6-2008

Channel-access and routing protocols to utilize multiple heterogeneous channels for ad hoc networks

Crystal Jackson

Clemson University, crystalajackson@hotmail.com

Follow this and additional works at: https://tigerprints.clemson.edu/all_theses

Part of the [Electrical and Computer Engineering Commons](#)

Recommended Citation

Jackson, Crystal, "Channel-access and routing protocols to utilize multiple heterogeneous channels for ad hoc networks" (2008). *All Theses*. 392.

https://tigerprints.clemson.edu/all_theses/392

This Thesis is brought to you for free and open access by the Theses at TigerPrints. It has been accepted for inclusion in All Theses by an authorized administrator of TigerPrints. For more information, please contact kokeefe@clemson.edu.

CHANNEL-ACCESS AND ROUTING PROTOCOLS TO UTILIZE MULTIPLE
HETEROGENEOUS CHANNELS FOR AD HOC NETWORKS

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
Computer Engineering

---

by
Crystal Alicia Jackson
August 2008

Accepted by:
Dr. Harlan Russell, Committee Chair
Dr. Michael Pursley
Dr. Kuang-Ching Wang

ABSTRACT

In this thesis, we consider a multi-channel ad hoc network employing frequency-agile radios that utilize direct-sequence spread-spectrum signaling. Two of the key distributed protocols for this type of network control channel access and routing. The channel-access protocol is responsible for controlling access to the channels available to the terminals in the network, and the routing protocol determines how packets are forwarded among the terminals in the network. To achieve reliable and efficient network performance, these protocols should cooperate with one another and take advantage of the multiple channels available to the network.

In this thesis, we investigate a number of channel-access strategies for selecting a channel as well as various channel metrics to be used with routing. For our channel-access protocol, one channel is designated the control channel and is used to reserve access to one of the traffic channels. The channel-access protocol selects the traffic channel for a data packet transmission by examining the characteristics of the different traffic channels. New channel metrics are proposed to characterize the channels, and the metric values are used to assign a link resistance value for a link. Least-resistance routing utilizes the link resistances to calculate routes. The performance of the channel metrics for the routing protocol and the channel-access strategies are examined with a discrete-event simulation. From our investigations, we show that a jointly designed protocol that coordinates the channel-access strategies with the channel metrics results in network performance that is better than traditional channel-access and minimum-hop routing protocols.

ACKNOWLEDGMENTS

I would like to sincerely thank my advisor, Dr. Harlan Russell, for his insight, direction, and commitment throughout my graduate studies. I would also like to thank Dr. Michael Pursley and Dr. Kuang-Ching Wang for serving on my thesis committee.

TABLE OF CONTENTS

	Page
TITLE PAGE.....	i
ABSTRACT	ii
ACKNOWLEDGMENTS	iii
LIST OF TABLES	vi
LIST OF FIGURES.....	vii
 CHAPTER	
I. INTRODUCTION	1
1.1 Ad hoc networks	1
1.2 Software-defined radio	2
1.3 Brief literature review.....	3
1.4 Organization of thesis.....	5
II. SYSTEM DESCRIPTION	6
2.1 Physical layer model.....	6
2.2 Link layer model	9
2.3 Network layer model	13
III. PROTOCOLS.....	15
3.1 Channel-access protocol	15
3.2 Routing protocol.....	22
IV. SIMULATION MODEL AND RESULTS.....	28
4.1 Simulation parameters	28
4.2 Network scenarios	30
4.3 Network topologies	32
4.4 Channel-access independent of routing.....	34
4.5 Channel-access with routing.....	43

Table of Contents (Continued)

	Page
V. CONCLUSIONS	55
REFERENCES	57

LIST OF TABLES

Table	Page
2.1 Channel availability for terminals in Figure 2.1	11
3.1 Δ_i for channels of example network.....	22
4.1 Parameters used by the simulation model.....	29
4.2 Traffic channel attributes for the small scenario	31
4.3 Traffic channel attributes for the mid scenario.....	31
4.4 Traffic channel attributes for the large scenario.....	31
4.5 Comparison of the data rate and alternative data rate metrics for Figures 4.18-4.20	50

LIST OF FIGURES

Figure	Page
2.1 Sample transmission from terminal A to terminal B	11
3.1 Base channel-access protocol for source and destination terminals	19
3.2 Base channel-access protocol for neighboring terminals.....	21
3.3 Example network.....	22
3.4 Δ_i ranges for the channels of the example network	24
3.5 Routing example.....	27
3.6 Routing example after link resistance update.....	27
4.1 Grid topology.....	33
4.2 Large-scaled topology.....	33
4.3 Performance of channel-access strategies for small- scaled topology with the small scenario.....	38
4.4 Performance of channel-access strategies for medium- scaled topology with the small scenario.....	39
4.5 Performance of channel-access strategies for large-scaled topology with the small scenario	39
4.6 Performance of channel-access strategies for small-scaled topology with the mid scenario.....	40
4.7 Performance of channel-access strategies for medium- scaled topology with the mid scenario	40
4.8 Performance of channel-access strategies for large-scaled topology with the mid scenario.....	41
4.9 Performance of channel-access strategies for small-scaled topology with the large scenario	41

List of Figures (Continued)

Figure	Page
4.10 Performance of channel-access strategies for medium-scaled topology with the large scenario	42
4.11 Performance of channel-access strategies for large-scaled topology with the large scenario	42
4.12 Performance of channel metrics for medium-scaled topology with the small scenario	45
4.13 Performance of channel metrics for large-scaled topology with the small scenario	46
4.14 Performance of channel metrics for medium-scaled topology with the mid scenario	46
4.15 Performance of channel metrics for large-scaled topology with the mid scenario	47
4.16 Performance of channel metrics for medium-scaled topology with the large scenario	47
4.17 Performance of channel metrics for large-scaled topology with the large scenario	48
4.18 Performance of channel-access strategy and channel metric combinations for large-scaled topology with the small scenario	51
4.19 Performance of channel-access strategy and channel metric combinations for medium-scaled topology with the large scenario	51
4.20 Performance of channel-access strategy and channel metric combinations for large-scaled topology with the large scenario	52
4.21 Comparison of data rate/nbr count channel metric for medium-scaled topology with the large scenario	54

CHAPTER ONE

INTRODUCTION

1.1 Ad hoc networks

An ad hoc wireless network is a collection of wireless mobile terminals that self-configure to form a network without the aid of any established infrastructure [1]. Unlike other infrastructure-based networks, the terminals of an ad hoc wireless network are responsible for coordinating their own packet transmissions in a distributed manner. Packets are routed via multihop routing in which intermediate terminals are responsible for forwarding a packet from its source to its destination. The channel-access protocols for this type of network should promote the fair use of all the channels and ensure adequate throughput for the network. Routing protocols that correctly and efficiently establish routes are needed so that a packet can be successfully forwarded to its destination. Mobility has a significant impact on the channel-access protocols since it affects link characteristics as well as link connectivity. The routing protocols must also be designed to be responsive to mobility, and for example, they must be able to repair routes after changes in network connectivity. Some advantages of an ad hoc wireless network are that it can be rapidly deployed and configured, can be tailored to specific applications, and is highly robust. These networks are used where infrastructure-based networks are infeasible or where a temporary network needs to be quickly deployed. Ad hoc networks are primarily used in military applications, though other example applications include emergency search-and-rescue and data acquisition in inhospitable terrains [2].

1.2 Software-defined radio

Future wireless networks will benefit from being able to utilize multiple frequency channels with widely different characteristics [3]-[6]. Emerging software-defined radios are enabling increasing flexibility in specifying the carrier frequency, transmission rate, and receiver bandwidth over a very wide range of possible configurations. As components of the radios that have typically been implemented in hardware are replaced with software-based systems, it becomes possible to update the software quickly to change the transmission frequency and format with very little delay [3]. These types of frequency-agile radios allow the channel parameters to be modified at the time the network is deployed or as the operating conditions change.

While some portions of the spectrum are becoming saturated due to the increasing demand for mobile and wireless applications, other bands are idle or underutilized. For a network equipped with frequency-agile radios, the network operators can select appropriate channels for the current application, and the terminals can self-configure to utilize these bands. Future networks may also employ cognitive radios [4]. Cognitive radio has been proposed as the means to promote the efficient use of the spectrum by exploiting the existence of spectrum holes [5]. A key feature of a cognitive radio is the ability to sense underutilized portions of the spectrum and to utilize channels in the spectrum holes. The configurability of software-defined radios allows a network of cognitive radios to transmit and receive on a variety of different channels so the network can fully exploit the available capacity [6].

1.3 Brief literature review

Most of the research on networks employing the use of multiple traffic channels, [7]-[10], involve equipping a terminal with multiple radios or network interface cards tuned to a specific frequency. A link layer protocol, Multi-Radio Unification Protocol (MUP), was introduced in [7] that monitors channel quality on each interface and selects the appropriate interface whenever transmitting a packet using standard IEEE 802.11 hardware. The authors of [8] provide a routing protocol, Multi-Radio Link-Quality Source Routing (MR-LQSR), for multi-radio IEEE 802.11 networks using the Weighted Cumulative Expected Transmission Time (WCETT) metric that assigns weights to links based on their bandwidth and loss rate. They also allow for simultaneous transmissions on each of the radios assigned to a terminal. The work of [9] attempts to improve the capacity of wireless mesh networks by assigning multiple radios to non-overlapping channels, and it also presents a centralized algorithm that assigns these channels to the radios. The authors of [10] also consider channel assignment for the interfaces assigned to each terminal, but it is a hybrid interface assignment strategy that designates a certain number of interfaces to stay fixed to a channel while others can frequently switch between the remaining channels to ensure communication. The Multi-Channel Routing Protocol (MCRP) is presented in [11]. This routing protocol uses a single transceiver and a single-channel MAC protocol that allocates different channels to different flows. The protocol assigns a common channel to all terminals in a flow and allows terminals to switch channels but does not allow two consecutive terminals in a flow to switch

channels. MRCP also assumes a single channel MAC protocol such as IEEE 802.11 DCF.

In this thesis, we consider frequency-agile radios that have the ability to easily change their carrier frequency and chip rate over a wide range of possibilities. However, unlike the work of [7]-[10], we assume that each terminal is equipped with one frequency-agile radio. This software-defined radio has a single half-duplex transceiver that can be tuned to a particular carrier frequency and its associated chip rate for each transmission or reception. The details for selecting the carrier frequency and chip rate are outside the scope of this thesis, but instead we assume that a set of frequency allocations is available to the radios in the network. We propose a new channel-access protocol and a new routing protocol that are specifically designed to account for the capabilities of such a software-defined radio. We show that the network performance of an ad hoc network of such radios can be significantly improved with a channel-access protocol that accounts for the ability of the network to utilize multiple bands. Furthermore, a jointly designed channel-access and routing protocol leads to even greater improvements in network performance compared to an approach in which the channel-access and routing protocols are not designed to cooperate. In scenarios in which the set of bands have considerable differences in carrier frequency and chip rate, the improvements in network performance are particularly significant.

1.4 Organization of thesis

In this thesis, we investigate and evaluate the performance of channel-access strategies and routing metrics for ad hoc networks consisting of frequency-agile radios. Chapter 2 offers a description of the system we are considering including details for the physical, link, and network layers. Chapter 3 provides details of the channel-access strategies and routing metrics created for the system. Chapter 4 provides the attributes for the simulation model and presents results of our investigation of the channel-access strategies and also of the channel-access strategies when used with the routing metrics developed in Chapter 3. Lastly, Chapter 5 presents the conclusions obtained from these investigations.

CHAPTER TWO

SYSTEM DESCRIPTION

The model for the system that is used in our investigations is described in this chapter. We consider a three-layer system consisting of the physical, link, and network layers. The following sections give an overview of the model used for each layer. The layers above the network layer are not modeled in this thesis.

2.1 Physical layer model

The radios for this system employ direct-sequence spread-spectrum modulation. The information bits of a packet are encoded using a rate $R = 1/2$ convolutional code with constraint length 7. The encoded bits are referred to as *symbols*. There are a fixed number of symbols, S , for each data packet. Each symbol is spread using a spread-spectrum waveform consisting of N chips. Therefore, a data packet consists of NS chips where N is referred to as the *spreading factor*. The terminals use binary phase shift keying with coherent demodulation.

Each terminal has a single half-duplex transceiver that can be instantaneously tuned to any one of multiple channels that are available to the terminals. We assume a frequency-agile radio system in which M nonoverlapping channels are available for use by the terminals. The carrier frequency and chip rate are different for each channel. All terminals tuned to a particular channel use the same carrier frequency and chip rate. Denote the carrier frequency for channel i as f_i and the channels are numbered so that $f_1 <$

$f_2 < \dots < f_M$. The chip duration for channel i is T_{C_i} . For the systems considered in this thesis, we assume that if $f_i < f_j$, then $T_{C_i} > T_{C_j}$ (i.e., a channel with a higher carrier frequency has a larger chip rate). We assume N and R are fixed and the same for each channel. The data rate for channel i is

$$D_i = \frac{R}{NT_{C_i}}, \quad (2.1)$$

so an increase in chip rate results in an increase in data rate. The model for each channel includes additive white Gaussian noise, path loss, and multiple-access interference.

The transmit power is fixed and the same for all terminals. Let P_T denote the transmit power and d denote the distance between the transmitter and receiver. Also, allow λ_i to denote the wavelength of the carrier frequency for channel i (i.e., $\lambda_i = c/f_i$ where c is the speed of light). For this channel, the received power, P_{0_i} , is calculated as

$$P_{0_i} = P_T \left(\frac{\lambda_i}{4\pi d} \right)^\alpha \quad (2.2)$$

where α is known as the *path loss factor* [12]. Even though we consider multiple channels, a single omni-directional antenna model is employed in which it is assumed that the antenna gains are unity for all carrier frequencies. We also assume the path loss factor is the same for all channels. An area of future work is to develop improved models for the antennas and path loss.

The probability that a packet is successfully acquired and decoded depends on the symbol-energy to interference plus noise ratio (EINR). We briefly summarize the EINR model here, and additional details are found in [13]. Even though the transmit power is

the same for all channels, the chip duration and path loss are not, and the received symbol energy for channel i is $NP_{0_i}T_{C_i}$. Let N_0 denote the one-sided noise power spectral density. We assume that the receiver bandwidth for channel i , B_i , is $B_i = 1/T_{C_i}$. Let P_{I_i} denote the received power due to multiple-access interference from all transmissions except the intended transmission. The average spectral density due to multiple-access interference is P_{I_i}/B_i . The EINR for channel i is defined as

$$\mathcal{E}_i = \frac{NP_{0_i}T_{C_i}}{N_0 + P_{I_i}T_{C_i}}. \quad (2.3)$$

An acquisition header precedes each transmission. The receiver must acquire this header before the packet can be demodulated and decoded. For each channel, a single acquisition threshold is selected via [14] that provides acceptable performance for a variety of different channel conditions as described in [15]. The acquisition threshold is chosen so that performance is limited by the probability of successfully decoding the packet rather than acquiring it. The packet error probability model for this system is described in [13]. This probability is computed using the bit error probability and the first-event error probability for the convolutional code.

We define the *communication range* as the value of d that results in a target $\mathcal{E}_i$ for channel i with no multiple-access interference. To illustrate the difference in communication ranges for different channels consider a target EINR of β and fixed transmit power. Let Δ_i denote the maximum distance between a transmitter and receiver to achieve the target EINR assuming no multiple-access interference for channel i . Using

(2.1), (2.2), and (2.3) and solving for the distance, Δ_i , we see that Δ_i is related to f_i and D_i by

$$\Delta_i = \frac{1}{f_i^{\alpha} \sqrt{D_i}} \cdot \frac{c}{4\pi} \left(\frac{P_T R}{N_0 \beta} \right)^{\frac{1}{\alpha}}. \quad (2.4)$$

This illustrates that Δ_i decreases with an increase in carrier frequency or an increase in data rate. Using the assumption above, a channel with a higher carrier frequency has a larger data rate and hence a smaller communication range. For our system, channel 1 has the lowest carrier frequency and longest communication range among all the channels.

2.2 Link layer model

A channel-access protocol for a system with multiple channels is described in [13], however, the protocol assumes that the communication range and data rate are the same for all channels. We describe the key details of the channel-access protocol next, and in Chapter 3 we describe our modifications to the protocol that account for our system model. Channel 1 is reserved for the control channel and the remaining $M-1$ channels are for traffic. Request-to-send (RTS) and clear-to-send (CTS) packets are transmitted on the control channel and serve to reserve access on a traffic channel for a data packet transmission. Packets transmitted on the traffic channels are data packets as well as positive acknowledgment (ACK) and negative acknowledgement (NACK) packets. The source terminal sends an RTS packet to initiate a transmission with the destination terminal. This RTS packet includes a list of the traffic channels that are available to the source terminal. A traffic channel is *available* if it is currently unblocked.

Determining when a traffic channel is blocked is described below. If the destination terminal acquires and decodes the RTS packet, it checks if the transmission is acceptable. The transmission is *acceptable* if at least one of the traffic channels that are available to the destination terminal matches a channel indicated by the source terminal in the RTS packet. If the destination terminal deems the transmission acceptable, it sends a CTS packet indicating the traffic channel on which the data packet transmission will occur. The destination terminal then tunes to that traffic channel to await the data packet transmission. If the source terminal acquires and decodes the CTS packet, it transmits the data packet to the destination terminal on the traffic channel indicated in the CTS packet. Upon the acquisition of the data packet, the destination terminal responds with an ACK packet if the data packet is decoded and with a NACK packet if the data packet is not decoded.

Suppose we have the scenario depicted in Figure 2.1 in which terminal A wishes to transmit to terminal B . The traffic channel availability for each terminal is listed in Table 2.1. As shown, terminal A transmits an RTS packet indicating its available channels (i.e., 3 and 4) to terminal B . Terminal B acquires and decodes this RTS packet and replies with a CTS packet indicating that the packet transmission should occur on channel 4. Channel 4 is chosen because it is the only channel indicated in the RTS packet that is available to terminal B . Terminal A transmits the data packet on channel 4 and the packet is acquired and decoded by terminal B . Lastly, terminal B transmits an ACK packet which is acquired and decoded by terminal A . New rules for selecting available channels are described in Chapter 3.

Figure 2.1 Sample transmission from terminal *A* to terminal *B*

Terminal	Channel Availability		
	2	3	4
A	blocked	unblocked	unblocked
B	unblocked	blocked	unblocked

Table 2.1 Channel availability for terminals in Figure 2.1

We assume both *receiver-directed* and *common* spreading codes are available to the terminals (e.g., see [16] or [17]). An RTS, ACK, NACK, or data packet is transmitted using a receiver-directed spreading code. These transmissions can only be acquired by their intended recipient. A CTS packet is transmitted using a common spreading code and can be received by any neighbor that is in the receive mode on the control channel.

A channel-access protocol can be classified as either a blocking or non-blocking protocol. For the blocking protocols considered in this thesis, a receiver uses the CTS packet to signal to its neighbors that they should not initiate a new transmission on the same traffic channel while the receiver is using the channel. For a non-blocking protocol, the receiver does not attempt to prevent other terminals from transmitting. If a neighboring terminal acquires and decodes a CTS packet intended for another terminal, referred to as an *overheard CTS* packet, and if a blocking channel-access protocol is being utilized, the terminal will refrain from using the channel indicated by the CTS packet for a period of time equivalent to the duration of the data packet and subsequent ACK packet transmissions. This channel is considered *blocked*. However, if a non-blocking channel-access protocol is being utilized, overheard CTS packets are ignored and the channel indicated by the CTS packet will not be blocked.

After receiving or transmitting a packet on a traffic channel, a terminal may initiate a new attempt to forward a data packet. However, this terminal does not know the current availability of the traffic channels because it has not been listening on the control channel. To reduce the chance that this terminal uses a traffic channel that is not available, a *pacing* mechanism is enabled. This mechanism requires a terminal to listen on the control channel for a certain period of time to learn the availability of the traffic channels before initiating another forwarding attempt. The calculation of the pacing time is described in [13]. A terminal waiting for a CTS packet, data packet, or ACK packet that fails to acquire the transmission, times out and declares the transmission attempt unsuccessful. The timeout time is calculated using the same pacing mechanism. Pacing

also reduces contention on the control channel and improves fairness. The details of pacing are further explained in [13].

2.3 Network layer model

Least-resistance routing (LRR) [18] is a routing protocol in which each link is assigned a resistance. This link resistance is a measure of the quality of the link, the ability to forward a packet on the link, and the ability to receive and store a packet. Consider the link from terminal A to terminal B . The metric $IR(A,B)$ is based on the link quality for the forward link and the metric $L(A,B)$ is based on the recent history of unsuccessful transmission attempts for the forward link. The link resistance measure of the link from terminal A to B is calculated as

$$LR(A,B) = L(A,B) + IR(A,B). \quad (2.5)$$

The route resistance for a source-destination pair is the sum of the link resistances for the links in the route. New metrics are described in Chapter 3.

Information needed for LRR is transmitted in packet radio organization packets (PROPs), data packets, and acknowledgements. Data packets update the link resistance of the reverse link of a transmission while acknowledgements update the link resistance of the forward link of a transmission. PROPs are network layer packets that contain control information needed to build routing tables. A distributed and asynchronous routing protocol based on the Bellman-Ford algorithm [19] is used with LRR. A PROP also contains a table of incoming resistance values for the reverse links from the neighbors of the terminal to itself. Each terminal periodically transmits a PROP. For the system considered in this thesis, PROPs are assigned to a traffic channel in a cyclical manner.

For example, if there are three channels, the first, second, and third PROP will be transmitted on channels 2, 3, and 2, respectively. When the assigned traffic channel is available, the RTS packet for the PROP is transmitted on the control channel and the PROP is transmitted on the assigned traffic channel. Both transmissions use the common spreading code.

CHAPTER THREE

PROTOCOLS

In this section, we present our channel-access and routing protocols. The channel-access protocol includes new methods for selecting the traffic channel for a data packet transmission. The routing protocol uses our new metrics to assign a link resistance that accounts for the different channel characteristics. These protocols are designed to cooperate with one another and to take advantage of the multiple traffic channels available to the radio.

3.1 Channel-access protocol

Our new channel-access protocol is an extension to the link-layer protocols described in Section 2.2. A new addition to the system is the ability to declare a traffic channel as good or bad. A terminal keeps track of the outcome of recent transmissions and receptions on each of its traffic channels to each of its neighbors. If a traffic channel from terminal A to terminal B is declared *good*, then terminal A is allowed to transmit to terminal B using that particular channel. However if the traffic channel is declared *bad*, terminal A is not permitted to transmit to terminal B using that channel.

An overview of the channel-access protocol is outlined in Figure 3.1. All traffic channels for each source-destination pair are initially bad. A traffic channel is declared good for transmitting from terminal A to terminal B when terminal A receives a PROP on that particular channel from terminal B . A source terminal keeps a counter, C_{err} , for each traffic channel to each neighbor. This counter keeps track of the number of NACK

packets received and the number of CTS packets that are received without receiving the corresponding acknowledgement for the data packet. When C_{err} exceeds a threshold, γ , the traffic channel is declared bad. A terminal resets C_{err} for a traffic channel to a neighbor whenever a PROP or ACK packet is received on the traffic channel from that neighbor. If all the traffic channels from terminal A to B are bad, terminal A removes B as its neighbor and A updates its routing tables.

For the channel-access protocol described in Section 2.2, the selection of a traffic channel depends on the blocking status of the channels. We extend the protocol to also consider the good or bad status of the channels. For a channel-access protocol with blocking enabled, a *free* channel refers to a traffic channel that is good and is not blocked. If blocking is not enabled, a free channel simply refers to a traffic channel that is good. Before the network layer sends a data packet to the MAC layer, it first checks if there exists at least one free channel. If there are no free channels available for the transmission, the packet is skipped and the next data packet in the queue is considered for forwarding.

The operation of the source and destination terminals for a forwarding attempt is shown in Figure 3.1. We consider four strategies for selecting a channel. The *highest frequency with blocking* approach finds the traffic channel with the largest carrier frequency that is not blocked at both the source and destination. The source terminal lists all of the free channels in the RTS packet. The destination terminal selects the channel with the largest carrier frequency from the RTS packet that is also free at the destination terminal. If a free traffic channel is not found, the destination ignores the RTS packet and

the data packet transmission does not occur. For our system, this method selects the channel with the fastest data rate and smallest communication range that is not blocked. This reduces the transmission time and limits the multiple-access interference created for the other terminals. While this method attempts to select the good channel with the fastest data rate, the source and destination will utilize another channel that is free rather than wait for the fastest channel to become free.

The second strategy is similar to the first, except the source and destination terminals must find that the good channel with the largest carrier frequency is not blocked in order to transmit the data packet, and this is called the *highest/deferred* approach. If the source terminal finds that the good traffic channel with the largest carrier frequency is blocked, the packet is also skipped and an RTS packet is not sent. Otherwise, the source terminal lists all the good channels in the RTS packet, and the destination terminal selects the traffic channel from the RTS packet with the largest carrier frequency that is also good at the destination terminal. The destination terminal ignores the RTS packet if the channel it selects is blocked. This limits the channel-access protocol to using the channel with the fastest data rate only, and a forwarding attempt must wait for the channel to become unblocked rather than use a slower channel that is not blocked.

The final two strategies are simpler. The third strategy does not consider blocking but just the carrier frequency, and the fourth strategy considers blocking only and ignores the carrier frequency. The *highest frequency without blocking* approach chooses the traffic channel with the largest carrier frequency that is good at both the source and destination terminals. Note that this method does not include blocking and the good

channel with the fastest data rate is always selected. The *random with blocking* approach has the source list all the good channels that are not blocked in the RTS packet. The destination determines which of the channels in the RTS are not blocked at the destination, and chooses one of the channels randomly with a uniform distribution. This method is similar to the scheme described in [13].

Figure 3.1 Base channel-access protocol for source and destination terminals

Another change to the basic channel-access protocol described in Section 2.2 concerns the processing of overheard CTS packets. The actions of terminals that acquire an overheard CTS packet are outlined in Figure 3.2. Because the control channel and the traffic channels have different data rates and carrier frequencies, the communication range on different channels can be significantly different. For the system model employed in this thesis, we assume that channels with a higher carrier frequency also have a larger data rate. From (2.4), we see that an increase in carrier frequency or an increase in data rate results in a smaller communication range for a particular channel.

Consider the example network of Figure 3.3 in which the system consists of four channels with Δ_i for each channel listed in Table 3.1. Terminal A initiates a forwarding attempt with terminal B and terminal B replies with a CTS packet indicating that the data packet transmission will occur on channel 4. This CTS packet is also acquired at terminal C since it is transmitted on the control channel. However, it is extremely unlikely that terminal C will have received a PROP on channel 4 from terminal A or B because the distances from terminal A to C and from terminal B to C are larger than the communication range on channel 4. A transmission from terminal C to any other terminal on channel 4 does not cause a significant amount of interference at terminals A and B . Thus, while terminal C can receive overheard CTS packets from terminals A and B , it is not necessary for terminal C to block channel 4. Because terminal C is unable to receive PROPs from terminals A and B on channel 4, terminal C has the links to terminals A and B on channel 4 as bad. Hence, we update the blocking protocol so that a terminal that overhears a CTS packet does not block the traffic channel listed in the CTS packet if the

terminal has declared both links to the terminals that are the source and destination of the CTS packet transmission on this channel bad.

Figure 3.2 Base channel-access protocol for neighboring terminals

Figure 3.3 Example network

Channel	Δ_i
4	322.8 m
3	473.7 m
2	813.4 m
1 (Control)	813.4 m

Table 3.1 Δ_i for channels of example network

3.2 Routing protocol

We have developed two new channel metrics that are used to characterize the traffic channels. These channel metrics are incorporated into the link metric, $IR(A,B)$, for the link from terminal A to B . The link metric is used in conjunction with LRR as described in Section 2.3.

The *data rate* channel metric is based on the channel's data rate. Let W_i denote the channel metric for channel i , and let D_{max} denote the maximum data rate among all the traffic channels. The channel metric for channel i is

$$W_i = \frac{D_{max}}{D_i}. \quad (3.1)$$

For example, suppose channels 2, 3, and 4 of a system have data rates of 100kbps, 200kbps, and 1800kbps, respectively. The data rate channel metric values for channels 2, 3, and 4 are 18, 9, and 1, respectively. This channel metric accounts for the amount of time it takes for a data packet transmission. A transmission takes less time on a traffic channel with a lower channel metric value than a traffic channel with a higher channel metric value.

We also consider a second channel metric, called *fastest link*. The $M-1$ traffic channels are arranged in order of increasing data rate ($D_2 < D_3 < \dots < D_M$), and the channel metric for channel $M-i$ is

$$W_{M-i} = T^i, \quad 0 \leq i \leq M-2 \quad (3.2)$$

where T is the number of terminals in the network. This metric assigns the traffic channel with the highest data rate a value of 1. The channel metric values for the remaining traffic channels are much larger. With this metric, the routing protocol is limited to utilizing only the links with the highest data rates, when possible. A route includes a link at a lower data rate only if no route exists using only links at higher data rates.

The link metric for the link from terminal A to B , $IR(A,B)$, is equal to the minimum channel metric value among the traffic channels that are good. If none of the channels are good, the value for the link is infinity. Whether a channel is blocked or unblocked is not considered.

For the systems considered in this thesis, we assume that channels with a higher carrier frequency have a larger data rate. The maximum range for reliable communication assuming no interference for each channel listed in Table 3.1 is depicted in Figure 3.4.

The terminal's location is at point (0,0). Observing this graph makes it obvious that choosing a channel with a large carrier frequency produces interference in a smaller area. Also, by opting for channels with higher data rates, the length of time that the transmission causes interference for other terminals is reduced. Thus, a channel metric that emphasizes using links with a high data rate reduces the level of multiple-access interference from the transmission in addition to the amount of time that the transmission causes interference.

Figure 3.4 Δ_i ranges for the channels of the example network

The reception of a PROP, data packet, acknowledgement, or the lack of reception of an acknowledgment can cause the link resistance between the transmitter and receiver to change. As mentioned in Section 2.3, the reception of a PROP or data packet updates the link resistance for the reverse link and the reception of an acknowledgement updates the link resistance for the forward link. After the reception of a PROP, a channel will be declared good if it is not already good. The value of the link metric for the link from the receiver to the transmitter of the PROP is also updated.

Whenever the source A does not acquire an acknowledgement for a data packet transmission to destination B , the value of the unsuccessful attempts metric, $L(A,B)$, is incremented by inc_res . The failure of A to receive an acknowledgment from B indicates that B may not be in range of A on that channel. However, the link resistance measure is not incremented when a NACK packet is received. A packet that is acquired but not decoded may indicate a short period of multiple-access interference rather than a significant change in the position of the two terminals. This reflects the quality of the particular traffic channel and not necessarily the quality of the link between the source and destination. So instead of increasing the resistance of the link, we increment C_{err} for the traffic channel that was used for the transmission.

Recall that when the number of NACK packets received in addition to the number of expected acknowledgements that are not acquired exceeds γ ($C_{err} > \gamma$), the channel is declared bad. If a channel from terminal A to B is declared bad after acquiring a NACK packet, $L(A,B)$ is reset to zero and $LR(A,B)$ is simply equal to $IR(A,B)$, the new link metric. However, if the channel is declared bad after the failure to receive any type of

acknowledgment, $L(A,B)$ is not reset. Although the next transmission on this link will use a different channel, the unsuccessful attempts metric, $L(A,B)$ is increased by *inc_res* because of the unsuccessful forwarding attempt.

Whenever the link resistance is updated, the routes and route resistances for all destinations using that link are also updated. The route resistance is updated by adding any change in the link resistance to the current value of the route resistance. For each data packet transmission from terminal A to B , terminal A updates its routes and route resistances for all destinations that use the link to terminal B whether an ACK/NACK packet is received or no acknowledgement is received at all. Also whenever terminal B acquires a data packet from terminal A , terminal B will update all of its routes and route resistances for destinations that use the link to terminal A . Consider the example of Figure 3.5. The dotted line between two terminals represents a link between the terminals and the number associated with the dotted line represents the resistance for that link. The solid arrows illustrate the route from terminal A to D as $A-B-D$ and the dashed arrows illustrate the route from terminal A to E as $A-B-E$. Both routes have a resistance of 8. Assume one of the traffic channels becomes bad for the link from terminal A to B so that the resistance value of the link changes to 8. This causes the routes and route resistances to change as is depicted in Figure 3.6. The route from terminal A to E is now $A-C-E$ with a route resistance of 9, and the route from terminal A to D is now $A-C-E-D$ with a route resistance of 11.

Figure 3.5 Routing example

Figure 3.6 Routing example after link resistance update

CHAPTER FOUR

SIMULATION MODEL AND RESULTS

In this chapter, we investigate the performance of the channel-access and routing protocols presented in Chapter 3. A brief overview of the simulation model is given along with the values for key parameters. Simulation results for the approaches to channel access are first compared with one another. Then, the performance of channel access in conjunction with the channel metrics is examined.

4.1 Simulation parameters

An OPNET simulation is used to model the system and investigate the performance of the protocols formulated in Chapter 3. Our simulation model is an extension of the model described in [20] and we summarize the key details of the model next. The acquisition and packet error probability models of the physical layer follow the work of [13] and [15]. The acquisition header for each packet is fixed and the acquisition threshold is selected for each channel based on the work of [14]. The link layer follows the channel-access protocol and pacing mechanism of [13] while the network layer utilizes LRR as described in [18]. The link layer and network layer of the OPNET simulation are modified to include the channel-access and routing protocols discussed in Chapter 3. The simulation parameters used for all simulations are listed in Table 4.1.

Parameter	Value
Information bits per data packet	5000
Information bits per PROP packet	5000
Information bits per control packet	50
Spreading factor (N)	16
Number of channels (M)	4
Carrier frequency of control channel (f_1)	1GHz
Control channel data rate (D_1)	125kbps
Δ_i for control channel	1626 meters
Transmit power (P_T)	1.0 W
Path loss factor (α)	3
One-sided noise power spectral density (N_0)	4×10^{-21} W/Hz
C_{err} threshold (γ)	5
Increment for failed forwarding attempt (<i>inc res</i>)	0.25
Number of terminals (T)	25
Simulation duration	5000s
Queue size	10 pkts
Forwarding attempts (F)	6
Forwarding attempts using primary link (P)	4

Table 4.1 Parameters used by the simulation model

Each terminal generates packets via a Poisson packet generator and the destination for each packet is selected randomly with a uniform distribution among the other terminals in the network. A terminal is allowed up to F forwarding attempts for each packet. Each terminal has a primary and secondary outgoing link to each destination where the first P forwarding attempts occur on the primary outgoing link and the remaining attempts are made using the secondary outgoing link. After F failed forwarding attempts, the packet is discarded. A failed forwarding attempt occurs when the source terminal fails to receive a CTS packet after an RTS packet transmission or

fails to receive an ACK packet after a data packet transmission. The simulation employs lateral forwarding [18] to prevent a packet from being forwarded on a route with a loop.

The performance metric examined is the end-to-end success probability, which is the fraction of the packets generated that reach their destinations. In addition, we consider the *performance threshold* as the smallest generation rate for which the end-to-end success probability is less than 90%. For example, if the performance threshold for protocol A is 4.3 packets/second and is 3.6 packets/second for protocol B , then we say that the traffic that can be carried by protocol A increases by 19.4% over that which can be carried by protocol B . The performance metric and threshold are examined for each simulation as the packet generation rate increases.

4.2 Network scenarios

We consider three different network scenarios. Each scenario employs three traffic channels and one control channel. The carrier frequency for channels 2, 3 and 4 are 1GHz, 3GHz, and 9GHz, respectively. Note that the carrier frequency for the control channel and channel 2 differ by a small amount so that the channels are nonoverlapping. The differences between the scenarios involve the assignment of the data rates among the traffic channels. The differences between the data rates on the traffic channels are small in the small scenario, larger in the mid scenario, and the largest in the large scenario. The attributes for the small, mid, and large scenarios are in Tables 4.2, 4.3, and 4.4, respectively. The data rates for the small scenario differ by a factor of 1.5 between channels 3 and 4 and by a factor of 2.25 between traffic channels 2 and 4. These factors

are 1.5 and 3, respectively, for the mid scenario and are 3 and 9, respectively, for the large scenario.

Channel	f_i (GHz)	D_i (kbps)	Δ_i (meters)
2	1	125	1626
3	3	187.5	473
4	9	281.25	138

Table 4.2 Traffic channel attributes for the small scenario

Channel	f_i (GHz)	D_i (kbps)	Δ_i (meters)
2	1	125	1626
3	3	250	430
4	9	375	125

Table 4.3 Traffic channel attributes for the mid scenario

Channel	f_i (GHz)	D_i (kbps)	Δ_i (meters)
2	1	125	1626
3	3	375	376
4	9	1125	87

Table 4.4 Traffic channel attributes for the large scenario

4.3 Network topologies

Each scenario is tested for three different network topologies consisting of 25 terminals. For the small- and medium-scaled topologies, the terminals are arranged in a 5 by 5 grid as shown in Figure 4.1. The value of d for the small-scaled topology is 15m and the diameter is approximately 85m. For each scenario, this topology allows each terminal to transmit to every other terminal using any of the three traffic channels. The value of d for the medium-scaled topology is 87m. In this topology for each scenario, a terminal can only transmit to its closest neighbors on channel 4, a subset of terminals, C_M , on channel 3, and all terminals on channel 2. The large-scaled topology is composed of three clusters that are denoted A , B , and C in Figure 4.2. The distance between adjacent terminals, d_1 , is 85m. The distances d_2 and d_3 are 274m and 357m, respectively. The distance between clusters A and B , d_{AB} , is 600m. The distances d_{AC} and d_{BC} are the distances between clusters A and C and clusters B and C , respectively. These distances are both 376m. For each scenario, a terminal in cluster A and a terminal in cluster B can communicate directly using channel 2 only. To communicate directly between terminals in clusters A and C or clusters B and C , traffic channels 2 or 3 can be used. Also, for each scenario, this topology allows a terminal to communicate with its closest neighbors on channel 4, a subset of terminals, C_L , on channel 3 ($C_M > C_L$), and all terminals on channel 2.

Figure 4.1 Grid topology

Figure 4.2 Large-scaled topology

4.4 Channel-access independent of routing

The performance of the four strategies for selecting a traffic channel (i.e., highest frequency with blocking, highest/deferred, highest frequency without blocking, and random with blocking) is evaluated in this section for all combinations of topologies and scenarios. We have examined the performance of the channel-access strategies with two different network-layer models. In one model, relaying is disabled and a terminal must forward a packet directly to its destination. In the other model, relaying is permitted and a simple metric that results in minimum-hop routing is employed. However, for the topologies employed in this study, all terminals are within communication range for the channel with the lowest carrier frequency, so the difference between the two network-layer models is minor. We have found the performance and our conclusions for the channel-access strategies to be similar for both network-layer models. Due to space considerations, we present results for only the minimum-hop routing model here.

The performance results for the channel-access approaches in the small-, medium-, and large-scaled topologies for the small scenario are shown in Figures 4.3, 4.4, and 4.5, respectively. In Figures 4.6, 4.7, and 4.8 are the results from the mid scenario for the small-, medium-, and large-scaled topologies, respectively, and the results from the large scenario for the small-, medium-, and large-scaled topologies are in Figures 4.9, 4.10, and 4.11, respectively. Similar results were also obtained for investigations using a different set of carrier frequencies and data rates, and they are not included here.

Examining these figures reveals that the highest frequency with blocking approach performs well across all network topologies and scenarios. In fact, the highest frequency with blocking approach has larger success probabilities than the random with blocking and highest frequency without blocking approaches. In Figures 4.3- 4.11, we see that there is a small improvement in the success probabilities of the highest frequency with blocking approach over the random with blocking approach. The improvements in the performance thresholds in the small-, medium-, and large-scaled topologies for the small scenario are 3.125%, 4.2%, and 5.9%, respectively. These improvements are 7.1%, and 13.3% for the medium- and large-scaled topologies, respectively, for the mid scenario and are 4.5%, 3.2% and 8.3% for the small-, medium-, and large-scaled topologies, respectively, for the large scenario. The performance thresholds are identical for the highest frequency with blocking and random with blocking approaches in the small-scaled topology with the mid scenario. The success probabilities for both approaches are similar because both employ blocking and with heavy traffic loads, both utilize all of the traffic channels.

We have also examined the highest frequency with blocking and random with blocking approaches in networks in which some packets must be relayed to their destinations. In these networks, there is a modest improvement in network performance for the highest frequency with blocking approach compared to the random with blocking approach. Because some transmission attempts require a traffic channel with a lower carrier frequency, the highest frequency with blocking approach increases the probability

that transmissions on links that do not require a low carrier frequency do not use these channels.

The highest frequency with blocking approach achieves higher end-to-end probability of success values than the highest frequency without blocking approach. Because there are significant sources of multiple-access interference even in the large-scaled topology, blocking significantly improves the probability that a data packet transmission is successful. The network performance increase of the highest frequency with blocking approach over the highest frequency without blocking approach increases as the network size increases. As terminals move further apart, the distance between them becomes too large for transmissions to occur on the shorter traffic channels. Without blocking enabled, the longer traffic channels are used by more terminals simultaneously causing more interference to a larger set of terminals for a longer amount of time. The additional interference caused by these neighboring transmissions results in an increased probability that the receivers fail to acquire or decode the data packets. The improvement in the performance threshold of the highest frequency with blocking approach over that of the highest frequency without blocking approach in the large-scaled topology is 157%, 183% and 225% for the small, mid, and large scenarios, respectively. This performance increase decreases to 108%, 100%, and 100% for the medium-scaled topology with the small, mid, and large scenarios, respectively. It decreases even further to 106%, 74%, and 25% for the small-scaled topology with the small, mid, and large scenarios, respectively.

The highest frequency with blocking approach also has larger success probabilities than the highest/deferred approach in networks for which the density of the

terminals is medium or high. The difference in success probabilities is the largest for high density networks, and the gain decreases for lower density networks. The traffic that can be carried by the highest frequency with blocking approach at our performance threshold increases by 120%, 100%, and 43% over that which can be carried by the highest/deferred approach at our performance threshold in the small-scaled topology for the small, mid, and large scenarios, respectively. This performance improvement decreases to 56%, 50% and 28% for the medium-scaled topology with the small, mid, and large scenarios, respectively. Because the short fast links with high carrier frequencies are used more often in dense networks, the highest/deferred approach defers many transmissions and does not utilize all of the channels.

Although the highest frequency with blocking approach has the largest success probabilities in many networks, the highest/deferred approach performs well in networks in which the density of the terminals is low. In the large-scaled topology for the small and large scenarios, the performance threshold of the highest/deferred approach is higher than that of the highest frequency with blocking approach by 5.6% and 7.7%, respectively. The performance thresholds are approximately the same for the two in the large-scaled topology with the mid scenario. This shows that it is advantageous to reserve the long links with low data rates in networks with smaller densities. Although the highest/deferred approach performs well in these networks, its performance is much worse in medium and large density networks. This is the reason we claim that the highest frequency with blocking approach has the best overall performance. However, when used

in conjunction with routing, there are situations in which the highest/deferred approach to channel access performs very well, and this is illustrated in the next section.

Figure 4.3 Performance of channel-access strategies for small-scaled topology with the small scenario

Figure 4.4 Performance of channel-access strategies for medium-scaled topology with the small scenario

Figure 4.5 Performance of channel-access strategies for large-scaled topology with the small scenario

Figure 4.6 Performance of channel-access strategies for small-scaled topology with the mid scenario

Figure 4.7 Performance of channel-access strategies for medium-scaled topology with the mid scenario

Figure 4.8 Performance of channel-access strategies for large-scaled topology with the mid scenario

Figure 4.9 Performance of channel-access strategies for small-scaled topology with the large scenario

Figure 4.10 Performance of channel-access strategies for medium-scaled topology with the large scenario

Figure 4.11 Performance of channel-access strategies for large-scaled topology with the large scenario

4.5 Channel-access with routing

In this section, we evaluate the performance of the channel-access protocol of Section 3.1 combined with the routing metrics discussed in Section 3.2. We compare the data rate and fastest link channel metrics with a min hop channel metric. The *min hop* channel metric simply sets the channel metric of each traffic channel equal to one, and this results in minimum-hop routing. Because the highest frequency with blocking approach has the largest success probabilities for a variety of topologies and network scenarios, our first investigations of the channel metrics use this approach. We found that for the small-scaled topology of each scenario, the performance thresholds of the various channel metrics are nearly identical, and results for these simulations are not shown. The channel metric results for the medium- and large-scaled topologies with the small scenario are in Figures 4.12 and 4.13, respectively. Figures 4.14 and 4.15 depict the results for the medium- and large-scaled topologies, respectively, with the mid scenario, and the results for the medium- and large-scaled topologies with the large scenario are in Figures 4.16 and 4.17, respectively.

The data rate channel metric, which accounts for the data rate of the channel, has higher end-to-end success probability values than the min hop channel metric and the fastest link channel metric. There is a 16% and 11% increase in the performance thresholds of the data rate channel metric over those of the min hop channel metric for the medium- and large-scaled topologies, respectively, with the small scenario. These percentages increase to 16.7% and 23.5% for the medium- and large-scaled topologies, respectively, with the mid scenario and increase even further to 46.88% and 85% for the

medium- and large-scaled topologies, respectively, with the large scenario. The poor performance of the min hop channel metric is because it assumes that all links are equal.

We now compare the results of the fastest link channel metric with those of the data rate and min hop channel metrics. For the medium- and large-scaled topologies with the small and mid scenarios (Figures 4.12-4.15), we see that the success probabilities of the fastest link channel metric is even worse than that of the min hop channel metric. The amount of traffic that can be carried at our performance threshold by the data rate channel metric increases by 38% and 25% over that which can be carried at our performance threshold by the fastest link channel metric in the medium- and large-scaled topologies, respectively, with the small scenario. This increase is 29.6% and 23.5% in the medium- and large-scaled topologies, respectively, with the mid scenario. In Figure 4.17, we see that the performance threshold of the fastest link channel metric is larger than that of the min hop channel metric but still lower than that of the data rate channel metric by 26%. Although the fastest link channel metric emphasizes using the shorter links with faster data rates, it is not taking advantage of the additional capacity available on the other channels.

While the data rate channel metric has a higher performance threshold than the other metrics in most situations, notice that for the medium-scaled topology with the large scenario, the fastest link channel metric has the highest performance threshold, as shown in Figure 4.16. In fact, the performance threshold of the fastest link channel metric is higher than that of the data rate channel metric by 8.5%. This shows that the

fastest link channel metric may be advantageous in some situations, and we present additional investigations next.

Figure 4.12 Performance of channel metrics for medium-scaled topology with the small scenario

Figure 4.13 Performance of channel metrics for large-scaled topology with the small scenario

Figure 4.14 Performance of channel metrics for medium-scaled topology with the mid scenario

Figure 4.15 Performance of channel metrics for large-scaled topology with the mid scenario

Figure 4.16 Performance of channel metrics for medium-scaled topology with the large scenario

Figure 4.17 Performance of channel metrics for large-scaled topology with the large scenario

Although the highest frequency with blocking approach to channel access has larger success probabilities in most of our topologies and scenarios, a combination of the highest/deferred approach to channel access, certain networks, and certain channel metrics allow the highest/deferred approach to perform considerably better than the highest frequency with blocking approach. Three of the combinations are considered next, and the results are shown in Figures 4.18-4.20. In Figure 4.19, we see that the performance threshold of the data rate channel metric is 17.5% higher with the highest frequency with blocking approach than it is with the highest/deferred approach. However, this is not true in Figures 4.18 and 4.20 where the performance threshold of the data rate channel metric is 15% and 20.8% higher, respectively, with the highest/deferred approach

than it is with the highest frequency with blocking approach. Both of these later scenarios are for the large-scaled topology and suggest that a forwarding attempt that can utilize a channel with a shorter communication range should wait for the channel to become available rather than use a channel with a longer communication range. These long-range channels are needed for forwarding attempts that cannot utilize the short-range channels.

We observe that a moderate improvement in network performance is achieved with the data rate channel metric if the channel-access strategy is matched to the particular topology and scenario. Because the highest/deferred approach has larger success probabilities in certain topologies and scenarios, we investigate alternative channel metrics for this particular channel-access strategy. Using the data rate channel metric, we modify the weights for the second and third channels to examine the sensitivity to these metric values. Testing a wide range of channel metric values, the values that produce the best network performance for the particular topologies and scenarios in Figures 4.18, 4.19, and 4.20 are shown in Table 4.5. We refer to these as the *alternative data rate* channel metrics.

Figures 4.18-4.20 show that a combination of the highest/deferred approach with the alternative data rate channel metric has larger success probabilities than the highest frequency with blocking approach and data rate channel metric as well as the highest/deferred approach and data rate channel metric. Figure 4.18 shows that the performance threshold of the highest/deferred approach and alternative data rate channel metric is higher than that of the highest frequency with blocking approach and data rate channel metric by 20%. This is also true for the medium-scaled topology with the large

scenario (Figure 4.19) by 42.5% and the large-scaled topology with the large scenario (Figure 4.20) by 29.2%. This shows that the performance threshold of the highest/deferred approach can be significantly better than that of the highest frequency with blocking approach for a particular network if an appropriate channel metric is also employed.

Channel	Figure 4.18		Figure 4.19		Figure 4.20	
	Data rate metric	Alternative data rate metric	Data rate metric	Alternative data rate metric	Data rate metric	Alternative data rate metric
2	2.25	4.5	9	9	9	9
3	1.5	3	3	4.5	3	4.5
4	1	1	1	1	1	1

Table 4.5 Comparison of the data rate and alternative data rate metrics for Figures 4.18-4.20

Figure 4.18 Performance of channel-access strategy and channel metric combinations for large-scaled topology with the small scenario

Figure 4.19 Performance of channel-access strategy and channel metric combinations for medium-scaled topology with the large scenario

Figure 4.20 Performance of channel-access strategy and channel metric combinations for large-scaled topology with the large scenario

Next, consider a preliminary investigation to jointly select both the channel-access strategy and the routing metric. Our preliminary study is for the medium-scaled topology with the large scenario and the highest/deferred channel-access strategy. A new channel metric, *data rate/nbr count*, is based on both the network connectivity and channel data rate. For this topology, there are approximately 4, 24, and 24 neighbors on channels 2, 3, and 4, respectively. Let $Nbrs_i$ denote the number of neighbors for channel i , and let W_D_i denote the channel metric for channel i using the data rate channel metric from (3.1). The channel metric for channel i for the data rate/nbr count channel metric is

$$W_i = Nbrs_i + W\_D_i. \quad (4.1)$$

By accounting for the number of neighbors as well as the data rate of the traffic channel, the data rate/nbr count channel metric has end-to-end probability of success values close to that of the alternative data rate channel metric in the medium-scaled topology with the large scenario. These results are depicted in Figure 4.21. The data rate/nbr count channel metric decreases the gap between the performance thresholds of the data rate channel metric and the alternative data rate channel metric from 67.5% to 6.35%. However, this combination of channel-access strategy and channel metric performs poorly for the small-scaled topologies, in part due to the channel-access strategy failing to utilize all the channels.

Future work will investigate channel metrics that consider the data rate of the channel as well as a better estimate of the activity on the channels and at the terminals. The activity at a terminal can be more accurately determined by monitoring the fraction of time that a terminal is on-air transmitting, or receiving, or is blocked because a neighbor has reserved a channel. The channel activity gives a more accurate estimate of the business of the channels rather than simply using the number of neighbors. A joint channel-access and routing protocol should adapt the strategy for channel access as well as the channel metric values based on measurements of the network environment.

Figure 4.21 Comparison of data rate/nbr count channel metric for medium-scaled topology with the large scenario

CHAPTER FIVE

CONCLUSIONS

This study considers ad hoc networks employing frequency-agile radios that can use multiple channels. Each radio has a single half-duplex transceiver that can change its carrier frequency and chip rate. We implement new channel-access strategies and channel metrics for routing specifically designed for this type of software-defined radio. The channel-access strategies that account for the carrier frequency and data rate increase network performance over a strategy that does not. The performance is further increased when our new channel-access strategies are used in conjunction with our channel metrics. We show that these protocols perform well for a variety of different topologies and networks.

We conclude that our highest frequency with blocking channel-access strategy works well for a variety of network densities and channel conditions. This approach employs blocking and transmits data packets on the unblocked traffic channel with the highest carrier frequency. The highest/deferred approach also employs blocking and transmits on the traffic channel having the highest carrier frequency if unblocked and defers the transmission if the traffic channel is blocked. This approach can produce very good network performance compared to the highest frequency with blocking approach in scenarios for which it is important to reserve heavily utilized long-range channels, but in most of the situations investigated here, it performs poorly.

The data rate channel metric is investigated along with the two above-mentioned channel-access strategies. This routing metric assigns channel metric values to traffic

channels based on the amount of time it takes to transmit a packet using that particular traffic channel. Improved network performance is achieved for this channel metric compared to minimum-hop routing and a channel metric designed to select routes using only the links with the fastest data rate.

We have found that simply selecting the highest frequency with blocking channel-access strategy and the data rate channel metric results in good network performance across a wide range of topology and channel characteristics. However, additional improvements in network performance are possible if the channel-access strategy or routing metric is selected for the specific operating conditions. Future work will consider mechanisms for measuring the environment, including measures such as connectivity and activity, and mechanisms to utilize these measures to adapt channel access and routing.

REFERENCES

1. A. J. Goldsmith and S. B. Wicker, "Design challenges for energy-constrained ad hoc wireless networks," *IEEE Wireless Communications*, vol. 9, no. 4, pp. 8-27, Aug. 2002.
2. E. M. Royer, C. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Personal Communications*, vol. 6, no. 2, pp. 46-55, April 1999.
3. C. Evci and B. Fino, "Impact of software radio on efficient spectrum sharing," in *Proceedings of the ANWIRE Workshop on Reconfigurability*, Sept. 2003.
4. J. Mitola III, and G. Maguire Jr., "Cognitive radio: Making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13-18, Aug. 1999.
5. S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201-220, Feb. 2005.
6. I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127- 2159, May 2006.
7. A. Adya, P. Baul, J. Padhye, A. Wolman, and L. Zhou, "A multi-radio unification protocol for IEEE 802.11 wireless networks," in *Proceedings of the International Conference on Broadband Networks*, Oct. 2004.
8. R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in *Proceedings of the International Conference on Mobile Computing and Networking*, Sept. 2004.
9. K. N. Ramachandran, E. M. Belding, K. C. Almeroth, and M. M. Buddhikot, "Interference-aware channel assignment in multi-radio wireless mesh networks," in *Proceedings of the International Conference on Computer Communications*, April 2006.
10. P. Kyasanur and N. Vaidya, "Routing and interface assignment in multi-channel multi-interface wireless networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference*, March 2005.

11. J. So and N. Vaidya, "A routing protocol for utilizing multiple channels in multi-hop wireless networks with a single transceiver," University of Illinois at Urbana-Champaign, Urbana, IL, Tech. Rep., Oct. 2004.
12. T. S. Rappaport, *Wireless Communications*, 2nd ed., Upper Saddle River, NJ: Prentice Hall, 2002, pp. 105-110.
13. A. Raghavan and C. Baum, "An unslotted multichannel channel-access protocol for distributed direct-sequence networks," *Mobile Networks and Applications*, vol. 5, no. 1, pp. 49-56, 2000.
14. D. L. Noneaker, A. Raghavan, and C. Baum, "The effect of automatic gain control on serial matched-filter acquisition in direct-sequence packet radio communications," *IEEE Transactions on Vehicular Technology*, vol. 50, no. 4, pp. 1140-1150, July 2001.
15. A. R. Raghavan and C. Baum, "Analysis of a serial acquisition scheme for unslotted distributed direct-sequence packet radio networks," in *Proceedings of the IEEE International Conference on Communications*, vol. 3, pp. 1248-1252, June 1998.
16. M. B. Pursley, "The role of spread spectrum in packet radio networks", *Proceedings of the IEEE*, vol. 75, no. 1, pp. 116-134, Jan. 1987.
17. J. G. Andrews, S. Weber, and M. Haenggi, "Ad hoc networks: To spread or not to spread?" *IEEE Communications Magazine*, vol. 45, no. 12, pp. 84-91, Dec. 2007.
18. M. B. Pursley and H. B. Russell, "Routing in frequency-hop packet radio networks with partial-band jamming," *IEEE Transactions on Communications*, vol. 41, no. 7, pp. 1117-1124, July 1993.
19. D. Bertsekas and R. Gallager, *Data Networks*, 2nd ed., Saddle River, NJ: Prentice Hall, 1992, pp. 404-410.
20. A. R. Raghavan, "Protocols for distributed direct-sequence packet radio networks," Ph.D. dissertation, Clemson University, Clemson, SC, 1999.