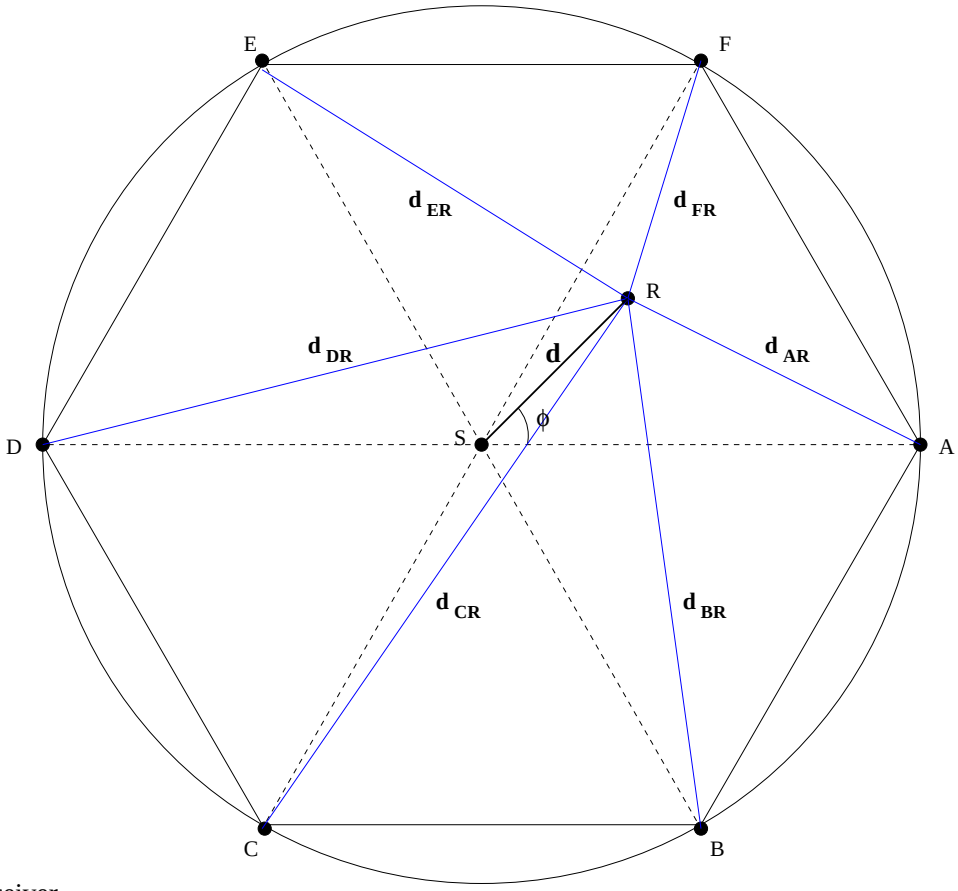


Figure 7. Actual Interference Area Vs. Distance between Sender and Receiver

$$\begin{aligned} I_{B,CS} &= IP_d - A_{(A,CS)\cap(B,R_{IP})} \\ I_d &= \max(I_{B,CS} - I_{B,CSI}, 0) \end{aligned} \tag{4.5}$$

Note that $IP_d = A_{(A,CSI)\cap(B,R_{IP})}$ because $max(d) = RX$ and $CSI = 2.78 \times RX$. Therefore, the possible interference around B is completely contained within the interference rangeCSI of A. Thus $I_{B,CSI} = 0$ and $I_d = \max(I_{B,CS}, 0)$

In order to observe the area that can cause interference for a receiver, we plot equation 4.5 for varying distances between the sender and the receiver. The X-axis is the distance between the sender and the receiver and the Y-axis shows actual interference area with RX=250. From figure 7 it can be observed that, as the distance between the sender and the receiver increases, the area which causes hidden terminal problems with the receiver increases. We also observed the actual interference area for different values of CS. Larger the noise range, smaller the collision area. Ideally, we would like $CS = 2.78 \times RX$ such that $RX = RL$. However, the values of RX and CS are dependent on the hardware used. Thus in the following sections we shall provide software solutions to provide reliable transmission. However, a large noise range reduces the overall throughput[XGB02] for



R receiver
S sender
A B C D E F interfering nodes
d distance between the sender and receiver

Figure 8. A Sender: S, a Receiver: R and the Interfering Nodes: A,B,C,D,E,F

unicast traffic through increased exposed terminal problems.

3.3. Lower Bound on the Reliable Radius. In the previous sections we have measured the reliable radius for only one interfering node. However, this might not be the case all the time. As the number of interfering nodes increase, the reliable radius decreases. In this section we measure the lower bound on the reliable radius.

Consider the scenario where a node S is transmitting to node R. Any other node, say

node A, transmitting simultaneously as node S must be at a distance of CS from the node S. A third node, say node B, which is transmitting simultaneously as node S and node A must be at a distance of CS from node A and node S. These three nodes, which are equidistant from each other, are closest to each other when they form the vertexes of an equilateral triangle. In the same we can have at most seven nodes transmitting simultaneously around a receiver. This scenario is depicted in Figure 8. Though there can be other nodes beyond the first CS circle transmitting simultaneously, we shall ignore these transmission because of their signal strengths at the receiver R are negligible. In figure 8, node S is the sender. Node R is the receiver. Nodes A, B, C, D, E and F are the interfering nodes. The interference is maximum when the effect of the interfering signals is additive. Node R can receive the signal from node S only when the SNR is greater than or equal to 10. Let d be the distance between node S and node R and let $d_{AR}, d_{BR}, d_{CR}, d_{DR}, d_{ER}, d_{FR}$ be the distance of node A, node B, node C, node D, node E and node F from node R respectively. Also, let θ be the angle between line segments SR and SA. Let P_{SR} be the signal strength from the sender A at node R and let $P_{AR}, P_{BR}, P_{CR}, P_{DR}, P_{ER}, P_{FR}$ be the signal strengths from A, B, C, D, E and F at node R respectively. Then,

$$SNR = \frac{P_{SR}}{P_{AR} + P_{BR} + P_{CR} + P_{DR} + P_{ER} + P_{FR}} \tag{4.6}$$

Substituting for signal strengths using equation 4.1, we get

$$SNR = \frac{\frac{1}{d^4}}{\sum_{i=A,B,C,D,E,F} \frac{1}{d_i{}^4}} \tag{4.7}$$

Table 1 shows the distance of receiver from every interfering node. By substituting these values in Equation 4.7 and varying θ and d we can find the lower bound on the reliable radius. For all values of θ, the minimum reliable radius is given by the distance minimum d for which the SNR is equal to 10. From figure 10, it is observed that the lower bound for

Table 1. Relating the Receiver and the Interfering Nodes: Distances and Signal Strengths

Distance			Signal Strength		
d_{AR}	=	$\sqrt[2]{(d \times \sin(\theta))^2 + (CS - d \times \cos(\theta))^2}$	P_{AR}	=	$P_t G_t G_r \frac{{h_t}^2 {h_r}^2}{{d_{AR}}^4}$
d_{BR}	=	$\sqrt[2]{(CS \times \sin(60 + \theta))^2 + (d - CS \times \cos(60 + \theta))^2}$	P_{BR}	=	$P_t G_t G_r \frac{{h_t}^2 {h_r}^2}{{d_{BR}}^4}$
d_{CR}	=	$\sqrt[2]{(d \times \sin(60 - \theta))^2 + (CS + d \times \cos(60 - \theta))^2}$	P_{CR}	=	$P_t G_t G_r \frac{{h_t}^2 {h_r}^2}{{d_{CR}}^4}$
d_{DR}	=	$\sqrt[2]{(d \times \sin(\theta))^2 + (CS + d \times \cos(\theta))^2}$	P_{DR}	=	$P_t G_t G_r \frac{{h_t}^2 {h_r}^2}{{d_{DR}}^4}$
d_{ER}	=	$\sqrt[2]{(d \times \sin(120 - \theta))^2 + (CS - d \times \cos(120 - \theta))^2}$	P_{ER}	=	$P_t G_t G_r \frac{{h_t}^2 {h_r}^2}{{d_{ER}}^4}$
d_{FR}	=	$\sqrt[2]{(d \times \sin(60 - \theta))^2 + (CS - d \times \cos(60 - \theta))^2}$	P_{FR}	=	$P_t G_t G_r \frac{{h_t}^2 {h_r}^2}{{d_{FR}}^4}$

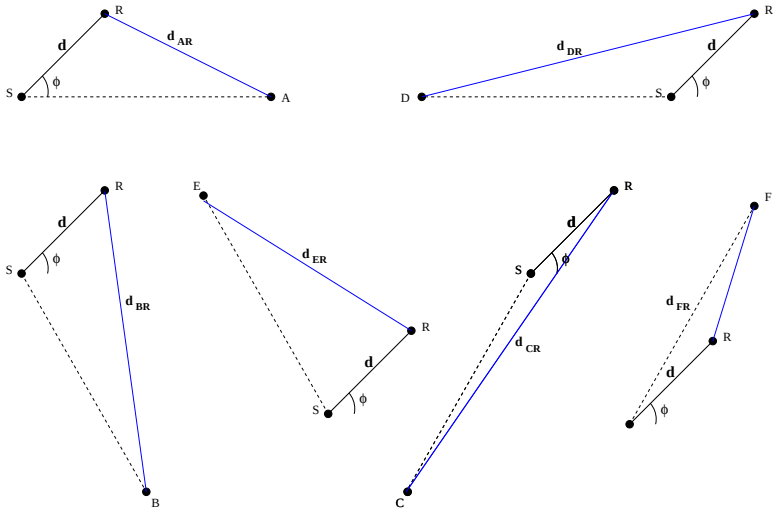


Figure 9. Calculating the distance between the receiver R and the interfering nodes

minimum reliable radius is around $170m$ for $CS = 550m$

3.4. M-RDNP for multicasting ad hoc networks. As explained in the previous sections, nodes within the collision free zone of a sender will not suffer from hidden terminal problems. Nodes within the collision zone can suffer from hidden terminal problems. This means the when using RDNP, receivers within the collision zone will experience collisions due to hidden terminals within its interference zone. However, nodes within the collision free zone of the multicast sender do not experience collisions. They might lose packets

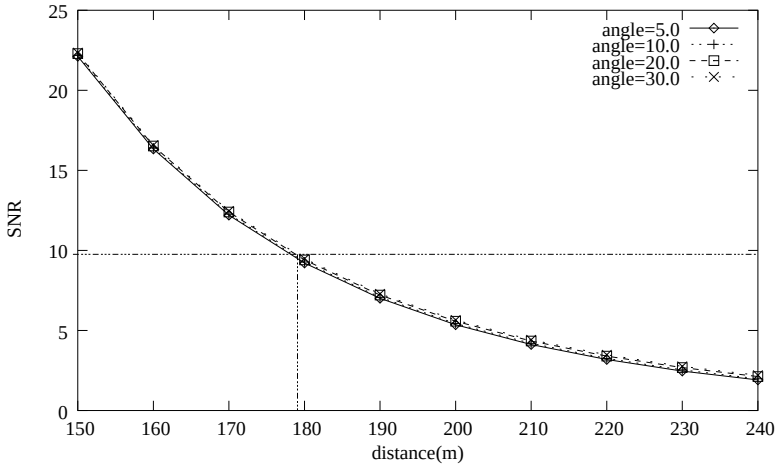


Figure 10. Minimum Reliable Radius

from transmission errors which will be recovered by the NACK. In order to overcome this problem, we suggest building routes using only reliable neighbors. This might increase the dis-connectivity of the network for scarcely populated networks. However, it increases the reliability of transmissions for densely populated networks. This can easily achieved by dropping all routing packets which arise from unreliable neighbors at the MAC layer. This way the routing protocols will be forced to build routes only using reliable neighbors.

The signal strength of a packet from a reliable neighbor should be at least

$$\begin{aligned} RL_T &= P_t G_t G_r \frac{h_t^2 h_r^2}{RL^4} = P_t G_t G_r \frac{h_t^2 h_r^2}{(\frac{CS}{\min RL})^4} \\ &= (\frac{550}{170})^4 \times NOISE_T \end{aligned} \tag{4.8}$$

where the $NOISE_T$ is the minimum signal strength required for a signal to be picked up by the receiver. This $NOISE_T$ defines the CS range. We shall call RL_T as the **reliable threshold**. If the signal strength of the packet received is less than the RL_T then it is dropped by M-RDNP at the link layer. This ensures that the routing layer builds a tree using reliable neighbors. We shall call this version of RDNP as M-RDNP.

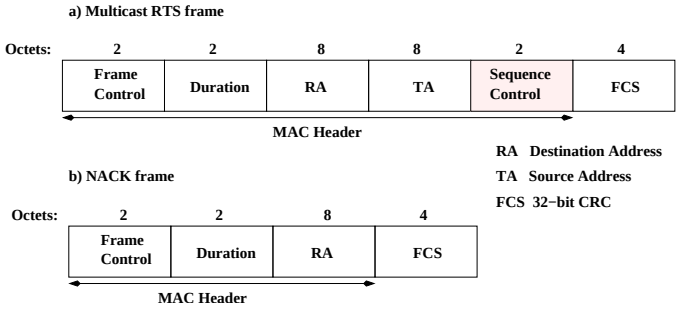


Figure 11. Frame Formats: Multicast RTS and NACK

4. Adapting our protocol to IEEE 802.11

Note that, IEEE 802.11 does not support reliable multicast or broadcast. RDNP can be easily adapted to IEEE 802.11 with slight modifications. The following changes need to be made to IEEE 802.11 to implement both RDNP and M-RDNP.

1. Add a packet sequence number in the RTS packet.

2. Suppress CTS packets transmission for multicast-RTS packets.

3. New packet type - NACK packet.

4. Send NACK packets if DATA is received incorrectly.

5. For M-RDNP, if signal strength of the packets received are lesser than the reliable threshold, then drop the packets.

CHAPTER 5

Simulation Results

This chapter describes the experiments conducted to study the performance of the proposed reliable multicast protocols and provides an explanation of the behavior of the protocols under different network conditions. The protocols have been compared using simulations in Network Simulator[FV]

The following are the performance metrics used to evaluate the performance of the protocols.

1. Performance Metrics

1. **Average Packet Drop Ratio per Node:** We measure the fraction of packets lost per receiver. This is equivalent to the average number of retransmissions required in order to recover from packet loss. The higher the average packet drop ratio, the lesser is the protocol reliability.

2. **Average Energy Consumed per Packet per Node:** Energy consumed when a packet is transmitted and when it is received. We measure the average energy consumed per packet per node in each protocol as the ratio of the total energy consumed to the total number of packets received by the node.

The objective of these experiments is to determine the protocol with the best performance for different network conditions. Another purpose of these experiments is to determine whether self stabilizing routing protocols benefit through the use of reliable MAC layer multicast.

Experiments were conducted for

- varying the bit error rate of the channel for both stationary and mobile nodes, introducing unicast traffic and measuring the end-to-end delay with higher layer error recovery for wireless LANs.
- varying mobility rate of nodes, varying number of multicast nodes and varying the bit error rate of the channel for ad hoc networks.

2. Network Simulator (NS)

The Network Simulator[Net02, FV] is a discrete event simulator.

- It provides support for network protocol performance evaluation in both wired and wireless network.
- It also provides support for implementing different routing protocols, medium access protocols, traffic generators and error models for both wired and wireless networks.

Several protocols come with the standard distribution of the simulator. NS is built in using two languages: C++ and OTCL. C++ is used to implement different protocol which requires a system programming language in order to efficiently manipulate bytes, packet headers, and implement algorithms that run over large data sets. For these tasks run-time speed is more important than turn-around time. OTCL is used to implement the initial

configuration and setup which requires low turn-around time. It also allows users to vary parameters and configurations easily. "tclcl" is used to interface between the two languages and make objects and variables appear on both languages.

The simulator takes as input the placement of the nodes in the network, the configuration of the nodes, traffic flows in the network and the duration for which the simulation has to be run. All this information is supplied through OTCL. Using this information, the appropriate object and event queue initialization is performed. Once the run command is issued, the simulator executes each event in the queue which might add or delete more events to or from the queue respectively.

The link layer has three subparts: MAC module, ARP module and Interface queue. For the purpose of this research we have implemented the following variations of the MAC module : LBP, PBP, DBP, RDNP, M-RDNP. Figure 12 shows the schematic model of a mobile node with our MAC and SPST extensions. All MAC modules have been implemented as a super class of the IEEE 802.11 MAC module supplied with the standard distribution of NS.

The input to the simulator is the simulation configuration file, the node mobility file and the connection pattern file. The simulation configuration files specify the protocols to be used at each layer, the topology of the network, and the channel model , error model and energy model to be used. The mobility file specifies the number of nodes in the network, the initial position of the nodes and the mobility of the nodes. The connection pattern specifies the group members using join and leave group messages and the traffic flow between the network nodes.

The output from the simulator is an energy trace file and several data reliability trace files. The energy trace file hold the information about the amount of energy consumed at

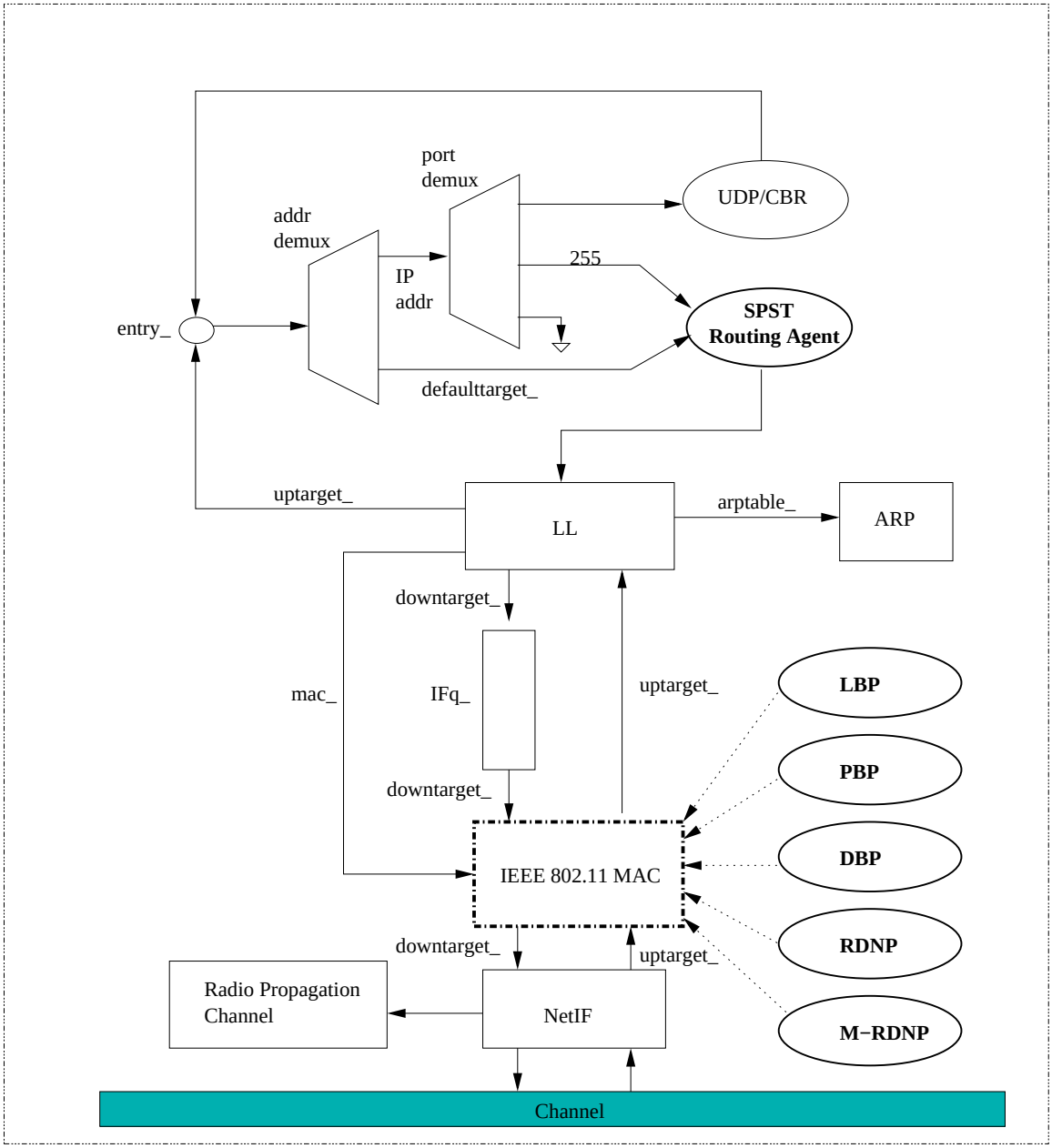


Figure 12. Schematic Model of a Mobile Node in NS[FV] with MAC and SPST extensions

Table 2. Physical Parameters used in Simulation

Parameter	*Value*
CP (capture) Threshold	10.0dB
CS (noise) Threshold	1.559e-11
RX (receive) Threshold	3.652e-10
Transmission range	250m
Noise range	550m
Frequency	914e+6
Power Consumed for transmission	0.660W/s
Power Consumed for reception	0.395W/s
Power Consumed for idle state	0.035W/s
SIFS Time	$10\mu s$
PIFS Time	$20\mu s$
DIFS Time	$50\mu s$
Data Payload	512bytes

every node. The reliability trace files contain information about the sequence number of every packet received, the time at time the packet was received and the address of the node from which sent the packet for every node. By parsing these files we calculate the desired performance metrics.

3. For Wireless LANs

All the simulation results presented below have been averaged over forty five trial runs. We have studied the performance of the protocols for five different scenarios as described below. Under ideal operating conditions(stationary nodes, no channel errors) the maximum achievable throughput of IEEE 802.11($\approx 1.56 Mbps$), RDNP($\approx 1.36 Mbps$), LBP($\approx 1.30 Mbps$), DBP($\approx 1.04 Mbps$) and PBP($\approx 0.79 Mbps$) is inversely proportional to the control byte overhead.

Scenario 1 - Channel with bit errors and stationary nodes. In this scenario, 1) all hosts are stationary, and 2) packets are prone to bit errors varying from 1×10^{-6} to 100×10^{-6}. Figure 13 shows the reliable throughput for such a scenario. Though the

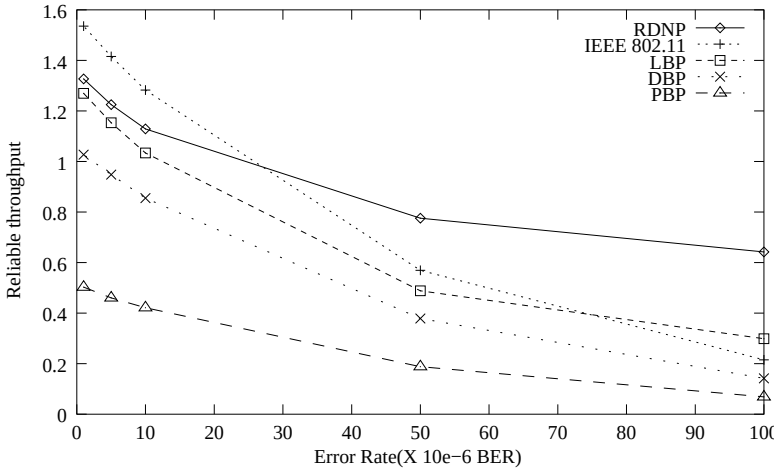


Figure 13. Reliable Throughput Vs. BER, nodes=40

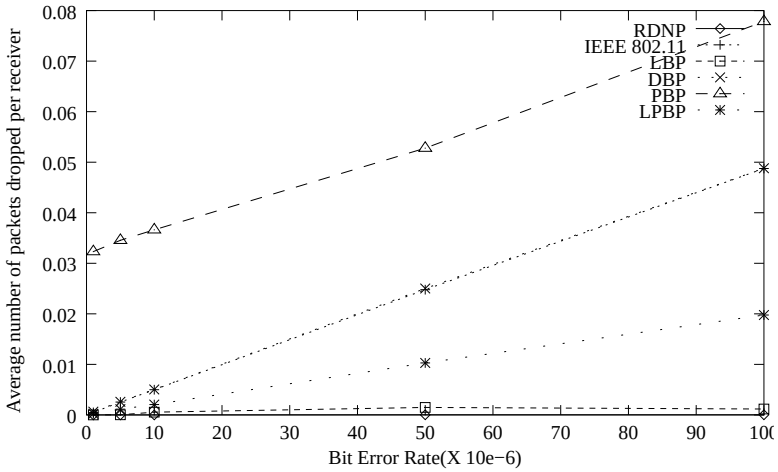


Figure 14. Average Drop Ratio Vs. BER, nodes=40

throughput of IEEE 802.11 is high when the error rate is low, it drops sharply as the error rate increases. On the other hand, RDNP has a good throughput even when channel has a high bit error rate (BER). When $BER \approx 30 \times 10^{-6}$, the throughput of RDNP is equal to that of IEEE 802.11 multicast. For all increasing BERs, the throughput of RDNP is higher than IEEE 802.11 multicast.

Figure 14 shows the variation in the average number of drops per packet in any receiver. Receivers in RDNP and LBP do not lose many packets because they immediately recover from such losses by sending NACK packets. Closer observation of the graph reveals that LBP does lose a few packets. This can be caused by capture effect. Consider the scenario when the leader node sends an ACK and one of the other receivers sends a NACK. If the distances of the leader and the receiver, from the sender, are such that $\frac{P_{ACK}}{P_{NACK}} > SNR_T$, where P_{ACK} is the power of reception of the ACK packet, P_{NACK} is the power of reception of the ACK packet, then the ACK packet is processed successfully(NACK is dropped). In such a case the packet is not retransmitted and the receiver that sent the NACK does not recover from its loss. DBP, PBP and IEEE 802.11 multicast exhibit an increase in the drop rate as the channel BER increases. This behavior can be easily explained by lack of local error recovery in DBP, PBP and IEEE 802.11 Multicast.

Scenario 2 - Channel with bit errors and mobile nodes. In this scenario, 1) all nodes exhibit random way point motion[JMIK96]. A node does not change its speed of motion during the simulation. However, the speed of a node can range from 1m/s to 10 m/s. Nodes can move in and out of the cell at any time. 2) packets are prone to bit errors varying from 1×10^{-6} to 100×10^{-6}. In this scenario, we measure the average packet drop ratio per receiver (See Figure 15). As nodes move in and out of the cell, they affect the reliability of packets delivered. In RDNP and IEEE 802.11 a mobile node can only lose

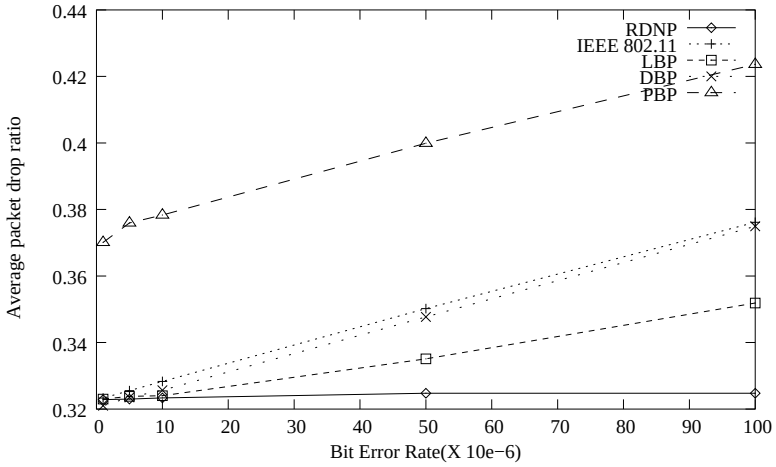


Figure 15. Average Drop Ratio Vs. BER, nodes=40

its own packets and will not affect other nodes in the cell. However, in LBP, PBP and DBP a mobile node not only loses its own packets but it can also affect the throughput of the cell that it moved out of. In LBP there can be unnecessary retransmissions until the leader movement is discovered. In PBP and DBP the probability and delay parameters need to reflect the number of nodes in the receivers[KK01] for optimal performance. Thus, it is observed that RDNP has the least packet drop ratio(Figure 15). This value remains a constant with respect to the channel BER because all corrupted packets are retransmitted by NACK transmissions. Packets lost due to mobility must be recovered by the routing layer.

Scenario 3 - Performance with link-level retransmissions. In this scenario, we have turned on higher layer retransmission requests for every protocol. Any packet lost by the MAC layer is recovered using explicit retransmission requests. We then observe the delay experienced by high layers. From Figure 16 we can see that the end-to-end delay per packet is the least for RDNP and the highest for IEEE 802.11 multicast. This shows that RDNP preserves the order to data delivery. The end-to-end delay of LBP is slightly more

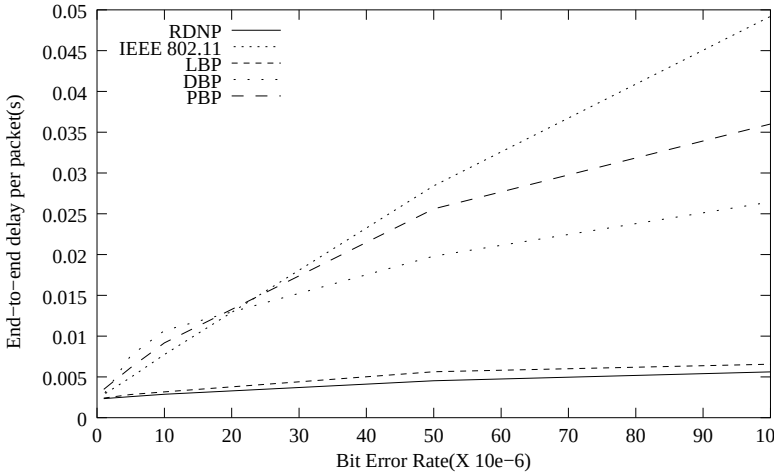


Figure 16. End-to-End Delay per Packet Vs. BER, nodes=40

than that of RDNP.

Scenario 4 - Performance with other traffic. So far we have seen how reliability is affected by channel errors and node mobility with just one sender, the base station. We now see how interference affects the reliability of the protocols. We test the performance of the protocols by increasing the number of nodes contending for the channel. The base station multicasts packets to the group nodes and the contending nodes try to send unicast packets to the base station. Figure 17 and Figure 18 shows the packet drop ratio per node and the reliable throughput respectively.

From Figure 17 it can be observed that RDNP and LBP have the least drop count, while IEEE 802.11 drops most of the packets. This is because both RDNP and LBP enforce reliability at the MAC layer, while IEEE 802.11 multicast does not perform any kind of error recovery at the MAC layer. In IEEE 802.11, if the base station and one or more contenders start transmission at the same time then there is a collision of the multicast-DATA and the unicast RTS. The multicast transmission is corrupted and the unicast transmission is suppressed. Thus, they have the highest percentage of packet drops per node. Also, from

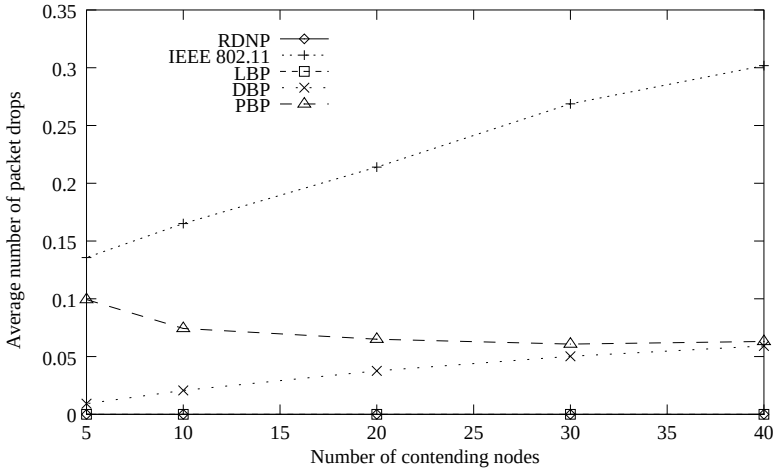


Figure 17. Packet Drop Ratio Vs. Number of contending nodes, BER=0

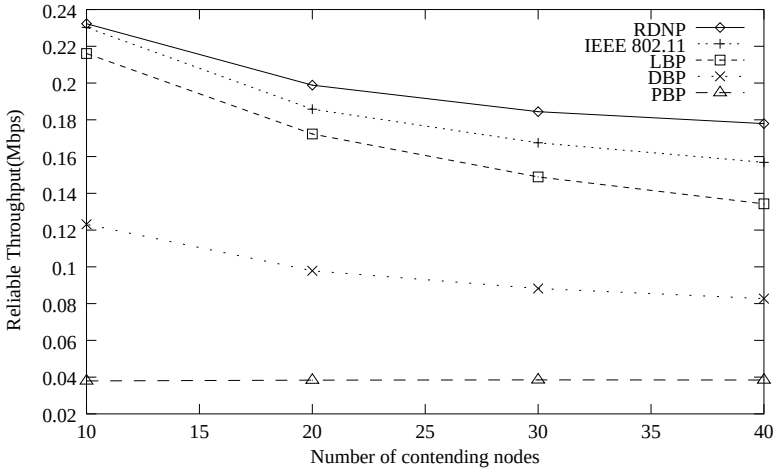


Figure 18. Reliable Throughput Vs. Number of contending nodes, BER=0

Figure 18 it can be observed that RDNP has the highest throughput.

4. For Wireless Ad Hoc Networks

This section illustrates the performance of the protocols in ad hoc networks. We compare the performance of IEEE 802.11, RDNP and M-RDNP for both stationary and mobile ad hoc networks. All the simulation results presented below have been averaged over forty five trial runs in order to achieve a 5% accuracy for a 99% confidence interval[Jai91].

We have studied the performance of the protocols for three different scenarios as described below.

4.1. Scenario 1 - Stationary Ad Hoc Networks. In this scenario,

- All hosts are stationary
- The number of hosts in an area of 1000×1000 is varied in steps of 10, 20, 30, and 40. This averages to a neighbor node density of 1.8, 3.6, 5.4 and 7.2 respectively
- The channel BER is varied from 1 in 10^5 to 10 in 10^5.

Figure 19, figure 20, figure 21 and figure 22 shows the average packet drop ratio per node when the number of nodes in the network are 10, 20, 30 and 40 respectively. In all cases, performance of M-RDNP is better than RDNP and IEEE 802.11. Also, the performance of IEEE 802.11 is the worst compared to the other two protocols. Once the self stabilizing routing protocol forms the routes, the packets are forwarded along those routes to the group members. In IEEE 802.11 the packets lost due to bit errors are not recovered. Thus the packet drop ratio increases as the BER increases. In RDNP and M-RDNP data packets corrupted due to bit errors are recovered through NACK packets sent by the MAC layer. M-RDNP is more reliable compared to RDNP because M-RDNP uses reliable links to route packets. RDNP on the other hand loses some packets due to hidden terminal collisions at the receivers. Note that M-RDNP also drops some packets because of corrupted RTS-DATA packets.

Figure 23, figure 24, figure 25 and figure 26 shows the average energy consumed per packet per node for 10, 20, 30 and 40 nodes in the network. For all protocols as the number of nodes in the network increases, the average energy consumed. Also the energy

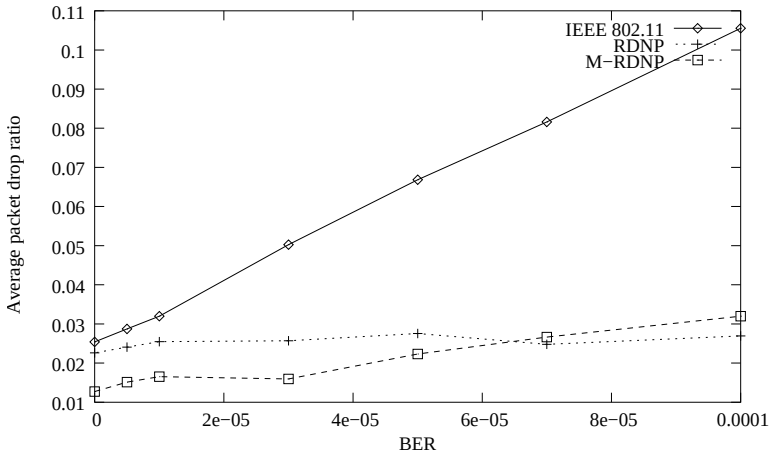


Figure 19. Packet Drop Ratio Vs. BER, nodes=10

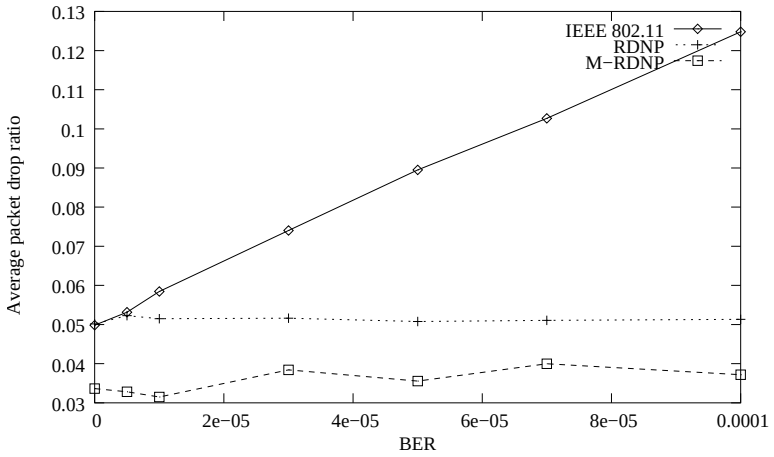


Figure 20. Packet Drop Ratio Vs. BER, nodes=20

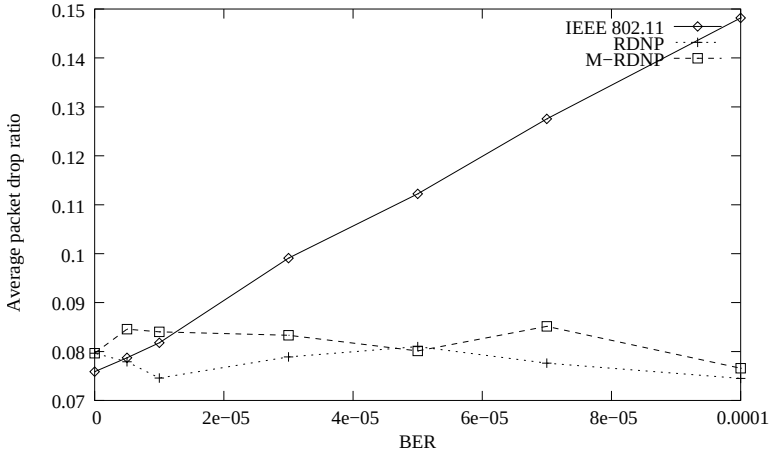


Figure 21. Packet Drop Ratio Vs. BER, nodes=30

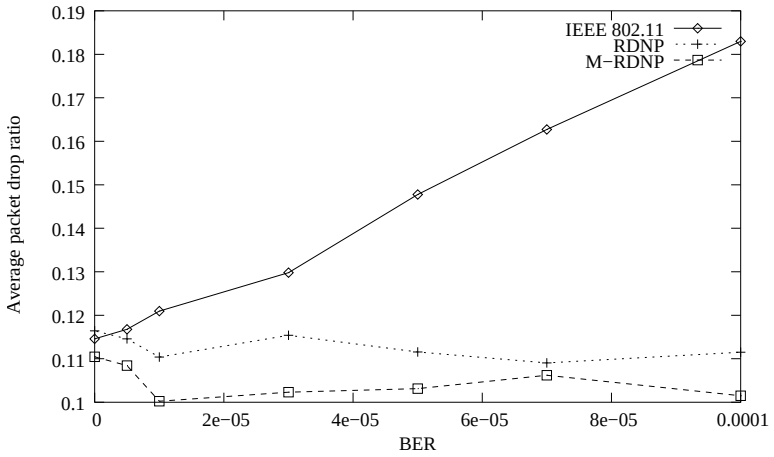


Figure 22. Packet Drop Ratio Vs. BER, nodes=40

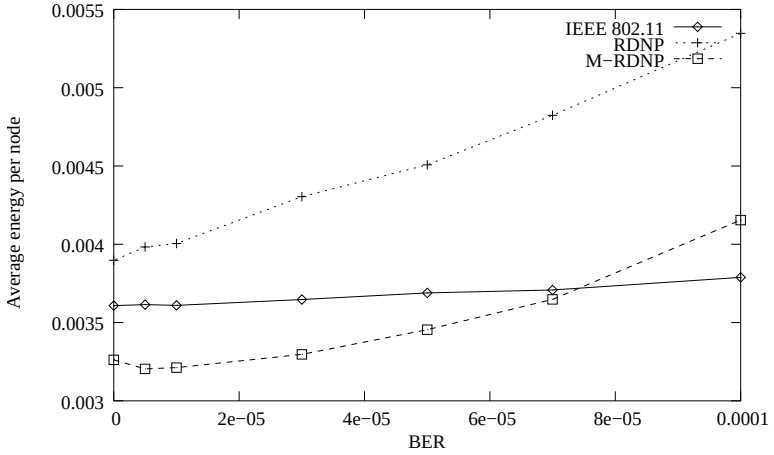


Figure 23. Average Energy Consumed Vs. BER, nodes=10

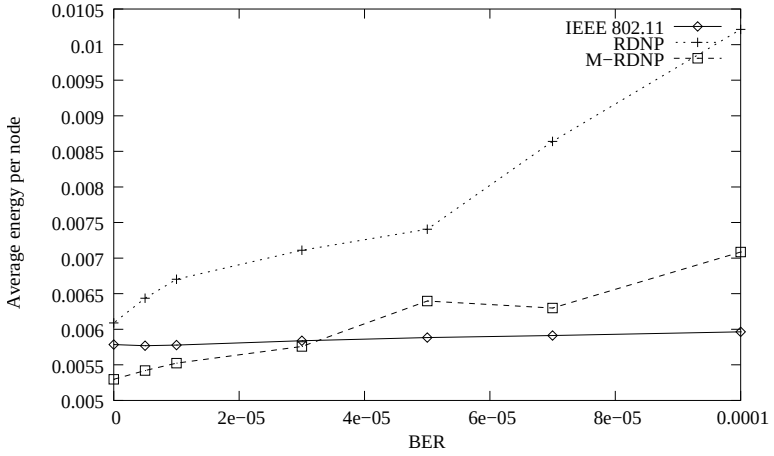


Figure 24. Average Energy Consumed Vs. BER, nodes=20

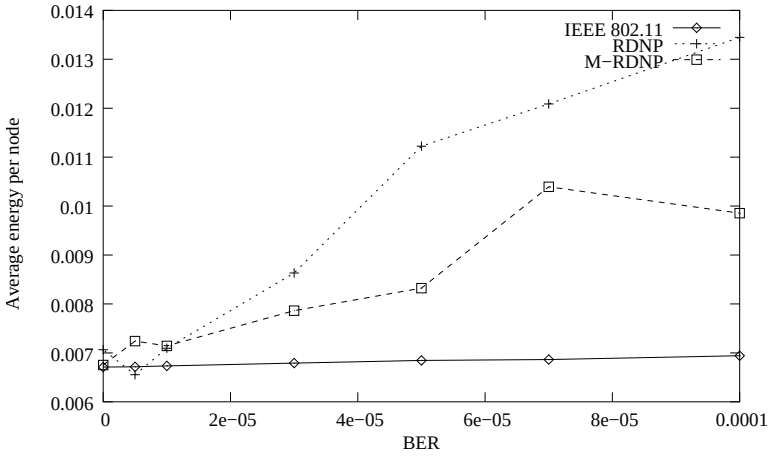


Figure 25. Average Energy Consumed Vs. BER, nodes=30

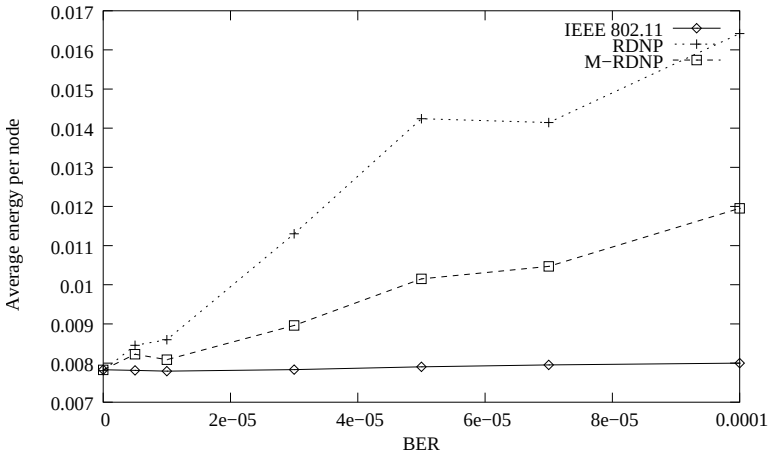


Figure 26. Average Energy Consumed Vs. BER, nodes=40

consumed per packet increases as the BER increases. This increase is greater for RDNP and M-RDNP because of the energy consumed for retransmissions. While the cost of a first transmission improves the reliability of all the receivers, the energy consumed for a retransmission improves the reliability of only a fraction of receivers. The energy consumed by RDNP is higher than that of M-RDNP because of the energy lost when two hidden terminals are transmitting simultaneously.

4.2. Scenario 2 - Mobile Ad Hoc Networks: Low-Moderate Speeds. In this section, we shall study the performance of the protocols subject to nodes moving at walking/running speeds. All nodes exhibit random way point motion[JMIK96]. All nodes move at walking speeds ranging from $1ms^{-1}$ to $10ms^{-1}$.

Channel with no errors and mobile nodes. In this section we observe the behavior of the protocols for MANETs when there are no channel errors. For such a scenario, we observe the protocols behavior when the number of nodes in the network are 10 and 30. M-RDNP performs better when the number of nodes in the network is 10(See Figure 27). However as the number of nodes in the network increases, IEEE 802.11 performs better when there are no channel errors(See Figure 28). This is because the main cause for packet loss in this scenario is because of mobility. Thus in M-RDNP as the number of nodes in the network increases, the number of hops also increases. This implies that as nodes move, routes are broken and rebuilt. As the number of hops increase the time taken to reach a receiver increases. Due to mobility the hosts may no longer be present when the packet actually reaches the last hop. In IEEE 802.11 fewer number of hops are present. Thus the time taken to reach a packet is less. Thus the number of packets dropped due to mobility is also less. The performance of RDNP follows IEEE 802.11 closely. This is because when

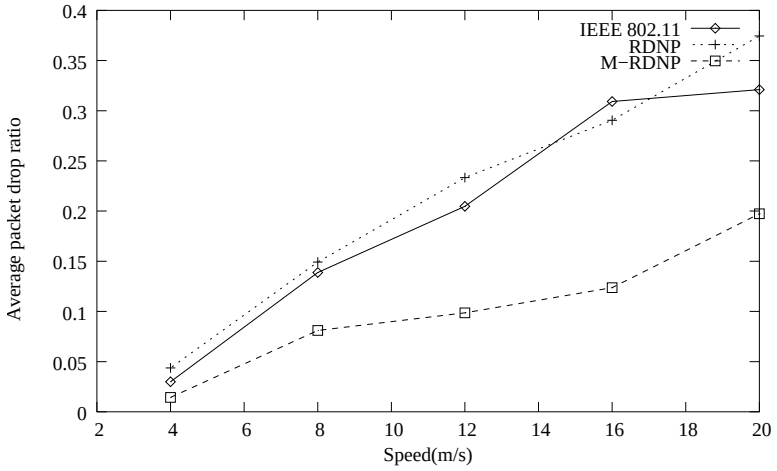


Figure 27. Packet Drop Ratio Vs. Mobility Rate, nodes=10, BER=0

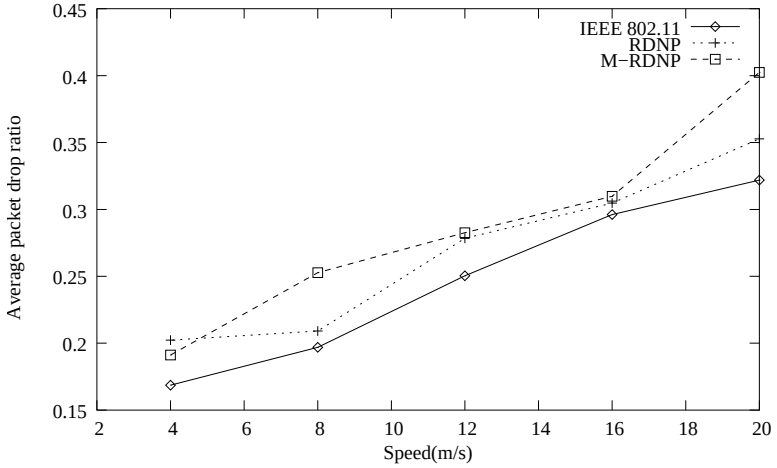


Figure 28. Packet Drop Ratio Vs. Mobility Rate, nodes=30, BER=0

there are no channel errors the performance of RDNP is similar to that of IEEE 802.11.

Channel with BER $= 10^{-4}$ *and mobile nodes.* In this section we observe the behavior of the protocols for MANETs when the channel BER is high i.e., BER $= 10^{-4}$. For such a scenario, we observe the protocols behavior when the number of nodes in the network are 10(Figure 31) and 30(Figure 32). M-RDNP performs better than IEEE 802.11 and RDNP in both cases. Though M-RDNP loses packet due to mobility, it recovers a lot of packets at the MAC layer unlike IEEE 802.11. In IEEE 802.11 fewer number of hops are present.

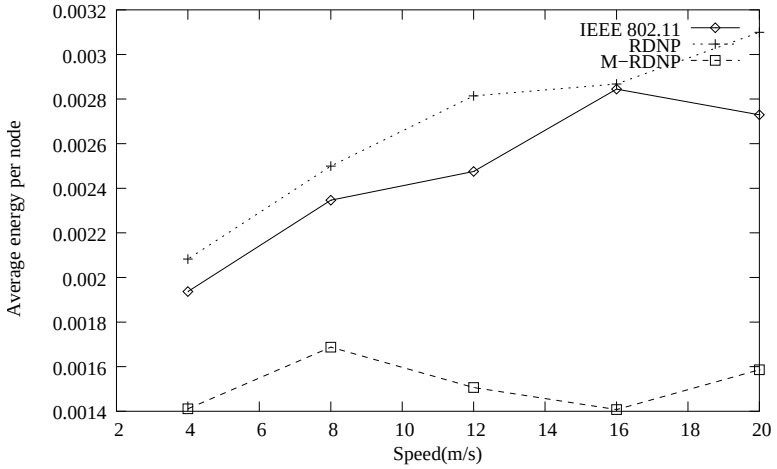


Figure 29. Average Energy Consumed Vs. Mobility Rate, nodes=10, BER=0

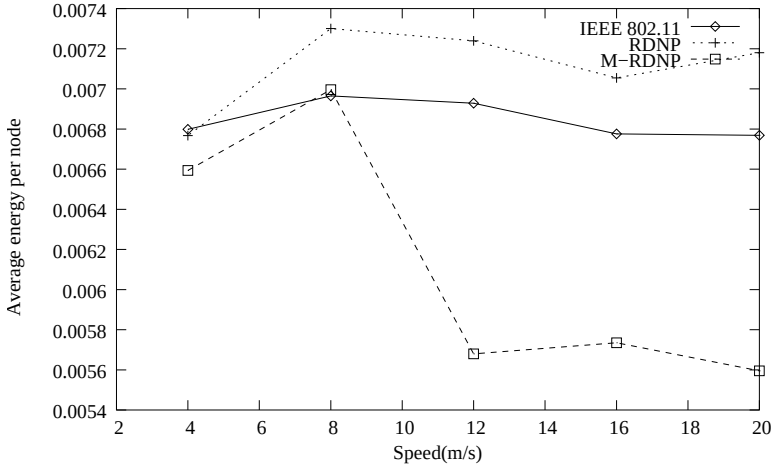


Figure 30. Average Energy Consumed Vs. Mobility Rate, nodes=30, BER=0

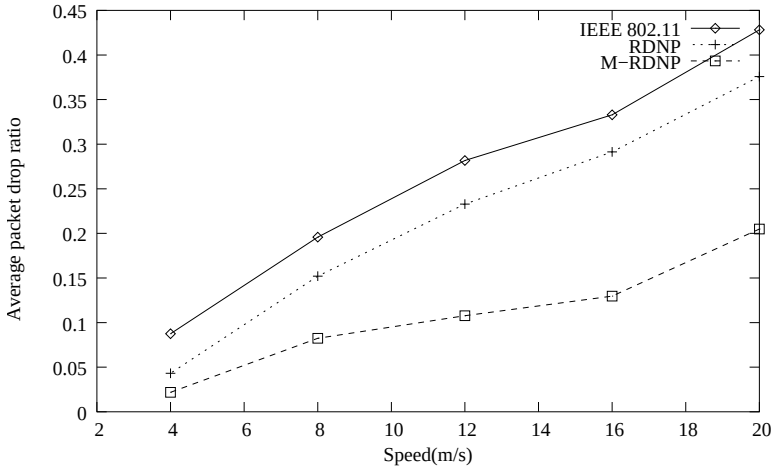


Figure 31. Packet Drop Ratio Vs. Mobility Rate, nodes=10, BER=10^{-4}

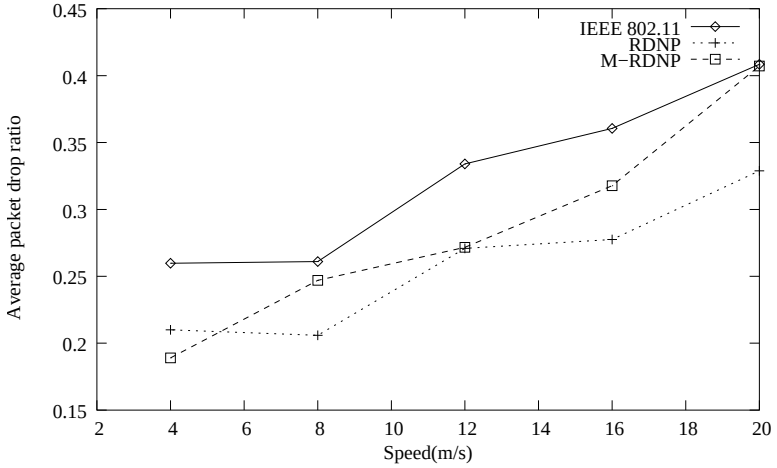


Figure 32. Packet Drop Ratio Vs. Mobility Rate, nodes=30, BER=10^{-4}

Thus the time taken to reach a packet is less. Thus the number of packets dropped due to mobility is also less. The performance of RDNP is better than IEEE 802.11 because RDNP recovers from packet drops due to channel errors.

Figure 29, figure 33 shows the energy consumed for 10 nodes in the network for low and high BERs respectively. The energy consumed by IEEE 802.11 and RDNP is more than that of M-RDNP in figure 29, because of the higher reliability of the network and low BER. No packets are lost due to hidden terminals. In figure 33, the energy consumed by

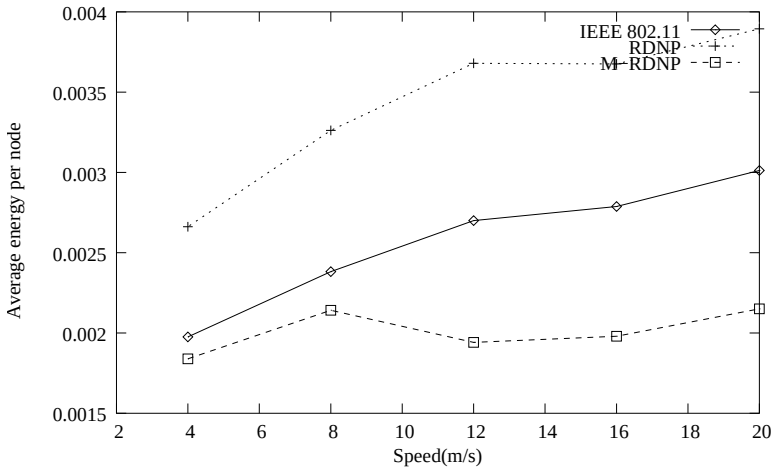


Figure 33. Average Energy Consumed Vs. Mobility Rate, nodes=10, BER=10^{-4}

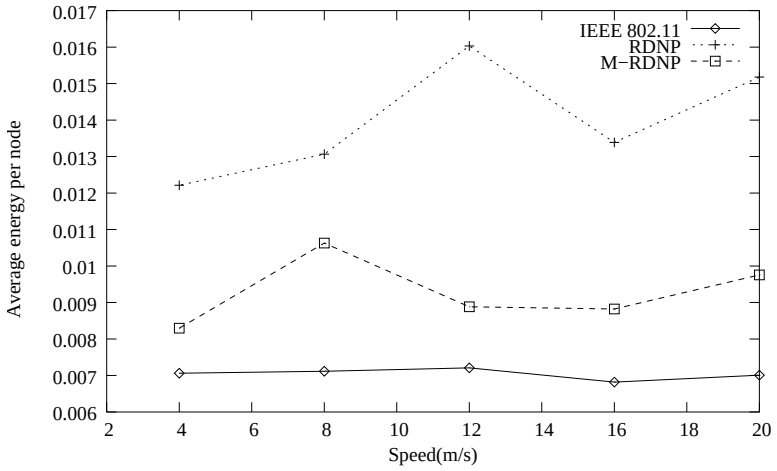


Figure 34. Average Energy Consumed Vs. Mobility Rate, nodes=30, BER=10^{-4}

RDNP and M-RDNP is higher because of increased retransmissions. Figure 30, figure 34 shows the energy consumed for 30 nodes in the network for low and high BERs respectively. The energy consumed by IEEE 802.11 and RDNP is more than that of M-RDNP in figure 30, because of more reliable links. However, in figure 34, the energy consumed by M-RDNP increases sharply because of higher packet loss owing to frequent routes changes in SPST caused by higher rate of changes in the neighbor node set.

4.3. Scenario 3 - Mobile Ad Hoc Networks: Very High Speeds. In this section, we shall study the performance of the protocols subject to nodes moving at very high speeds. All nodes exhibit random way point motion[JMIK96]. The performance has been observed for two speeds: 80 miles per hour, 150 miles per hour.

Speed = 80 miles per hour. In this section we observe the behavior of the protocols for MANETs when all nodes are moving at a speed of 80 miles per hour. For such a scenario, we observe the protocols behavior when the number of nodes in the network are 10(See Figure 35) and 30(See Figure 36) for low and high rate of channel errors. The performance of all the three protocols is almost similar for both low and high BER. This is because, the speeds are so high that the protocol behavior is mostly dependent on the effectiveness of the routing protocol. Most packets dropped are routing to mobility. There is no time to recover from channel errors due to high node mobility. The BER does not make a difference to the protocols. Observing figures 35 and 35, for all protocols the protocols, the average packet drop ratio is the same. As the number of nodes increase, figure 35 and figure 36, the reliability decreases. Also, from figure 37 and figure 38 it can be observed that the energy consumed by all protocols is the same for low BER. However, for higher BER, RDNP consumes more energy because it tries to recover from errors. The effect of

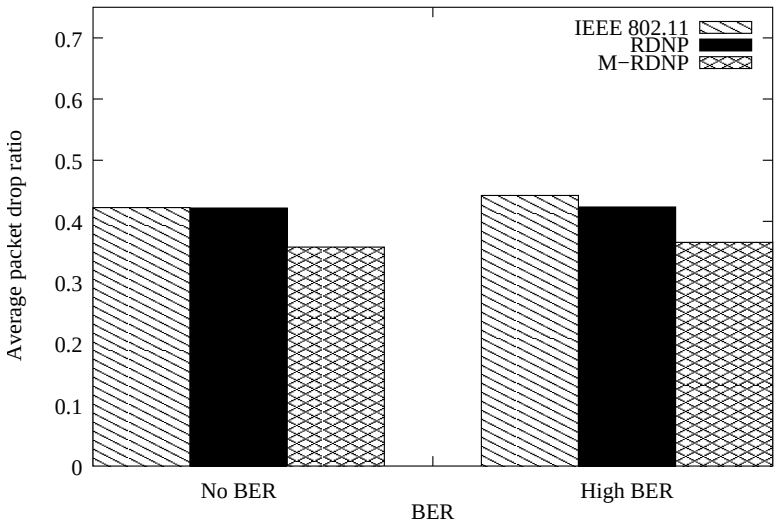


Figure 35. Packet Drop Ratio Vs. Mobility Rate, nodes=10, speed=80miles/hr

the recovery is not significant in terms of improvement in reliability.

Speed = 150 miles per hour. In this section we observe the behavior of the protocols for MANETs when all nodes are moving at a speed of 150 miles per hour. The behavior of the protocols at 150 miles per hour is similar to the behavior at 80 miles per hour. Figure 39 and figure 40 shows the reliability of the protocols when there are 10 and 30 nodes in the network. The performance of all the three protocols is almost similar in both cases. This is because, the speeds are so high that the protocol behavior is mostly dependent on the effectiveness of the routing protocol. Also, figure 41 and figure 42 shows the energy consumed per packet in the network for 10 and 30 nodes respectively.

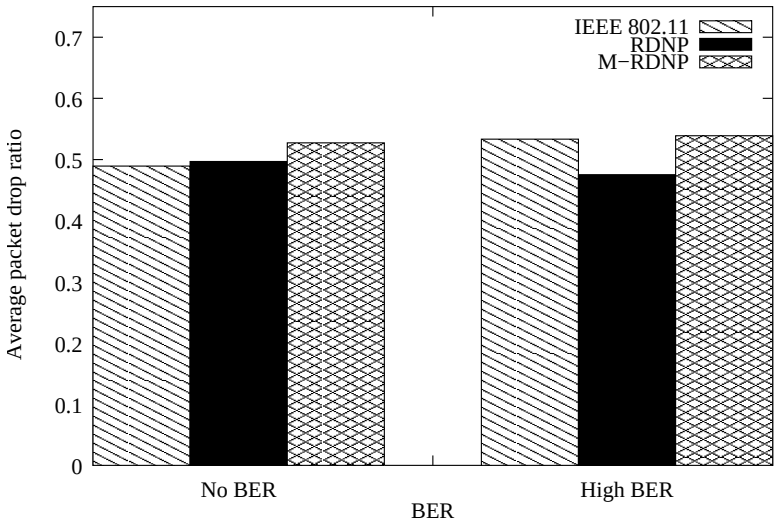


Figure 36. Packet Drop Ratio Vs. Mobility Rate, nodes=30, speed=80miles/hr

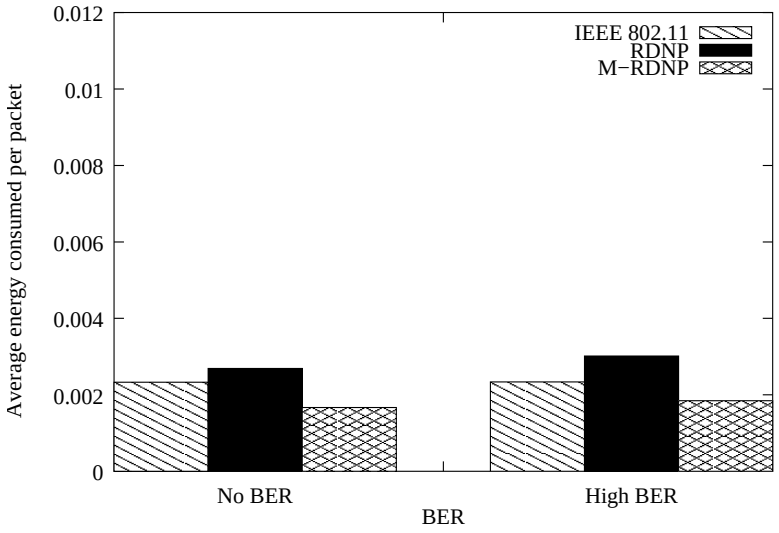


Figure 37. Average Energy Consumed Vs. Mobility Rate, nodes=10, speed=80miles/hr

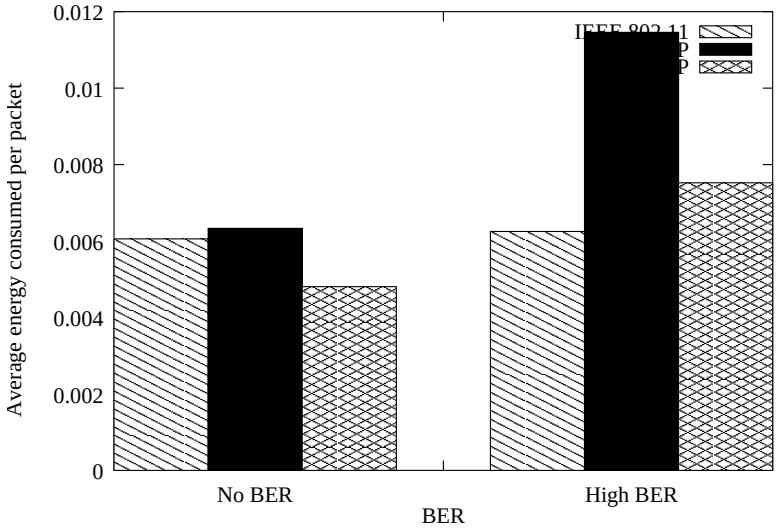


Figure 38. Average Energy Consumed Vs. Mobility Rate, nodes=30, speed=80miles/hr

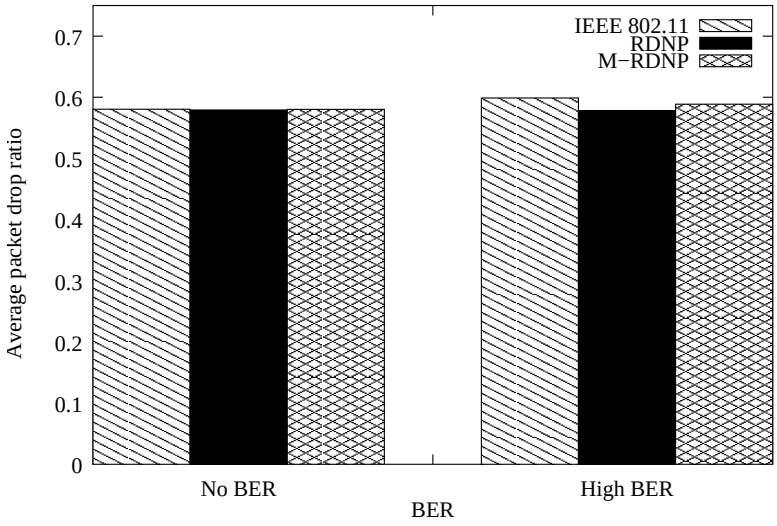


Figure 39. Packet Drop Ratio Vs. Mobility Rate, nodes=10, speed=150miles/hr

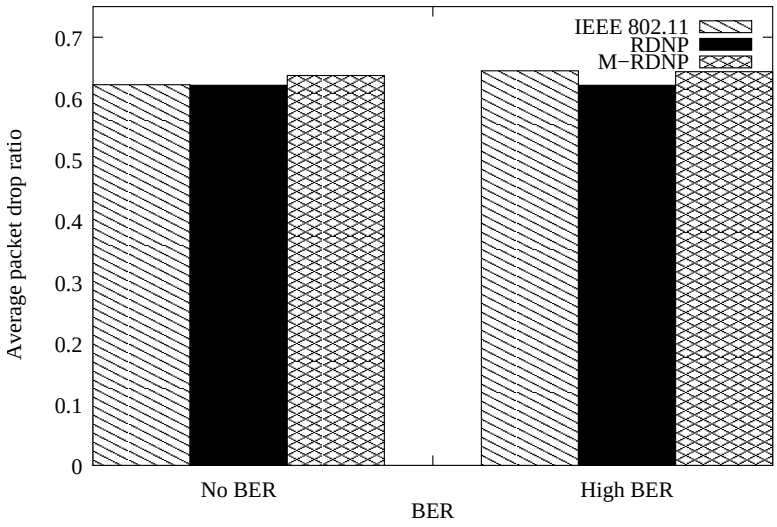


Figure 40. Packet Drop Ratio Vs. Mobility Rate, nodes=30, speed=150miles/hr

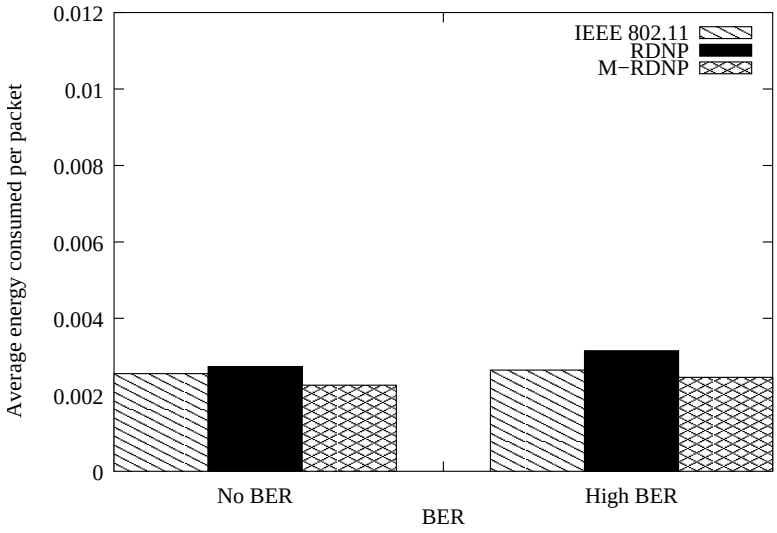


Figure 41. Average Energy Consumed Vs. Mobility Rate, nodes=10, speed=150miles/hr

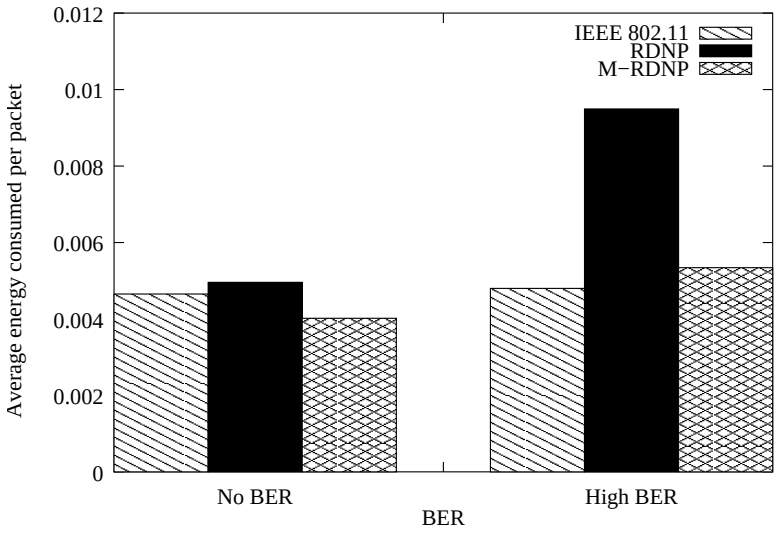


Figure 42. Average Energy Consumed Vs. Mobility Rate, nodes=30, speed=150miles/hr

CHAPTER 6

Conclusion and Future Work

1. Conclusions

In this thesis, we have identified the problems with achieving reliable multicast at the MAC layer. We have also presented a survey of several MAC protocols that have proposed for multicast and unicast at the MAC layer for wireless networks. We have also given a brief discussion of routing protocols and presented the detailed discussion of SPST.

We have shown that IEEE 802.11 does not support reliable multicast at the MAC layer and we have proposed an extension to the IEEE 802.11 MAC to improve link-level reliability for multicast data. Our scheme uses a NACK based approach to delivering data reliability to multiple receivers. A novel feature of this work is that it uses the concept of noise threshold in order to improve the reliability of the data communicated. Also, we have shown that the performance of our protocol is not affected by the corruption of feedback packets.

Using simulations we have compared the performance of RDNP to that of IEEE 802.11 multicast, LBP, DBP and PBP. We have also compared the performance of RDNP and M-RDNP protocol to that of IEEE 802.11 multicast in ad hoc networks. From our results, we can conclude that the data delivery of multicast communication is better using

our protocols in almost all scenarios for both ad hoc and wireless networks. Only when the BER is low and the number of neighbors is high(≥ 8) it is better to use IEEE 802.11 multicast for multihop networks.

We conclude that,

- For Stationary Ad Hoc networks
  - The reliability of M-RDNP is higher than RDNP and IEEE 802.11 for low(≤ 8) neighbor density.
  - M-RDNP and RDNP are statistically indifferent for higher neighbor densities.
- For Mobile Ad Hoc networks with low speeds
  - IEEE 802.11 achieves higher reliability when the channel BER is low and the number of neighbors is high(≥ 8).
  - RDNP achieves higher reliability when the channel BER is high and the number of neighbors is high(≥ 8).
  - M-RDNP achieves higher reliability when the channel BER is high and the number of neighbors is low(≤ 8)[1].
- For Mobile Ad Hoc networks with high speeds
  - Reliability of all three protocols is statistically indifferent
- Energy cost associated with a retransmission is much higher than that of a transmission because all nodes spend energy but only the reliability of those nodes that lost the packet is improved.

[1] Reliable neighbor density is ≤ 4

- Changing parents frequently reduces the reliability. In SPST, collision of beacon messages leads to a change in the multicast parent. This parent hopping reduces the overall reliability. As the number of nodes increases, the frequency of beacon collision also increases. It is important to reduce the frequency of such feedback collisions in order to improve reliability.

2. Future Work

M-RDNP uses more number of hops to reach an unreliable neighbor. Also, when no reliable neighbors are available, the unreliable neighbor is not connected to the network. In the absence of hidden terminals, such disconnection is a waste of resources. A more effective approach would be to connect to a reliable neighbor if available or connect to the unreliable neighbor otherwise. Though such a scheme does seem more efficient, it would be difficult to implement such a scheme without some minimal support from the routing layer. This can be achieved, if such reliable/unreliable neighbor information can be incorporated into the link cost metric in SPST.

Also, a hybrid scheme which can switch between the different MAC protocols based on the link metrics would be novel.

REFERENCES

[BDSZ94] Vaduvur Bharghavan, Alan Demers, Scott Shenker, and Lixia Zhang. MACAW: a media access protocol for wireless LAN's. *ACM SIGCOMM Computer Communication Review*, 24(4):212–225, 1994.

[Blu02] Bluetooth. The official bluetooth wireless info site, September 2002.

[Com99] IEEE Computer Society LAN MAN Standards Committee. IEEE std. 802.11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, August 1999.

[Dij74] E. W. Dijkstra. Self stabilizing systems in spite of distributed control. In *Proceedings of the Communications of the ACM*, November 1974.

[Dij86] E. W. Dijkstra. A belated proof of self-stabilization. In *Distributed Computing*, 1986.

[DJ98] Jing Deng and Zygmunt J.Haas. Dual busy tone multiple access (DBTMA): a new medium access protocol for packet radio networks. In *IEEE 1998 International Conference on Universal Personal Communications, ICUPC'98*, volume 2, pages 973–977, October 1998.

[FGLA95a] Chane L. Fullmer and J. J. Garcia-Luna-Aceves. FAMA-PJ: a channel access protocol for wireless LANs. In *Proceedings of the first annual international*

conference on Mobile computing and networking, pages 76–85. ACM Press, 1995.

[FGLA95b] Chane L. Fullmer and J. J. Garcia-Luna-Aceves. Floor acquisition multiple access (FAMA) for packet-radio networks. *ACM SIGCOMM Computer Communication Review*, 25(4):262–273, 1995.

[FGLA97] Chane L. Fullmer and J. J. Garcia-Luna-Aceves. Solutions to hidden terminal problems in wireless networks. *ACM SIGCOMM Computer Communication Review*, 27(4):39–49, 1997.

[FV] Kevin Fall and Kannan Varadhan. *NS Notes and Documentation.* The VINT Project, UC Berkeley, LBL, USC/ISI and Xerox PARC.

[GBS00] Sandeep K. S. Gupta, A. Bouabdallah, and P. K. Srimani. Self-stabilizing protocol for shortest path tree for multi-cast routing in mobile networks (research note). In *Proceedings of LNCS:1900, Euro-Par'00 Parallel Proceedings*, pages 600–604, 2000.

[GL00] Ajay Chandra V. Gummalla and John O. Limb. Wireless medium access protocols. *IEEE Communications Survey, Second Quarter*, 2000.

[GS99] Sandeep K. S. Gupta and P. K. Srimani. Using self-stabilization to design adaptive multicast protocol for mobile ad hoc networks. In *Proceedings of the DIMACS Workshop on Mobile Networks and Computing*, pages 67–84, 1999.

[GSL03] S. K. S. Gupta, V. Shankar, and S. Lalwani. Reliable multicast MAC protocol for wireless LANs. In *IEEE International Conference on Communications ICC*, May 2003.

[HS84] E. Horowitz and S. Sahni. *Fundamentals of Computer Algorithms.* Computer Science Press, 1984.

[IG00] Aron D. Ionut and Sandeep K. S. Gupta. Analytical comparison of local and end-to-end error recovery in reactive routing protocols for mobile ad hoc networks. In *Proceedings of the 3rd ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pages 69–76. ACM Press, 2000.

[Jai91] Raj Jain. *The Art of Computer Systems Performance Analysis - Techniques for Experimental Design, Measurement, Simulation and Modeling.* Wiley, 1991.

[JMIK96] David. B. Johnson, Davis. A. Maltz, Tomasz Imielinski, and Hank Korth. *Mobile Computing*, chapter 1.2, pages 153–181. Kulwer Academic Publishers, 1996.

[JT87] J. Jubin and J. D. Tornow. The DARPA packet radio network protocol. In *Proceedings of the IEEE*, volume 75, pages 21–32, January 1987.

[Kar90] P. Karn. MACA - a new channel access method for packet radio. In *AAR/CRRL Amateur Radio 9th Computer Networking Conference*, pages 134–140, 1990.

[KK99] J. Kuri and S. K. Kasera. Reliable multicast in multi-access wireless LANs. In *Proceedings of IEEE INFOCOM'99, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 2, pages 760–767, March 1999.

[KK01] Joy Kuri and Sneha Kumar Kasera. Reliable multicast in multi-access wireless LANs. *Wireless Networks*, 7(4):359–369, July 2001.

[MCP00] M.Impett, M. S. Corson, and V. Park. A receiver-oriented approach to reliable broadcast in ad hoc networks. In *IEEE Wireless Communications and Networking Conference, WCNC 2000*, volume 1, pages 117–122, September 2000.

[Net02] The network simulator - ns-2, July 2002.

[Rap96] Theodore. S. Rappaport. *Wireless Communications: Principles and Practices.* Prentice Hall, New Jersey, 1996.

[RP99] Elizabeth M. Royer and Charles E. Perkins. Multicast operation of the ad-hoc on-demand distance vector routing protocol. In *Proceedings of the fifth annual ACM/IEEE international conference on Mobile computing and networking*, pages 207–218. ACM Press, 1999.

[RV97] Luigi Rizzo and Lorenzo Vicisano. A reliable multicast data distribution protocol based on software FEC techniques. In *Proceedings of the Fourth IEEE Workshop on the Architecture and Implementation of High Performance Communication Systems (HPCS'97)*, Sani Beach, Chalkidiki, Greece, June 1997.

[RV98] Luigi Rizzo and Lorenzo Vicisano. RMDP: an FEC-based reliable multicast protocol for wireless environments. *ACM SIGMOBILE Mobile Computing and Communications Review*, 2(2):23–31, April 1998.

[SG03] Ganesh Sridharan and Sandeep K. S. Gupta. Performance comparison study of self stabilizing routing protocols for mobile ad hoc networks. In preparation, .

[Sha02] Vikram Shankar. A medium access control protocol with reliable multicast

support for wireless networks. Master's thesis, Arizona State University, Tempe, AZ - 85287, December 2002.

[SHAL02] Min-Te Sun, Lifei Huang, Anish Arora, and Ten-Hwang Lai. Reliable MAC layer multicast in IEEE 802.11 wireless networks. In *Proceedings of the International Conference on Parallel Processing, ICPP'02)*, pages 527–536, August 2002.

[TG00a] Kent Tang and Mario Gerla. MAC layer broadcast support in 802.11 wireless networks. In *Proceedings of the 21st Century Military Communications Conference, MILCOM 2000.*, volume 1, pages 544–548, October 2000.

[TG00b] Kent Tang and Mario Gerla. Random access MAC for efficient broadcast support in ad hoc networks. In *IEEE Wireless Communications and Networking Conference, WCNC 2000*, volume 1, pages 454–459, September 2000.

[TG01] Kent Tang and Mario Gerla. MAC reliable broadcast ad hoc networks. In *Communications for Network-Centric Operations: Creating the Information Force. IEEE Military Communications Conference, MILCOM'01*, pages 1008–1013, 2001.

[TK75] Fouad A. Tobagi and Leonard Kleinrock. Packet switching in radio channels: Part ii - the hidden terminal problem in carrier sense multiple-access modes and the busy-tone solution. *IEEE Transactions on Communications*, 23(2):1400–1416, 1975.

[TKP97] Donald F. Towsley, James F. Kurose, and Sridhar Pingali. A comparison of

sender-initiated and receiver-initiated reliable multicast protocols. *IEEE Journal of Selected Areas in Communications*, 15(3):398–406, 1997.

[XGB02] K. Xu, M. Gerla, and S. Bae. How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks. In *Proceedings of IEEE Globecom 2002*, 2002.

[YC99] Seong-Won Yuk and Dong-Ho Cho. Parity-based reliable multicast method for wireless LAN environments. In *IEEE 50th Vehicular Technology Conference, VTC'99*, volume 2, pages 1217–1221, September 1999.

[YL02] Y. Yi and S. Lee. On-demand multicast routing protocol (ODMRP) for ad-hoc networks, November 2002. Work in progress.

APPENDIX A

COMPARISON OF RELIABLE MULTICAST PROTOCOLS

Table 3. Comparison of the Reliable Multicast Protocols

Protocol	Medium Access	Error Recovery	Support from BS	Mobility Tolerant	Packets	Receiver Semantics	Network Support
LBP	physical CS + RTS from sender + CTS from leader or NCTS from non-leaders	ACK from leader or NACK from non-leaders	Leader Election	Mobility of leader detection	RTS, CTS or NCTS, ACK or NACK	all-or-none	infrastructure
DBP	physical CS + RTS from sender + delayed CTS from receivers	-	number of receivers	changes in the number of nodes needs to be detected	RTS, CTS	At-least-one	infrastructure
PBP	physical CS + RTS from sender + probabilistic CTS receivers	-	number of receivers	changes in the number of nodes needs to be detected	RTS, CTS	at-least-one	infrastructure
Simple NACK Recovery	physical CS + RTS from sender to one receiver + CTS from single receiver	delayed NACK	-	-	RTS, CTS, NACK, HELLO	at-least-one	ad hoc
BSMA	physical CS + RTS from sender + simultaneous CTS from all receivers	NACK from all receivers at same time	-	-	RTS, CTS, NACK	Everyone	ad hoc
BMW	physical CS + RTS from sender + CTS from single receiver	CTS with missed sequence number + ACK	exact list of all receivers	updated list of receivers	RTS, CTS, ACK	Everyone	ad hoc
BMMM	physical CS + RTS-CTS with each receiver	RACK-ACK with each receiver	exact list of receivers	updated list of receivers	RTS, CTS, RACK, ACK	all-or-none	ad hoc
IEEE 802.11MX	physical CS + RTS from sender + NCTS tone from receivers	NACK tone from receivers	-	-	RTS, NCTS tone, NACK tone, busy tone	all	ad hoc