

**Performance Study on
a Dual Prohibition Multiple Access Protocol
in Mobile Ad Hoc and Wireless Mesh Networks**

**By
Qian Wu**

A thesis submitted to the Department of Electrical and Computer Engineering
in conformity with the requirements for
the degree of Master of Science (Engineering)

Queen's University
Kingston, Ontario, Canada

September, 2007

Copyright © Qian Wu, 2007

ABSTRACT

Wireless networks are less reliable than wired networks because channels are “exposed” to the surrounding environment that is susceptible to interference and noise. To minimize losses of data due to collisions, wireless networks need a mechanism to regulate the access on the transmission medium. Medium Access Control (MAC) protocols control access to the shared communication medium so that it can be used efficiently.

In this thesis, we first describe the collision-controlled Dual Prohibition Multiple Access (DPMA) protocol [45]. The main mechanisms implemented in DPMA, such as binary dual prohibition, power control, interference control, and support for differentiated services (DiffServ), are presented in detail. We conducted a thorough simulation study on DPMA protocol from several aspects. First, we conduct simulations to observe the effects of binary competition number (BCN), unit slot length and safe margin on the performance of DPMA. Secondly, the DiffServ capability of DPMA is demonstrated through simulation results. Finally, we compare the DPMA protocol with the CSMA/CA protocol and find that DPMA with optimal configuration has better performance than CSMA/CA under both low and high network density.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor, Professor Chihsiang Yeh. His guidance, advice, and continuous support have played an irreplaceable role throughout my entire dissertation. I am very grateful to his patient guidance, valuable insights and professional advice in this work. It is my fortune and honor to have him as my advisor.

I would like to thank my wonderful colleague and friend Hairong Zhou. She has given me great help. She gave me many technical insights in this thesis. She also encouraged me all the time when I was frustrated.

I also would like to thank my many friends and classmates who made my studying and living at Queen's University a pleasant and unforgettable experience.

Last but not least, I give my dedicated thanks to my parents. Without their support and encouragement, I would not be able to finish the long journey towards the Master degree.

TABLE OF CONTENTS

ABSTRACT	i
ACKNOWLEDGMENTS.....	ii
LIST OF FIGURES.....	vi
LIST OF TABLES.....	ix
LIST OF ACRONYMS AND SYMBOLS.....	x
CHAPTER 1 INTRODUCTION	1
1.1 BACKGROUND	1
1.2 MOTIVATIONS AND OBJECTIVES.....	3
1.3 THESIS OUTLINE.....	6
CHAPTER 2 LITERATURE REVIEW ON MAC PROTOCOLS	7
2.1 SINGLE CHANNEL MAC PROTOCOLS	7
2.1.1 IEEE 802.11.....	7
2.1.2 IEEE 802.11e – QoS Extension of IEEE 802.11.....	10
2.1.3 Power Control Medium Access.....	12
2.2 SEPARATE CHANNEL MAC PROTOCOLS.....	14

2.2.1	Separate Channel MAC without Busy Tone	16
2.2.2	Separate Channel MAC with Busy Tone	18
2.2.3	Separate Channel with Power Control.....	22
2.2.4	Other Separate Channel MAC Protocols.....	25
2.3	SUMMARY	26
 CHAPTER 3 THE DUAL PROHIBITION MULTIPLE ACCESS (DPMA)		
SCHEME		
29		
3.1	PROTOCOL OVERVIEW	30
3.2	DPMA PROTOCOL DESCRIPTION.....	31
3.2.1	Binary Countdown Dual Prohibition.....	32
3.2.2	Power Control.....	35
3.2.3	Additive Interference Avoidance.....	37
3.2.4	Support for DiffServ and Fairness.....	40
3.2.5	Advantages of DPMA Protocol.....	42
3.3	SUMMARY	44
 CHAPTER 4 PERFORMANCE EVALUATION.....		
45		
4.1	SIMULATION MODEL	45
4.1.1	Experimental Setting	45
4.1.2	Performance Metric	47
4.2	DISCUSSIONS ON SIMULATION RESULTS.....	48
4.2.1	Effect of Binary Competition Number (BCN)	48
4.2.2	Effect of Slot Duration	54

4.2.3	Effect of Safe Margin	56
4.2.4	QoS Differentiation Capability of DPMA.....	58
4.2.5	Performance Comparisons for DPMA and CSMA/CA.....	60
4.3	SUMMARY	71
CHAPTER 5	CONCLUSIONS AND FUTURE WORK.....	73
5.1	CONCLUSIONS	73
5.2	FUTURE WORK	76
BIBLIOGRAPHY.....		77
APPENDIX	CONFIDENCE INTERVALS	86

LIST OF FIGURES

Figure 1.1 Ad hoc network architecture.	2
Figure 1.2 The hidden terminal problem.....	3
Figure 1.3 The exposed terminal problem.....	4
Figure 2.1 Virtual Carrier Sensing using CSMA/CA.....	8
Figure 2.2 Power control example in PCM protocol.....	14
Figure 2.3 Dedicated control channel approach.	17
Figure 2.4 A scenario that B's CTS is destroyed at D by C's RTS/CTS.	19
Figure 2.5 DBTMA frequency chart	21
Figure 2.6 Tradeoff of using directional BTr	25
Figure 3.1 The time diagram of the control channel in DPMA.....	32
Figure 3.2 The slot assignment for prohibition slots in DPMA	33
Figure 3.3 Comparison of power control and fixed transmission power.	36
Figure 3.4 Time diagram of prohibiting signals.	37
Figure 3.5 Example of DiffServ and fairness in DPMA	41
Figure 4.1 Network throughputs for CSMA/CA and DPMA with different BCNs.	50

Figure 4.2 Average delays for CSMA/CA and DPMA with different BCNs.	50
Figure 4.3 Collision rates for CSMA/CA and DPMA with different BCNs.....	51
Figure 4.4 Blocking rates for CSMA/CA and DPMA with different BCNs.....	51
Figure 4.5 Maximum throughputs for different ID lengths.....	53
Figure 4.6 Average delays for different ID lengths.....	53
Figure 4.7 Collision rates for different ID lengths.	54
Figure 4.8 Structure of transmitter/receiver subslots.....	55
Figure 4.9 Experiment on the effect of unit slot length in DPMA.....	56
Figure 4.10 The effect of safe margin on network performance.....	57
Figure 4.11 Differentiated throughput vs. arrival rate for DPMA.....	58
Figure 4.12 Differentiated delay vs. arrival rate for DPMA	59
Figure 4.13 Throughput comparison between DPMA and CSMA/CA (Density = 10).	60
Figure 4.14 Throughput comparison between DPMA and CSMA/CA (Density = 20).	61
Figure 4.15 Average delay comparison between DPMA and CSMA/CA (Density = 10). 62	
Figure 4.16 Average delay comparison between DPMA and CSMA/CA (Density = 20). 63	
Figure 4.17 Collision rate comparison between DPMA and CSMA/CA (Density = 10). . 64	
Figure 4.18 Collision rate comparison between DPMA and CSMA/CA (Density = 20). . 64	
Figure 4.19 Blocking rate comparison between DPMA and CSMA/CA (Density = 10). . 66	
Figure 4.20 Blocking rate comparison between DPMA and CSMA/CA (Density = 20). . 66	
Figure 4.21 Throughput comparison between CSMA/CA and DPMA with different unit slot lengths.....	67

Figure 4.22 Average delay comparison between CSMA/CA and DPMA with different unit slot lengths.....	68
Figure 4.23 Collision rate comparison between CSMA/CA and DPMA with different unit slot lengths.....	68
Figure 4.24 Throughput comparison between CSMA/CA and DPMA with different BCNs.	69
Figure 4.25 Average delay comparison between CSMA/CA and DPMA with different BCNs.	70
Figure 4.26 Collision rate comparison between CSMA/CA and DPMA with different BCNs.	70

LIST OF TABLES

Table 4.1 Simulation parameters setting	47
---	----

LIST OF ACRONYMS AND SYMBOLS

AC	Access category
ACK	Acknowledgement
AP	Access Point
AIFS	Arbitrary Inter-Frame Space
AIFSN	Arbitrary Inter-Frame Space Number
BCN	Binary Competition Number
BT _r	Receive Busy Tone
BT _t	Transmit Busy Tone
CAI	Current Additive Interference
CSMA	Carrier Sense Medium Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear-To-Send
CW	Contention Window
CW _{max}	Maximum Contention Window
CW _{min}	Minimum Contention Window
DBTMA	Dual Busy Tone Multiple Access

DCA	Dynamic Channel Assignment
DCF	Distributed Coordinate Function
DiffServ	Differentiated Services
DPMA	Dual Prohibition Multiple Access
EDCA	Enhanced Distributed Channel Access
GPS	Global Positioning System
HCCA	Hybrid Coordination Channel Access
HCF	Hybrid Coordination Function
LANs	Local Area Networks
MAC	Medium Access Control
MAI	Maximum Allowed Interference
MANET	Mobile Ad Hoc Networks
MAP	Maximum Allowed transmission Power
NAV	Network Allocation Vector
PCF	Point Coordination Function
QoS	Quality of Service
RIT	Remaining Interference Tolerance
RTS	Require-To-Send
SIR	Signal to Interference Ratio
WLAN	Wireless Local Area Network
CS_Thrs	Carrier sensing threshold
d	Distance between the transmitter and the receiver
G_t	Transmitter antenna gain
G_r	Receiver antennal gain
L	System loss factor

n	Path loss exponent
N	Total number of nodes
λ	Packet transmission rate
G_{tr}	Stationary channel gain between the transmitter and the intended receiver
P_{CAI}	Current additive interference
P_{\max}	Maximum transmit power level
P_{suff}	Minimum necessary power level
P_{TP}	Minimal power used for transmitting packets in power-controlled manner
P_{thermal}	Average thermal noise
P_{MAI}	Maximum allowed interference tolerance
P_{RIT}	Remaining interference tolerance
P_{RP}	<i>Receiver-prohibition-signal</i> power level
P_{RP_min}	Minimal <i>receiver-prohibition-signal</i> threshold
P_{RP_CAI}	Power of the received <i>receiver-prohibiting-signals</i> on the transmitters
$P_{PH_T_Thre}$	Prohibition signal threshold on the receiver side
$P_{PH_R_Thre}$	Prohibition signal threshold on the transmitter side

CHAPTER 1

INTRODUCTION

1.1 Background

Over the past few decades, wireless ad hoc networks have rapidly grown to one of the most active fields in the wireless communication research. Especially with the fast development of the innovated technologies, the size of the wireless devices has been shrunk to be more portable. The cost of the wireless devices is continuously reduced but more advanced functions are applied to those portable inexpensive wireless devices. These factors push the ad hoc wireless network from concept to the reality, fuel the increased interests in the wireless ad hoc network, and lead to the proliferation of the current wireless communication.

Wireless ad hoc networks consist of a number of wireless nodes that can be rapidly deployed and communicate through low-cost short-range radio without relying on any established infrastructure such as base stations or access points (APs). Ad hoc nodes directly communicate with one another in a peer-to-peer fashion. To facilitate

communications between distant nodes, each ad hoc node also acts as a router, storing and forwarding packets on behalf of other nodes. The result is an infrastructureless wireless network that can be rapidly deployed and dynamically performed to provide on-demand networking solutions. Figure 1.1 illustrates a simple ad hoc network.

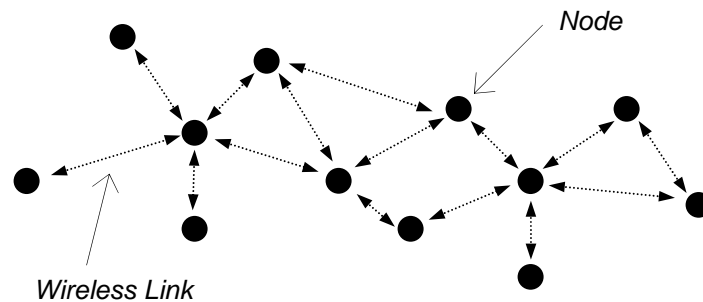


Figure 1.1 Ad hoc network architecture.

The main applications of the wireless ad hoc networks appear in places where the infrastructure networks are difficult to implement (e.g., conference meetings in the building, festival field grounds, battle fields, historic sites, and so on).

The MAC protocol is one of the keys which determine the performance of wireless ad hoc networks. The unique characteristics of the ad hoc wireless network make the design of a good MAC protocol very challenging. In addition to the lack of central control in ad hoc wireless networks, the challenges behind the fact are that the wireless communication channel in the ad hoc wireless network is inherently error prone and has limited channel bandwidth. These difficulties make it harder to design an efficient MAC protocol to share

limited spectrum resources, and dynamically adapt to the network traffic load, together with the simplicity of the mechanism and the desired performance.

1.2 Motivations and Objectives

In wireless ad hoc networks, nodes have to contend with each other for medium access. Kleinrock and Tobagi [3] identified the hidden-terminal problem of carrier sensing, which makes the CSMA protocol [2] perform very poorly as the senders of packets cannot hear one another. Figure 1.2 shows the hidden terminal scenario. Node A is transmitting to node B. Node C is out of the range of A, thus it can not sense the transmission from node A and wrongly concludes that the medium is idle. If Node C begins transmitting, it will interfere with the data reception at node B. The reason is that the damage-caused collisions happen at the side of the receiver (e.g. node B in Figure 1.2) instead of the transmitter (e.g. node C in Figure 1.2) and therefore, the carrier sensing employed by the transmitter cannot avoid collisions at the receiver side.

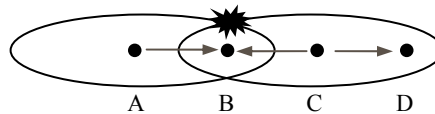


Figure 1.2 The hidden terminal problem

Another problem called exposed terminal problem may also occur when the CSMA scheme is used to allocate the channel to different nodes. As shown in Figure 1.3, node A is transmitting to node D. If node B senses the medium before attempting to transmit to

node C, it will falsely conclude that the medium is busy and hence it is unable to transmit at this time. However, since D is out of the range of B, B's transmission will not affect either D's reception or A's transmission. So the transmission of B is unnecessarily deferred by A when using CSMA to determine if it is available to access the channel. As a result, the achievable network throughput is reduced.

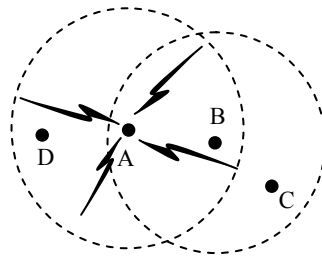


Figure 1.3 The exposed terminal problem

It is well known that the hidden terminal problem can introduce collisions and the exposed terminal problem may lead to low efficiency [4], thus both of them can severely degrade the performance of the ad hoc network.

Many approaches for attacking hidden/exposed terminal problems in the literature are based on the RTS/CTS mechanism, such as MACA [5], MACAW [4], and FAMA [6]. The most popular mechanism for the single-channel wireless MAC protocol, Carrier Sense Medium Access/ Collision Avoidance (CSMA/CA), becomes the basis of the MAC protocol for the IEEE 802.11 standard [7] [8]. However these RTS/CTS based protocols can neither successfully eliminate the hidden terminal problems nor deal with the exposed

terminal problems in the ad hoc environment. Moreover, as shown in [9], when the traffic load is heavy, the collisions of the data packets may also be caused by the loss of the RTS/CTS packets.

To alleviate above problems, the newly proposed MAC protocol named DPMA [45] makes use of the busy-tone like signals (i.e., dual prohibiting signals) to avoid collisions of RTS/CTS control messages. Also, DPMA implemented power control to increase the spatial reuse and reduce the interference to neighboring nodes, and thus significantly improve the network throughput.

In addition, the DPMA protocol takes the additive interference into account during the medium contention period to minimize the probability of the collisions caused by the additive interference.

Finally, with the increased demands on quality of service (QoS) applications in the wireless ad hoc networks, QoS provisioning is essential to the success of wireless ad hoc networks. Due to the unique feature of prohibiting signals, DiffServ can be easily implemented in DPMA.

In this thesis, we focus on performance evaluation on the DPMA protocol. By changing the system parameters, we observe the average throughput, packet delay, collision rate and blocking rate, to find out the effects of various factors such as binary competition number

(BCN), unit slot length and safe margin on the system performance when DPMA is employed. We also want to show through comprehensive simulations that by adjusting the system parameters to optimal values, DPMA can have better performance than the CSMA/CA MAC protocol in terms of higher system throughput, lower packet delay and lower collision rate in both low and high density network environment.

1.3 Thesis Outline

The remainder of the thesis is organized as follows. Chapter 2 overviews the related work on MAC protocols for wireless ad hoc networks. In Chapter 3, the main mechanisms of the collision-controlled MAC protocol – DPMA protocol are described in details. In Chapter 4, an event-driven simulator is developed to evaluate the performance of DPMA, and compare it with the CSMA/CA mechanism in terms of system throughput, end-to-end packet delay, and collision rate. Finally, Chapter 5 concludes the thesis and presents some future research directions.

CHAPTER 2

LITERATURE REVIEW ON MAC PROTOCOLS

Mobile ad hoc networks are gaining more and more popularity for various new applications. MAC protocols are responsible for coordinating the channel access to the shared communication medium so that it can be used efficiently. Various MAC schemes have been developed for wireless mobile ad hoc network and the problems they tried to tackle include contention/collision resolution, power control, signal interference, QoS, and etc. In this chapter, we will survey some important and typical works of previously proposed MAC protocols.

2.1 Single Channel MAC Protocols

2.1.1 IEEE 802.11

IEEE 802.11 is the most popular and widespread deployed standard for wireless local area networks. This standard specifies two modes of MAC protocols: distributed coordination function (DCF) mode (for ad hoc networks) and point coordination function (PCF) mode

(for centrally coordinated infrastructure-based networks). Since PCF is only applied for infrastructure-based network, we focus our study on the technical details of the DCF.

When DCF is employed, 802.11 networks use a CSMA/CA protocol for sharing the wireless medium. A combination of both physical and virtual carrier sense mechanisms enables the MAC protocol to determine whether the medium is busy or idle. The result of the physical channel sensing from the PHY layer is sent to the MAC layer as part of the information that decides the status of the channel. The virtual carrier sensing operation is based on MACAW [4].

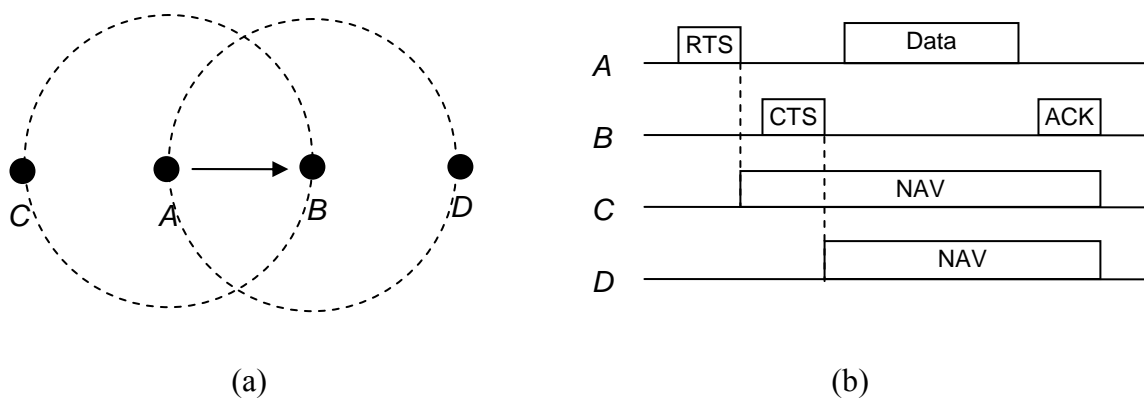


Figure 2.1 Virtual Carrier Sensing using CSMA/CA

As shown in Figure 2.1, node A has data packets to send to node B. Node C is a station within the range of A (and possibly within the range of B, but that does not matter). Node D is within the range of node B but not within the range of node A. First, Node A sends an RTS packet to node B in order to request the permission of transmitting data packets. Once

node B receives the RTS packet successfully, it will reply with a CTS packet if it is available to receive data. Upon receipt of the CTS reply, node A begins to transmit data packet and starts an Acknowledgement (ACK) timer. Upon the correct receipt of the data packet, node B responds with an ACK packet to terminate the dialogue. If node A's ACK timer expires before the ACK gets back to it, the whole procedure will run again. Now let us see how nodes C and D operate during this transmission process. Since node C is in the range of node A, after it hears the RTS packet sent by node A, it gets the information about node A intending use of the medium and places the information in its Network Allocation Vector (NAV) if the value is greater than the current NAV value. The NAV operates like a timer. After the NAV reaches zero, the station can transmit if the PHY coordination also indicates a clear channel. Node D does not hear the RTS, but it does hear the CTS, so it asserts the NAV for itself and defers from its transmission until node A finishes its data transmission.

The performance of the IEEE 802.11 MAC protocols in wireless ad hoc network has been investigated in [10] and [11]. It is observed that hidden and exposed terminal problems become worse in mobile ad hoc networks (MANET) while using IEEE 802.11 [10]. The ultimate results show the heavy degradation in throughput and instability of networks. In [11], it is shown that hidden and exposed terminal problems are more severe in large and dense wireless ad hoc networks.

2.1.2 IEEE 802.11e – QoS Extension of IEEE 802.11

IEEE 802.11 MAC protocols are very commercially successful and robust for best effort traffic, while they are unsuitable for multimedia applications (e.g., voice and video) with QoS requirements [12]. Without QoS support at the MAC layer, QoS support from higher layers is not possible. Therefore, QoS guarantee and provisioning at the contention-based wireless MAC layer is an important and challenging issue.

IEEE 802.11e [13] is the supplementary standard of 802.11 MAC to provide QoS for different types of applications. In 802.11e, QoS is supported with a new access method called the Hybrid Coordination Function (HCF). In HCF, two medium access mechanisms are defined: controlled channel access (Hybrid Coordination Channel Access - HCCA) and contention-based channel access (Enhanced Distributed Channel Access - EDCA). We omit the discussion of HCCA, since a centralized infrastructure is needed for its proper operation, which is not suitable for ad hoc mode. We describe the details of EDCA as follows.

The EDCA of 802.11e is an enhanced version of 802.11 DCF for priority-based QoS support. With EDCA, a station can implement up to four access categories (ACs), corresponding to voice, video, best effort, and background traffic, respectively. Each AC is associated with one backoff entity and some AC-specific parameters called the EDCA parameter set composed of Arbitrary Inter-Frame Space Number ($AIFS_N[AC]$), minimum contention window ($CW_{min}[AC]$), and maximum contention window ($CW_{max}[AC]$).

$AIFSN [AC]$ is used to determine the duration of Arbitrary IFS ($AIFS[AC]$) according to $AIFS[AC] = SIFS + AIFSN[AC] \times aslotTime$, where $AIFSN[AC] \geq 2$, and $aslotTime$ is the duration of one slot. Since the value of $AIFSN [AC]$ is at least 2, the earliest access time for an EDCA station is after a DIFS. The backoff entities are prioritized according to the values of their EDCA parameter sets. The smaller the $AIFS [AC]$ or $CWmin[AC]$, the higher priority in medium access, and thus, the higher throughput. The backoff interval for an AC in EDCA is randomly selected from $[1, CW]$, instead of $[0, CW-1]$ as in DCF.

The operation of 802.11e EDCA is described as follows. Each data frame from the higher layer arrives in the MAC layer with a specific priority value. Then, each frame is mapped into an AC based on the specified priority. The values of the EDCA parameter set for each AC are announced periodically by the AP via beacon frames. Each AC behaves as a single enhanced DCF contending entity, and the corresponding queue has its own AIFS, backoff interval, and contention window (CW). After each unsuccessful transmission attempt, the CW is doubled until a retry limit or the maximum CW is reached. The collision is handled in a virtual manner. That is, the highest priority frame among the colliding frames is chosen and transmitted, and the others perform a backoff with an enlarged CW value. Note that there is no priority among EDCA stations, different EDCA stations have to compete for channel access with equal opportunity.

IEEE 802.11e EDCA mechanism provides QoS differentiation by grouping traffic into ACs with different priorities. However, when the number of stations within an AC is

increased, the probability of two or more stations choosing the same backoff value leading to packet collision will be increased.

2.1.3 Power Control Medium Access

Power control is a critical research area of MAC protocols for mobile ad hoc networks because of the limited battery capacity of wireless devices and scarce radio resources. The goal of power control is to adjust transmitting power levels on wireless nodes to improve performance. There are two major benefits of power control: spatial reuse and energy saving.

- **Spatial Reuse:** Lower transmitting power leads to smaller interference. As a result, multiple concurrent transmissions may occur in the vicinity of each other. This increases the spatial reuse and leads to the increased capacity of the network.
- **Energy Saving:** By reducing the transmitting and receiving powers on wireless nodes, power consumption of the wireless nodes is reduced accordingly. Hence it is important to preserve energy and potentially extend the lifetime of an ad hoc network.

A lot of research has been performed to incorporate power control schemes into MAC protocols such as [14-18, 38]. As an example, we review the basic and typical power control MAC protocol named PCM proposed in [14].

In [14], the RTS and CTS packets are sent using the maximum transmit power level, whereas the data and ACK packets are sent with the minimum power required to

communicate between the sender and the desired receiver. An example scenario is depicted in Figure 2.2. Node D sends the RTS to node E at a maximum transmit power level (say, P_{\max}), and also includes this value in the packet. Node E measures the actual signal strength (say, P_r) of the received RTS packet. Based on P_{\max} , P_r and the noise level at its location, node E then computes the minimum necessary power level (say, P_{suff}) that would actually be sufficient for use by node D. Now, when node E replies with the CTS packet using the maximum power, it includes the value of P_{suff} that D subsequently uses for data transmission. Since Node G is able to hear this CTS packet, so it defers its own transmissions. Meanwhile, node E also includes the power level that it used for the transmission in the CTS packet, then node D follows a similar process and calculates the minimum required power level that would get a packet from node E to itself. It includes this value in the data packet so that node E can use it for sending the ACK. Note that the PCM also stipulates that the source node periodically increases the transmit power to the maximum power level, and also, the interval which the DATA is transmitted at P_{\max} should be long enough so that nodes in the carrier sensing range, such as node A, may sense it. Therefore nodes that can potentially interfere with the reception of ACK at the sender will periodically sense the channel as busy, and defer their own transmission. PCM thus achieves energy savings without causing throughput degradation. The operation of the PCM scheme requires a rather accurate estimation of received packet signal strength. Therefore, the dynamics of wireless signal propagation due to fading and shadowing effect may degrade its performance.

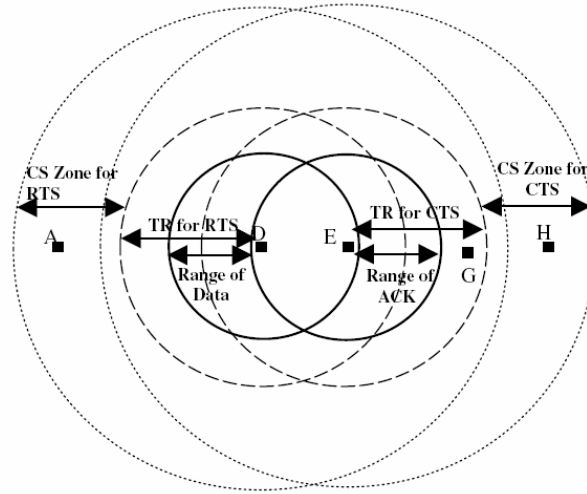


Figure 2.2 Power control example in PCM protocol.

Furthermore, in PCM, RTS and CTS packets are transmitted with maximum transmission power, which leads to low rate of spatial reuse and thus low system throughput. The reason is that the nodes within the range of senders or receivers are probably blocked by RTS or CTS packets unnecessarily. Another major problem with PCM protocol is the calculation of the required transmission power at senders and receivers. Only the distance factor is considered without taking into account the signal to noise ratio (SNR). The fact is that, if the value of SNR is below a certain limit, the signal of data packets can not be demodulated correctly which results in the failure of data packets reception.

2.2 Separate Channel MAC Protocols

The traditional RTS/CTS handshake mechanism usually operates with single frequency channel. Although such a direction of research on single channel is still dominant, the

recent technological advances in radio hardware for wireless networks have made available transceivers that can support two or more simultaneous channels. Moreover, the high collision rates for RTS/CTS dialogue mechanisms over a single channel also brought more attention to the research on multiple access by using multiple separate channels.

In this section, we investigate the previous works on using parallel independent frequency channels at the MAC layer. Those proposed schemes can be generally categorized into 3 approaches. Some of the multi-channel protocols dedicate one channel for the control packets and one separate channel for data packets [19, 20], thus the collisions between the data and the control messages are naturally avoided, packet delay is reduced, and the power consumption can be deducted. Those protocols can be further classified into separate channel without busy tone and separate channel with busy tone/busy-tone like signal. For the scheme without busy tone, only RTS/CTS handshake messages are exchanged in the dedicated control channel and the multiple channels are used for data packets transmissions [19]. It can potentially increase the throughput by assigning more channels for data transmissions, and significantly decrease collisions because parallel transmissions in different channels will not interfere with each other. However, it is hard to assign different channels to different nodes in real time. In the schemes with busy tone signals [3, 9, 21-25], the busy tone signal are transmitted in the control channel to notify the nearby nodes that an ongoing reception is in progress and thus the hidden/exposed terminal problems are solved or alleviated.

Another approach combining the power aware/power control mechanism with the separate channel technique [22, 23] is more focused on energy saving. The nearby nodes overhear the RTS/CTS messages can go into sleep mode to reduce the probability of collisions and increase energy efficiency. Power control can not only reduce the energy consumption, but improves the network throughput by increasing the channel spatial reuse.

Finally, there are lots of other approaches using separate channels studied in recent years. Such as using directional antennas in order to increase the spatial reuse and alleviate the hidden and exposed terminal problems. However, recent researches show that the new type of hidden/exposed terminal problems might be introduced by applying the directional antennas.

The following subsections provide a detailed description for some of the typical separate channel MAC schemes.

2.2.1 Separate Channel MAC without Busy Tone

As the number of nodes increases, the probability of the collision increases quickly with single channel implementation. Most of the collisions happen between RTS/CTS packets and the ongoing data transmission. There are many studies working on using separate channels for control and data packets [19, 20, 26].

Note that the mobile nodes assign data channels in “on demand” style. The simulation results indicate that the multi-channel MAC protocols outperform its single-channel counterpart. However, the hidden and exposed terminal problems can only be partially addressed, since the RTS/CTS-like dialogues are unable to solve hidden/exposed terminal problem completely in wireless ad hoc networks. Moreover, if all channels have the same bandwidth and the number of channels is small, one channel dedicated for control messages can be costly.

2.2.2 Separate Channel MAC with Busy Tone

In the above section, the approach using separate channel without busy tone is still RTS/CTS handshake based. The above approach can increase the throughput by utilizing one or more dedicated channels for data transmission simultaneously. Meanwhile data and control packets are separately transmitted in the independent dedicated channels, thus the overall collisions are greatly reduced by eliminating the interference between the data packets and control packets. However, when the propagation and transmission delays are long, the collisions between RTS/CTS packets will increase dramatically. This will result in the destruction of data packets especially when the traffic load is heavy. Consider the example shown in Figure 2.4.

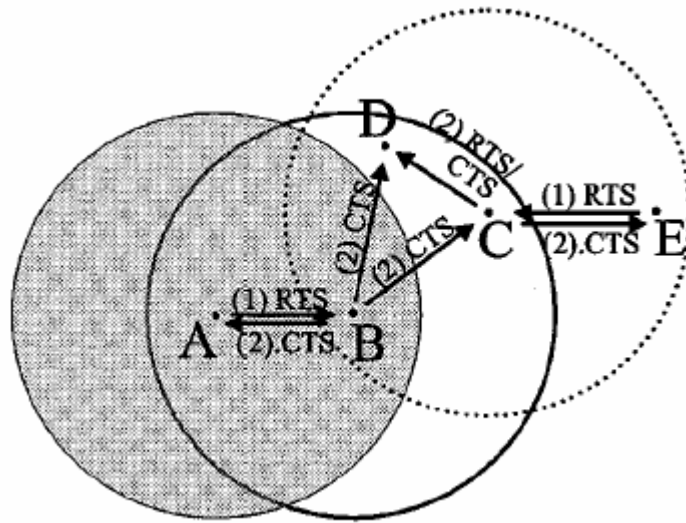


Figure 2.4 A scenario that B's CTS is destroyed at D by C's RTS/CTS.

In Figure 2.4, Node A sends an RTS to node B. Node B replies to node A with a CTS. Meanwhile, as node C cannot hear node A's RTS, it may send an RTS to start a data transmission with node D or a CTS to respond to node E's RTS. In either case, D can hear neither node C nor node B's RTS/CTS, but the data transmission from A and B will continue as normal. If later node D decides to send any packet while node A is transmitting to node B, the packet will be collided at node B.

To solve this problem, another scheme [3, 9, 21, 25] using a special signal called busy tone, to prevent the potential data collisions caused by the unawareness of the RTS/CTS dialogues. The scheme also employs two separate channels: one for the data channel, the other for the control channel, which is still RTS/CTS dialogues\ based. In addition, one or more narrow-band busy tone signals, which work on different frequency spectrums, are

applied to add the similar capability as the carrier sensing. By utilizing this early-warning mechanism, the scheme with busy tones may realize the collision free [9].

There are many schemes based on busy tones in the literature. BTMA [3] is the first protocol that proposed the idea about utilizing an additional channel transmitting the busy tone signal, in order to address the hidden terminal problem. When a base station senses a busy data channel, it broadcasts a busy tone signal over the busy tone channel to prevent the hidden neighboring terminals from accessing the channel. The BTMA was designed for a centralized network infrastructure, which is not applicable in mobile ad hoc networks. Even though the BTMA can be extended for packet radio networks by having all the nodes within the range of the sender turn on busy tone, it makes the exposed terminal problem worse since the potential concurrent transmission is blocked within the double radius of the sender. As a modification to BTMA, a receiver-initiated busy-tone multiple access (RI-BTMA) protocol has been proposed [27]. In this scheme, only the receiver generates the busy tone if it senses the channel to be idle and successfully receives the preamble including the receiver's address from the transmitter. Once the transmitter hears the busy tone, it knows that the receiver is ready to receive. IT then transmits data packets in the dedicated data channel. Otherwise, the sender reschedules another try in the next reserved slot. As shown in the paper [27], it can achieve data packets collision free, and improve the efficiency of the network resource by employing only one busy tone. However, the preambles may still suffer the collisions.

Building upon the earlier work of the BTMA and RI-BTMA, Hass et al. [9] introduces dual busy tone multiple access (DBTMA), and several revisions of the DBTMA [27]. DBTMA employs two independent separate channels, a narrow-band channel for control packages and a data channel for data packets. Meanwhile, the transmit busy tone (BT_t) and the receive busy tone (BT_r) are used to protect the transmission of the RTS packet and data packets. Those two narrow-band busy tones are placed on the spectrum at different frequencies with enough separation, as shown in Figure 2.5.

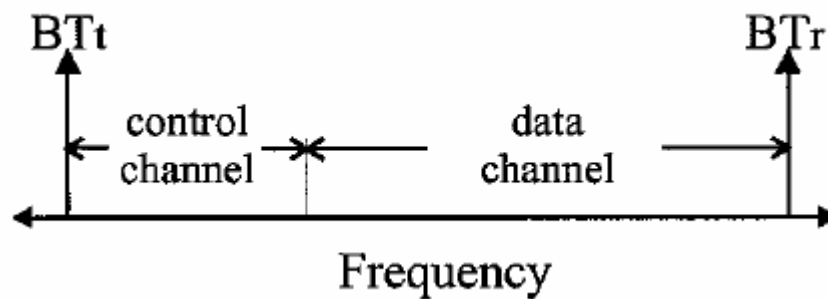


Figure 2.5 DBTMA frequency chart

As the transmitter is ready for transmitting data to the intended receiver, it senses the busy tone in the control channel first. If no BT_r is heard, which means the intended receiver is not currently receiving from any hidden station, the sender transmits a RTS packet to the intended receiver over the control channel. Once the receiver has received this RTS packet, it keeps sensing the BT_t in order to ensure that no other nearby ongoing data transmission will interfere with the forthcoming data packet reception. If no busy tone (BT_t) is sensed, the receiver replies with a CTS packet. Meanwhile, it turns on busy tone BT_r to prevent the hidden terminals from transmission until the whole data packet transmission is completed.

Upon receiving the CTS packet from the intended receiver correctly, the senders start sending the data packets and turn on the busy tone (BT_t) to avoid the exposed terminals from transmission until the data packet is completely received.

In summary, the operation of DBTMA is simply described as follows. A host should not send if it hears any BT_r and should not intend to send if it hears any BT_t . With the aid of the BT_t and the BT_r , DBTMA is able to handle the hidden/exposed terminal problems. By separating the data channel from the control channel, the collisions between the control and data packets are avoided. Moreover, in comparison with RI-BTMA, DBTMA provides extra protection for the RTS packet with the help of the BT_t . As shown in [9], the performance gain of DBTMA over RI-BTMA is about 20%. However, DBTMA scheme and its revised versions are still based on the exchange of RTS/CTS dialogues. Since control packets themselves are prone to collisions, CTS packet collisions will cause the collision of the data packet inevitably.

2.2.3 Separate Channel with Power Control

To further improve the performance of the mobile ad hoc network, the power aware/power control mechanism is integrated into the separate channel scheme [22, 23, 28]. With the benefit of employing power aware/ power control, more concurrent transmissions in the neighboring nodes are enabled and the network throughput can be improved consequently.

Power aware multiple access with signaling (PAMAS) [29] is developed from the MACA protocol [5]. It uses separate channels for RTS/CTS control packets and data packets. The RTS/CTS handshake is applied in the control channel. In addition, PAMAS includes the duration of the upcoming transmission in both RTS and CTS packets. Therefore, the nearby nodes overhearing RTS/CTS packets should turn off their power for the duration of the forthcoming transmission, which can be obtained from the received RTS/CTS packet. The results of simulation and analysis [29] show that around 10% to 70% power saving can be achieved. However the scheme is designed mainly for power saving. Collisions can still occur between probe messages or RTS/CTS packets, and thus the collisions might be the main wastage of the energy.

Dynamic channel assignment with power control (DCA-PC) [30] is an extension of DCA [31] protocol. DCA-PC combines the concepts of power control, channel assignment, and multiple channel medium access. It has one control and N data channels. The control packets are exchanged over the control channel with the maximum power. Based upon the exchanged control messages (RTS/CTS/RES), each node keeps updating a table of power level used to transmit to the intended nodes and maintains the list of the free channels. Therefore, the sender can choose an appropriate free data channel dynamically, and transmit the data with a power level appropriate to reach the receiver. It has been shown that DCA-PC can achieve higher throughput than DCA. However, the additional control packet (RES) will not only increase the total overhead of the control messages, but the collisions among RTS/CTS/RES packets themselves will happen with higher probability.

This will greatly degrade the network performance especially when the traffic load is heavy.

Another power control based protocol with busy tones was proposed in [23]. The idea is to combine the mechanisms of power control, RTS/CTS dialogue, and busy tones. In [23], the sender transmits data packets and BT_t with the minimum power, while the RTS packet is transmitted at the power level determined by the received highest level of the surrounding BT_r . Hence, the RTS signal should not go over the nearest nodes that are receiving data packets. If the RTS packet can be successfully received by the intended receiver, the receiver replies with CTS and sets up BT_r at the maximum power. The nearby nodes calculate the channel gain based upon the strength of the received busy tone. Finally, the power level of the data packets and BT_t is estimated by the following equation:

$$P_x = \frac{P_{\min} P_{\max}}{P_r} \quad (2.1)$$

Where P_r is the level of the power at which the sender receives the CTS packet. The above algorithm is to ensure that the yet-to-be-transmitted data packet will not corrupt the ongoing receptions. However the algorithm in this protocol does not take into account the changes of the interferences caused by the new joined transmissions. Consequently, the collisions might happen in the future transmission and the performance might get worse.

2.2.4 Other Separate Channel MAC Protocols

The MAC protocols stated above all assume the usage of the omni-directional antennas. In the recent years, another interesting approach [32] is proposed, which utilizes the directional antenna as an alternative means to increase the effectiveness of spatial reuse. In [32], DBTMA/DA is proposed as the extension of DBTMA [9] by adding the feature of transmitting the busy tones with directional antennas. Similar to DBTMA, in DBTMA/DA, separate channels are used for the transmission of the control and data packets, busy tones are transmitted directionally. By using the directionally transmitted BT_r , the exposed terminal problem is alleviated, and the network capacity is increased. In the mean time, the directional BT_r allows the nodes to transmit in the directions to avoid collisions with the ongoing transmission. In [32], DBTMA/DA was shown to have much better performance, in terms of throughput and end-to-end delay, than IEEE802.11 MAC.

However, the tradeoff of using directional busy tone (BT_r) is illustrated in Figure 2.6 [32].

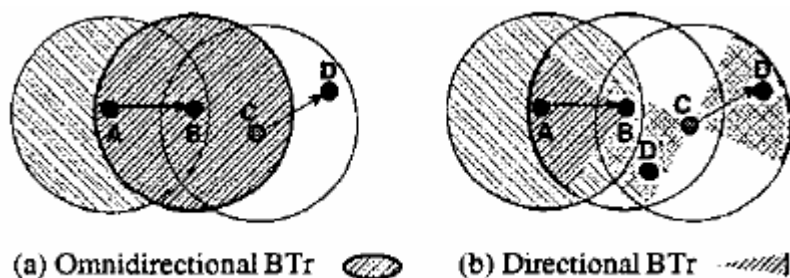


Figure 2.6 Tradeoff of using directional BTr

As shown in Figure 2.6, when directional BT_r is turned on during the data transmission from node A to node B, node C can not hear node B's BT_r . Therefore, node C is allowed to transmit RTS and data packets to node D, which could collide with the ongoing transmission between node A and node B. This is defined as the new hidden terminal problem. Moreover, the use of the directional busy tones brings not only the new hidden terminal problem, but the new exposed terminal problem and the deafness problem as well [33].

2.3 Summary

Some of the reported MAC protocols have been reviewed in this chapter. The aim is to give an overview of these important channel access mechanisms that are closely related to the research work in this thesis. We divided these MAC protocols into two categories: single-channel MAC and multi-channel MAC. In the single-channel category, we first reviewed the MAC schemes in the most deployed standard IEEE 802.11 and its QoS enhancement. Then we introduced the power control mechanism in the PCM protocol. From the study of this protocol, we can see that power control is very useful for saving energy and increasing the spatial reuse in mobile ad hoc network. For multi-channel category, we investigated in detail the busy tone mechanism in several protocols such as DBTMA, DCBMA, BTMA and DBTMA-DA. Through the study of these protocols, we found using busy tones can efficiently deal with exposed/hidden terminal problems in ad hoc network. Again, power control mechanisms for multi-channel MAC protocols such as PAMAS and DCA-PC are also studied. From insight into previous MAC protocols, we

found that the schemes in these protocols for collision-control and QoS provisioning are not efficient enough and still have much room to improve.

As we mentioned before that high collision rate is the main factor that degrades the performance of the single channel MAC schemes significantly with the number of mobile stations increasing. Hence the new MAC schemes, which have the independent dedicated channel for transmitting the data and control packets individually, are proposed to avoid the most collisions between those control and data packets. Meanwhile, by integrating the other novel and interesting techniques (such as power aware/ power control, busy tone/busy-tone like signal, directional antennas, etc.), the separate channel MAC scheme can further expand the capacity of the network, increase the effectiveness of the channel utilization, and improve the aggregate throughput.

For example, with the aid of busy tones, the new scheme [9] can provide additional protection for data and control packets, and solve the hidden/exposed terminal problem. It can also be extended to the wireless sensor networks. Antonio proposed DCMA/AP [34] as an example to apply dual channel with busy tones for wireless sensor networks. Another option is to apply one control and N data channels, and dynamically assign the channels for the concurrent data transmissions, to improve the network capacity and increase the channel reuse. Also, by introducing the sleep mode, the power-aware MAC schemes [29] focus on power saving and maximizing the battery life of the portable devices. The power

control based MAC schemes [23] are able to greatly improve the network capacity via limiting the transmission power and reducing the interference range.

However, the separate channel protocols stated above are still mostly based on the RTS/CTS dialogues to reserve the use of the channels for data packets transmission. Furthermore, the control overheads caused by those RTS/CTS like control packets will increase with the number of nodes increasing. Therefore, in the collision prone ad hoc network environment, the collisions caused by control packets are unavoidable, and considerably degrade the performance of the network and waste the network resources.

CHAPTER 3

THE DUAL PROHIBITION MULTIPLE ACCESS (DPMA) SCHEME

With the continuously increasing needs for the applications in wireless ad hoc networks, high collision rate in medium access becomes one of the important factors that molests various wireless applications to further extend themselves into diverse fields of the real world. In wireless ad hoc networks, central control is unavailable and nodes have to contend to access the channel in a distributed manner. The single-channel MAC protocols using RTS/CTS dialogues cannot deal with the hidden and exposed terminal problems very well, which leads to unavoidable collisions of data and control messages, especially under heavy traffic load. In [45], instead of employing conventional RTS/CTS dialogues, Yeh proposed the dual prohibition multiple access (DPMA) scheme, which applies power-controlled binary countdown dual prohibition mechanism as the core technique to solve some problems with previous RTS/CTS mechanisms. Meanwhile, DPMA is also able to control packet collision rates for data messages, and increase wireless network spatial utilization.

This chapter is organized as follows. In Section 3.1, we give a brief overview to DPMA. Section 3.2, main mechanisms of a synchronized DPMA protocol are described in more detail, and several advantages of DPMA are pointed out. Finally, Section 3.3 summarizes this chapter.

3.1 Protocol Overview

Medium access contention is one of the main challenges in wireless networks without central control. DPMA can be globally synchronized, locally synchronized, or asynchronous. In what follows, we describe a synchronized version of DPMA for simplicity. Two channels are used for the transmissions of control signals and data packets, respectively. The control channel is slotted for dual prohibition. The nodes with data packets to be transmitted compete with each other using dual prohibiting signals, which are busy-tone like signals (see details in Section 3.2.1), in the control channel. The advantage of the prohibiting signals is that those signals do not suffer from collisions. By employing binary countdown dual prohibition mechanism, collisions of data packets can be prevented or reduced. In addition, the additive interference control mechanism (see details in Section 3.2.2) is applied to reduce the collisions caused by the additive interference from the simultaneous data packet transmissions, and thus be able to support parallel data transmissions over the data channel. Furthermore, by combining with the power control mechanism, DPMA is able to increase the number of concurrent transmissions as long as those transmissions do not interfere with each other. Different from the power control

mechanism in the previous dual channel MAC protocols [1, 22, 23], receivers compute the power level of the prohibiting signals based on their remaining interference tolerance (RIT). In this way, the neighboring intended transmitters are able to calculate the maximum allowed transmission power (MAP) based on the received prohibiting signal strength to avoid colliding the packet reception at the receiver.

Finally, efficient differentiated services (DiffServ) with fairness (see Section 3.2.4) are supported in the DPMA protocol. Specifically, the DiffServ and fairness are realized through binary competition numbers (BCNs). Here, the BCN is composed of three parts, i.e., the priority number part, the random number part, and the station ID part. During the prohibition stage, transmitters are prohibited by nearby receivers with higher BCN and receivers are prohibited by transmitters with higher BCN through their prohibiting signals. Meanwhile, the random number part following the priority number part is useful for the data channel to be fairly shared by all the mobile nodes and the starvation problem is solved.

3.2 DPMA Protocol Description

Several key techniques and mechanisms are utilized in the synchronized DPMA protocol to reduce collision rates, increase system throughput and channel utilization, and provide QoS capability. We describe each of them in detail in the following sections.

3.2.1 Binary Countdown Dual Prohibition

First of all, for better understanding the operation of the dual prohibition mechanism in DPMA, we start by depicting the time diagram of slot assignment for the control channel.

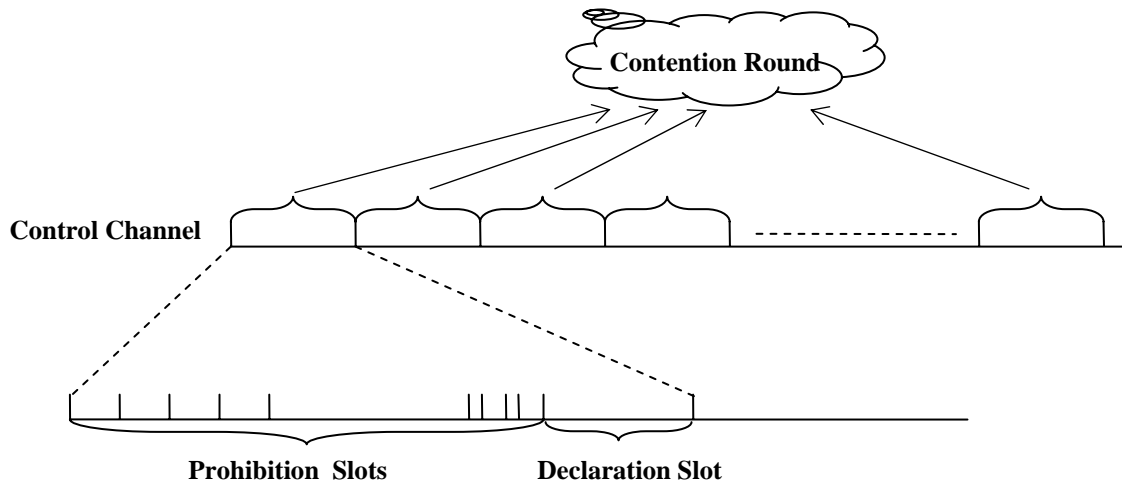


Figure 3.1 The time diagram of the control channel in DPMA

As shown in Figure 3.1, in the control channel, the time axis is partitioned into “contention round” of equal length of. Each “contention round” starts with the prohibition slots followed by a declaration slot. The “contention round” is used for resolving the access contention among mobile stations. At first, the competing nodes which have data packets to transmit begin to compete with each other in the prohibition slots. By applying the binary countdown contention mechanism, the competitors send the prohibiting signals according to their individual BCN. The nodes with lower BCN are prohibited by the competing nodes with higher BCN. The winners of the binary countdown competition will

transmit declaration messages in the declaration slot and then begin their data transmissions in the data channel right after the “contention round”.

In the following, we present an example for implementing the binary countdown dual prohibition mechanism in DPMA.

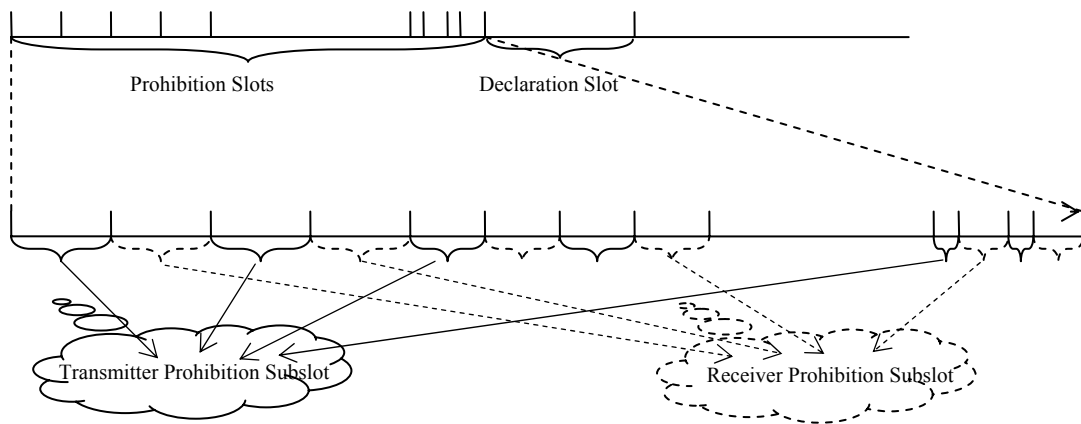


Figure 3.2 The slot assignment for prohibition slots in DPMA

As shown in Figure 3.2, the transmitter prohibition subslots and receiver prohibition subslots are interwoven in the contention round. Transmitters and receivers send their prohibiting signals in the transmitter prohibition subslots and the receiver prohibition subslots, respectively. Also, transmitters or receivers send prohibiting signals based on the corresponding BCNs which are k -bit binary numbers. Note that, a competing transmitter senses the status of all receiver prohibition subslots, but does not sense any transmitter prohibition subslot; while a competing receiver senses status of all transmitter prohibition subslots, but does not sense any receiver prohibition subslot.

In the transmitter prohibition subslot, the competing transmitters whose current bit of its BCN is “1” send prohibiting signals at an appropriate power level. The competing transmitters whose current bit of its BCN is “0” keep silent. All competing receivers sense whether there is any prohibiting signal during this slot. The receiver whose current bit of its BCN is “0” and receives a power level above the threshold $T1$ loses the competition. The receiver whose current bit of its BCN is “0” and receives a power level below the threshold $T1$ survives. The receiver whose current bit of its BCN is “1” and receives a power level below the threshold $T2$ loses the competition. Otherwise it survives. The calculations of $T1$ and $T2$ are as follows:

$$T1 = P_{RIT} \quad (3.1)$$

P_{RIT} is the receiver’s remaining tolerance of data interference.

$$T2 = P_{Min} \quad (3.2)$$

P_{Min} is the minimum received signal power for the receiver to correctly decode data packets.

Similarly, in the receiver prohibition subslot, the competing receivers whose current bit of its BCN is “1” send prohibiting signals at an appropriate power level. The competing receivers whose current bit of its BCN is “0” keep silent. All competing transmitters sense whether there is any prohibiting signal during this slot. The transmitter whose current bit of its BCN is “0” and receives a power level indicating that its intended transmission will collide with the corresponding receiver’s data reception loses the competition. The transmitter whose current bit of its BCN is “0” and receives a power level indicating that

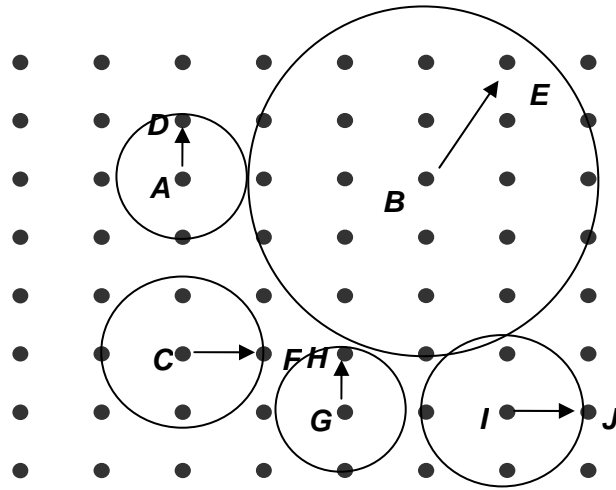
its intended transmission will not collide with any corresponding receiver's data reception survives and continue with the competition. The transmitter whose current bit of its BCN is "1" and receives a power level below the expected power level of its own receiver's prohibiting signal loses the competition. Otherwise it survives and continues with the competition.

If a mobile station survives all k bit-slots, it becomes a candidate for transmitting or receiving and will send declaration signal in the declaration slot. In the declaration slot, if a transmitter or receiver detects the declaration signal of its partner successfully, it becomes the winner of the competition and will be able to transmit or receive data packets in the data channel. Otherwise, it loses the competition.

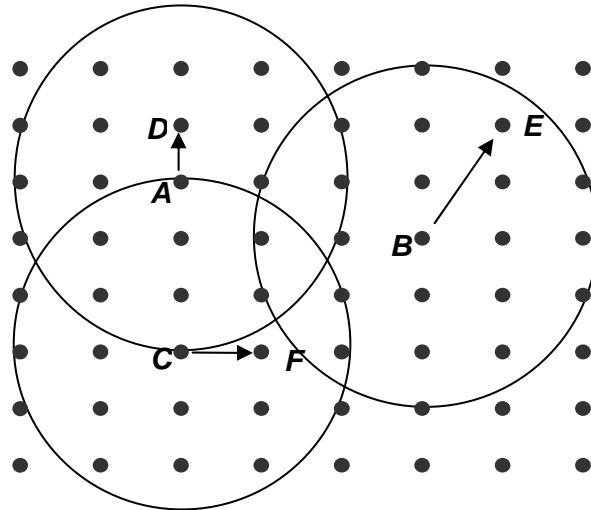
3.2.2 Power Control

In DPMA, the power control mechanism is implemented by controlling the power level of the prohibiting signal, declaring signal and the data packet signal during the contention round/data transmission period. Note that an on-going transmission could cause significant interference to its neighboring nodes. Therefore, by cooperating the power control mechanism with the dual prohibition mechanism in DPMA, a larger number of simultaneous transmissions may be permitted. As a result, the channel spatial utilization can be maximized and the network throughput is improved significantly. In addition, it also leads to energy efficiency. From the example scenarios shown in Fig. 3.3, we can obviously see that when nodes A, B, C, G, and I are transmitting to nodes D, E, F, H and J,

respectively, the number of blocked mobile nodes for the case of using power control is considerably reduced compared to the case of using fixed transmission power. Consequently, the former can produce higher throughput than the latter.



Scenario of transmission with power control



Scenario of transmission with fixed power

Figure 3.3 Comparison of power control and fixed transmission power.

3.2.3 Additive Interference Avoidance

Through the additive interference avoidance mechanism, unnecessary prohibitions by nearby competing mobile stations can be avoided.

First of all, the controlled power level of both the transmitter/receiver prohibiting signal and the transmitter/receiver declaration signal should be set properly by applying the additive interference avoidance mechanism. The time diagram for those prohibiting signals is illustrated in Figure 3.4.

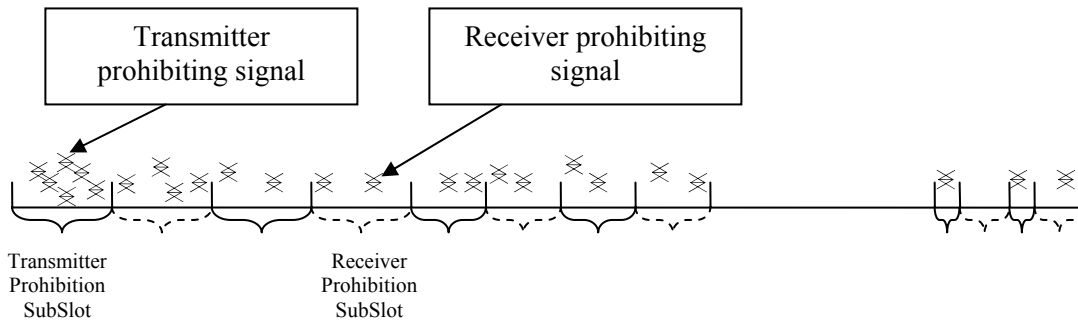


Figure 3.4 Time diagram of prohibiting signals.

Step 1:

During the transmitter prohibition subslot, all survival competing transmitters which have bit “1” of their BCN send prohibition signals at the power level related to the associated data packet transmission, which can be computed by the following equation:

$$P_{TP} = P_{Min} \times d^\alpha \quad (3.3)$$

Here we assume free space simulation model is used, where α is 2. However, in the real environment, because of pathloss, fading and shadowing factors, α will be larger than 2. P_{TP} denotes the transmission power of the transmitter. d is the distance between the transmitter and the intended receiver. P_{Min} is the minimum received signal power for the receiver to correctly decode data packets.

On the receiver side, those competing receivers measure the strength of the received additive prohibiting signal during the transmitter prohibition subslot. If the competing receiver is supposed to receive a signal with bit “0”, the prohibition signal threshold on the receiver side $T1$ should be computed using equation (3.1)

If the competing receiver is supposed to receive a prohibiting signal with bit “1” and the measured prohibiting signal strength is above the prohibition signal threshold $T2$ (see equation (3.2)), which means the receiver correctly receive the “matched” bit from the active corresponding transmitter, the competing receiver survives and remains in the competition. Otherwise, the competing receiver loses the competition and keeps silent for the rest of the “contention round”.

Step 2:

During the receiver prohibition subslot, the survival competing receivers with bit “1” at the corresponding bit of its BCN transmit the *receiver-prohibition-signal* with controlled

power level (P_{RP}). P_{RP} can be computed based on the measured additive *transmitter-prohibiting-signal* during the previous transmitter prohibition subslot, as shown in the following equation:

$$P_{RP} = \frac{1}{P_{RIT}} \quad (3.4)$$

P_{RIT} is the receiver's remaining tolerance of data interference.

At the same time, on the transmitter side, if the competing transmitter is supposed to receive prohibiting signal with bit "1" and the received signal power is above P_{RP} / d^2 (d is distance from the transmitter to its receiver), then the transmitter considers itself to have correctly received the "matched" bit from the its corresponding receiver. It survives. Otherwise, the transmitter loses the competition.

If the competing transmitter is supposed to receive prohibiting signal with bit "0", and its P_{TP} is less than P_{MAP} (which is the maximum allowed transmission power), it survives the competition. Otherwise it loses it because its transmission will probably collide the data reception of nearby receiver(s) with higher BCN.

Step 3:

In the declaration slot, the winning transmitters and receivers send declaring signals to inform their partners about their current status. If both sides of the transmitter/receiver pair are successful in the competition, this transmitter/receiver pair will be able to transmit in

the following transmission phase. Another important function of the declaring signals is to update the database of surrounding nodes. Particularly, the nodes in the range of the intended transmitters will update the total data interference they received, and the nodes in the range of the intended receivers will update their maximum allowed transmission power. After declaration, the winning competitors begin to transmit data packets in the data channel without causing data collisions to neighboring receivers.

3.2.4 Support for DiffServ and Fairness

As we stated in Section 3.1, a BCN consists of three parts: priority number part, random number part, and station ID part. The ID should be unique or be unique with high probability to reduce the collision rate. For the nodes with the same priority, nodes with higher station ID number will always prohibit nodes with lower station ID number, which results in unfair medium access. To eliminate this problem, we add a random number part before the station ID part. The random number part is selected randomly every time when we assign the BCN to the mobile station. In this way, DPMA achieves fairness among all the mobile stations. In the following, we explain these two mechanisms in detail.

Assuming there are four competing pairs (A, B, C, and D) with one of four priorities from the highest priority to the lowest priority and assigned a 2-bit binary priority number, i.e., 11, 10, 01 and 00, respectively (see Figure 3.5). They are located in the prohibiting signal range of each other, and are competing for the medium access. For the first bit, the competing pair A and B sends prohibiting signal of bit “1”. If the competing pairs C, and D

sense the channel and hear the prohibiting signal, they will quit at once. Therefore, the competing pairs C and D with lower priority are killed in the competition. Competing pair A and B win and continue to send prohibiting signal of bit “1” for A and bit “0” for B. Competing B is killed in this round and A with the highest priority wins the whole competition and gets the right to send its data packets. In this way, differentiated services are provided for mobile stations with different priorities.

Bit Number of BCN

A	1	1	0	1	0	0	0	0	1
B	1	0	0	0	1	0	0	1	0
C	0	1	1	0	1	0	1	0	0
D	0	0	0	0	1	1	0	1	0
	Priority Number		Random Number			Station ID number			

Figure 3.5 Example of DiffServ and fairness in DPMA

However, we can notice that, for different mobile stations with the same priority, higher station ID will always win the competition, which results in unfairness during the medium access process. The solution to this problem is to randomly assign a random number to each mobile station and put this random number part before the station ID part in the BCN. In this way, different mobile stations with the same priority will have the same chance to win the competition and get the right to send data packets. Please note that if two nodes obtain the same BCN by accidentally and their receivers are within each other's

transmission range, they will both win the competition and collisions could happen during data transmission.

3.2.5 Advantages of DPMA Protocol

- **Solving hidden/exposed terminal problems**

One advantage of the DPMA protocol is that it solves hidden/exposed terminal problems without relying on collision-prone RTS/CTS messages. With RTS/CTS handshake mechanism, intended transmitters and receivers block neighboring nodes by exchanging RTS/CTS control messages. However, in DPMA, the intended transmitters and receivers compete with neighboring nodes through prohibiting signals which do not suffer from collisions and at the same time, collided transmissions of data packets can usually be prevented by the competitions. As a result, several problems of IEEE802.11 and other RTS/CTS-based protocols can be avoided naturally.

- **Increasing spatial reuse**

The power control mechanism can easily cooperate with the dual prohibition mechanism by applying the appropriate transmission power levels for the data transmission in the data channel and the prohibiting/declaring signal in the control channel. This results in smaller prohibitive ranges as well as smaller coverage ranges for data packets, as compared to IEEE 802.11 RTS/CTS handshake mechanism. Therefore, it can allow more concurrent

transmissions within the same area/region, which improves the special reuse and reduces the energy consumption.

When both power control and additive interference control mechanisms are employed in DPMA, the special reuse can be increased, which leads to optimal network performance and efficient energy consumption.

- **Provisioning QoS and Fairness**

By simply utilizing the priority number part of the BCN in the dual prohibition mechanism during the competition period, DPMA is able to provision quality of service (QoS) during medium access control in wireless ad hoc networks.

During prioritized data transmissions, it is possible that a node occupies the channel for a long time and starves the other nodes with the same priority from accessing the medium, which is called the starvation problem. This problem can cause severe unfairness among nodes with the same priority. However, in DPMA, by inserting the random number part between the priority number part and station ID part, the nodes with the same priority are randomly assigned with different random numbers. In this way fairness is achieved among nodes with the same priority number. At the same time, DiffServ is still maintained.

3.3 Summary

In this chapter, the operation of DPMA protocol is described. Instead of employing the traditional RTS/CTS dialogue, binary countdown dual prohibition is applied as the core and powerful technique to solve the inherited problems from RTS/CTS mechanisms, such as hidden/exposed terminal problems. DPMA also supports power control and interference control, which can lead to considerably better spatial reuse and energy efficiency.

CHAPTER 4

PERFORMANCE EVALUATION

In this chapter, we conduct comprehensive simulations to investigate various factors on the performance of the DPMA protocol, such as the binary competition number (BCN), the unit slot length and the effect of the safe margin. We also test the DiffServ capability of DPMA. Finally, DPMA is compared to CSMA/CA in terms of system throughput, end-to-end packet delay, collision rate and blocking rate.

An event-driven simulator is developed using C programming language, which provides a good platform to observe and evaluate the performance of the DPMA protocol.

4.1 Simulation Model

4.1.1 Experimental Setting

The simulation is implemented using the following assumptions:

- All the nodes are randomly distributed within the 30 * 30 unit grid simulation field.
Two independent random number generators are used to generate the location for each

node, i.e., one for x axis and the other for y axis. The number of nodes varies from 90 to 180 to observe the effects of different densities on the evaluated protocols. That is to say, mobile stations (MSs) are distributed randomly with density D throughout the network area during the simulation initiation process. The density D is defined as the average number of MSs in the maximum transmission range of a mobile station. We assume that the MSs are stationary throughout the simulation.

- Each MS is a Poisson source with a data packet arrival rate. The total traffic load is the aggregate of the arrival rates of the MSs in the network. For each packet, a destination is selected from the set of possible neighbors of that mobile station.
- There are four queues of different priorities at each MS. The packet arrival rate of each queue is the same. The mean aggregated packet arrival rate λ is the sum of the arrival rates of the four queues.

In our simulation experiments, each node has the same maximum transmission power, which is set to 10 mw. The data channel capacity is set to 54 Mbps for both DPMA and CSMA/CA. We assume data packets have fixed length of 2K Bytes. The parameter settings are shown in Table 4.1.

SIMULATION PARAMETERS

Parameter	Nominal Value
Simulation area	30 *30-unit grid
Maximum data transmission power	10 mW
Maximum data transmission range	10-unit grid
Number of nodes	90 / 180
Data packet size	2K bytes
Packet arrival rate (λ)	10, 50, 100, ... packet/sec
Channel bandwidth(Data/Control)	54Mbps/1Mbps
Minimum SNR	4
A unit slot time	1 μs

Table 4.1 Simulation parameters setting

4.1.2 Performance Metric

The major performance metrics we used in our simulation are as follows:

- 1) Average system throughput: average number of successfully received data packets per node per time unit.

$$\text{Average system throughput} = \frac{\text{Total \# of data packets received successfully}}{\text{Total simulation time} * \text{Total \# of nodes}}$$

- 2) Average data packet delay: average end-to-end delay of data packets successfully sent from senders to receivers.

$$\text{Average data packet delay} = \frac{\text{Total delay for all successfully received data packets}}{\text{Total \# of data packets received successfully}}$$

3) Collision rate: portion of data packets which are collided.

$$\text{Collision rate} = \frac{\text{Total \# of collided packets}}{\text{Total \# of packets sent}}$$

4) Blocking rate: portion of data packets which are blocked from transmission.

$$\text{Blocking rate} = \frac{\text{\# of arrived packets} - \text{\# of successfully received packets}}{\text{\# of arrived packets}}$$

5) Density (D): average number of nodes in the node maximum transmission range.

$$D = \text{Total \# of nodes} / \frac{\text{grid size}^2}{\text{transmission_range}^2}$$

4.2 Discussions on Simulation Results

4.2.1 Effect of Binary Competition Number (BCN)

In this section, we show through experiments how the binary competition number (BCN) set in DPMA affects the system performance. Also, we simulate the system employing the CSMA/CA protocol with the same parameter settings (i.e., network density, packet arrival

rate) and obtain the results shown in the same figures (Fig. 4.1 - Fig. 4.7) as DPMA. Note that, “ID 2-3-4” means 2 bits for the priority number part, 3 bits for the random number part, 4 bits for the station ID part. The network density D is 10. The unit slot length is equal to $0.1 \mu s$. We change the number of bits for each part to compare the performance. We found that for all cases, at low traffic load ($\lambda \leq 80$ packets/sec), the achieved network throughput is almost the same as the offered traffic load (Figure 4.1). As the traffic load increases, the throughput continues to increase until reaching the maximum throughput. It can be seen that using shorter ID length can achieve higher network throughput than using longer ID length. The reason is that the overhead for access contention is smaller when shorter ID length used. We also found that the collision rate for the case of shorter ID length is higher than the case of longer ID length (Figure 4.3). It is because that, the shorter the ID length, the higher probability of ID overlapping, which could result in more collisions among the competing pairs in vicinity. Nevertheless, the benefit of smaller control overhead still leads to higher throughput in spite of higher collision rate. Figure 4.2 shows that using shorter ID length results in smaller average delay. This is also due to the fact that the overhead for access contention is smaller when shorter ID length used and therefore packets wait for shorter time before being transmitted. Figure 4.4 shows the results of blocking rate for DPMA with different BCNs and CSMA/CA. We can see that the blocking rates for DPMA with different BCNs are similar, but CSMA/CA has much higher blocking rate than DPMA in all cases. Furthermore, we can see from Figure 4.1 – Figure 4.3 that DPMA achieves better network performance than CSMA/CA in terms of higher throughput, lower average delay and collision rate. We will conduct comprehensive

simulations and discuss more on the performance comparison between DPMA and CSMA/CA protocols in section 4.2.5.

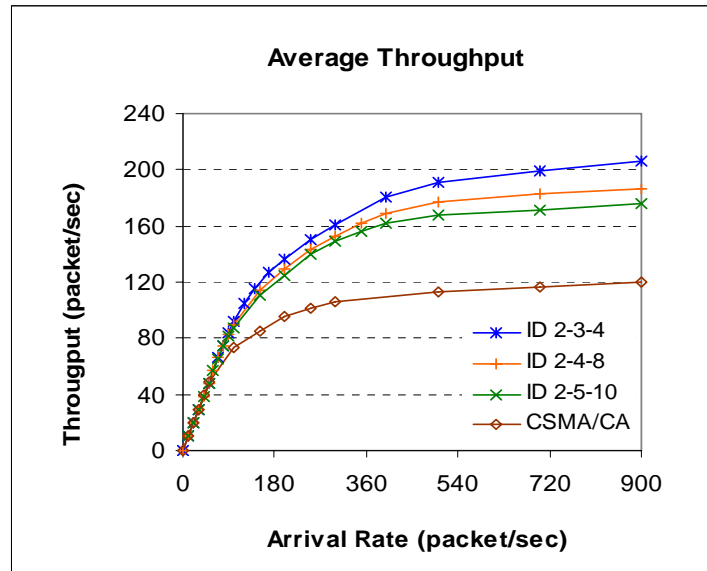


Figure 4.1 Network throughputs for CSMA/CA and DPMA with different BCNs.

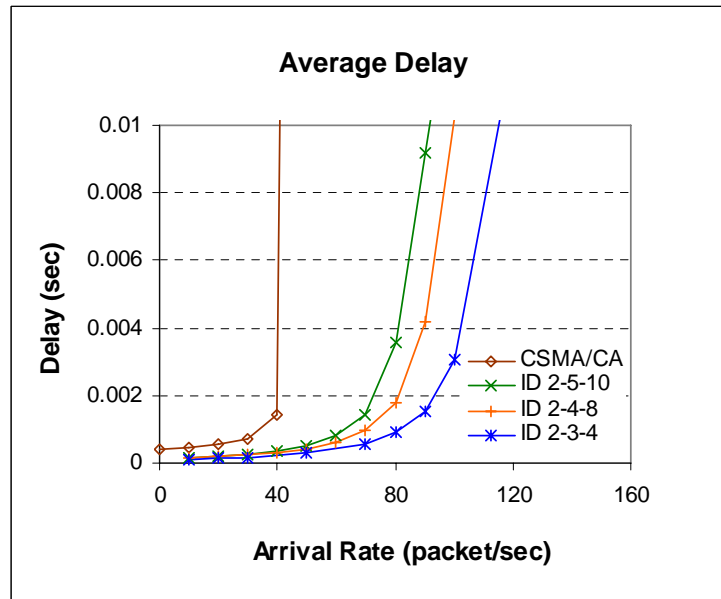


Figure 4.2 Average delays for CSMA/CA and DPMA with different BCNs.

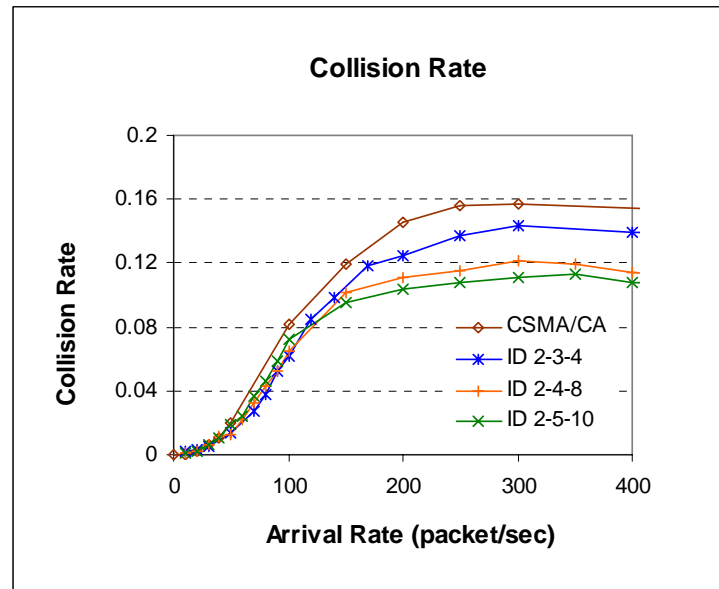


Figure 4.3 Collision rates for CSMA/CA and DPMA with different BCNs.

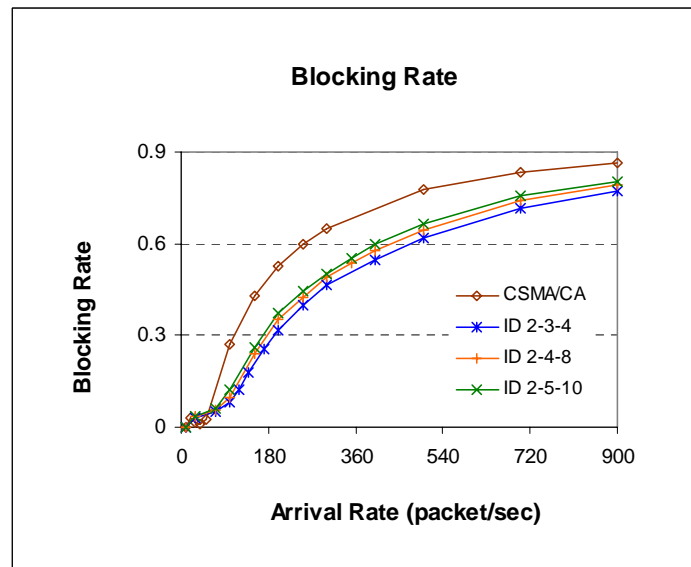


Figure 4.4 Blocking rates for CSMA/CA and DPMA with different BCNs.

From Figure 4.5 and Figure 4.6 we can see that there is an optimal value of ID length (i.e. ID = 14, means ID 2-4-8) which results in the best network performance in terms of maximum throughput and minimum average packet delay. The reason behind this fact is that as ID length is too short, the overlapping of IDs among neighboring stations causes too many collisions and thus the system has quite low throughput. Therefore using longer ID length reduces collisions caused by overlapping IDs and leads to higher throughput. However, as even longer IDs are used, the effect of large contention overhead reduces the network throughput considerably, although the collision rate is low. Therefore, to optimize network performance, we should choose an optimal value of ID length according to network density and traffic load. We can also see that CSMA/CA achieves a little higher throughput than DPMA with ID length = 7, but much lower throughput than the optimal value that DPMA with ID length = 14 achieves. In addition, Figure 4.6 shows that the average delay of CSMA/CA is the highest among all cases of DPMA. Figure 4.7 depicts that for DPMA, longer ID length always leads to smaller collision rate. The reason is the same as we discussed in the above.

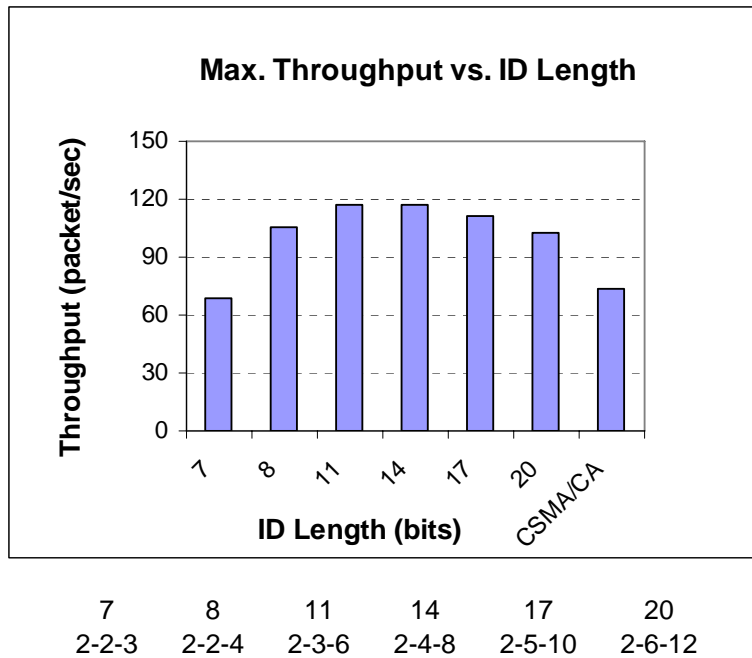


Figure 4.5 Maximum throughputs for different ID lengths.

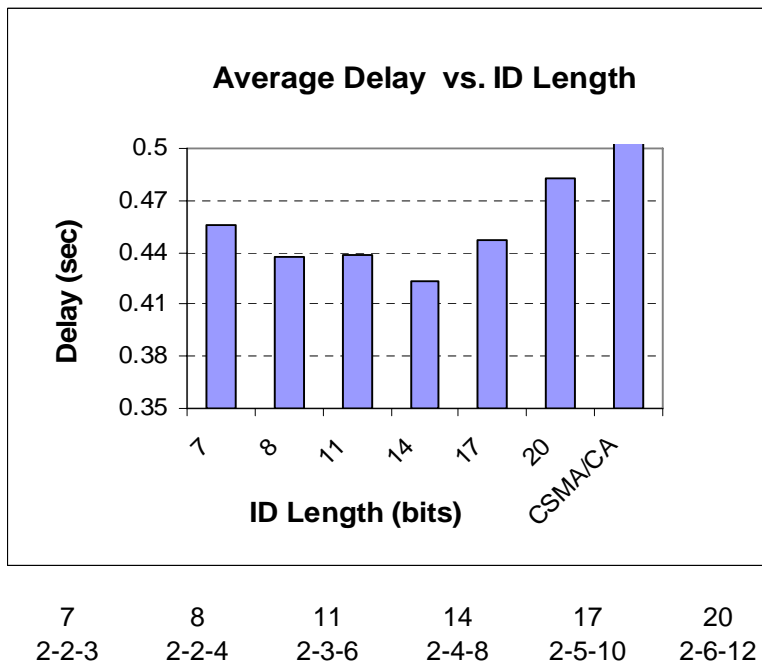


Figure 4.6 Average delays for different ID lengths.

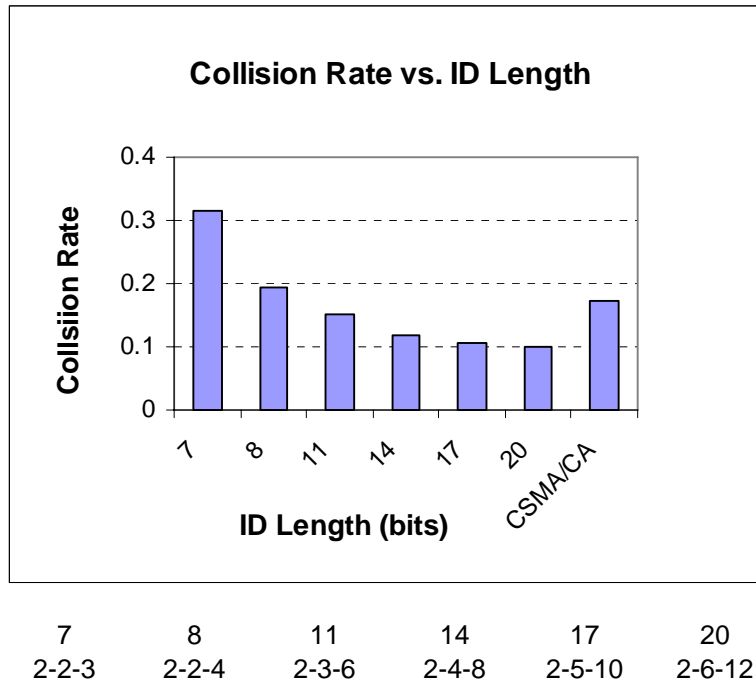


Figure 4.7 Collision rates for different ID lengths.

4.2.2 Effect of Slot Duration

Due to different application/networking environments and technology advances, the minimum slot duration that can be used will be different. In this experiment, we change the slot duration to observe its effect on the maximum throughput that can be achieved. A unit slot is a unit of transmitter/receiver prohibition subslots, which means a transmitter/receiver prohibition subslot consists of several unit slots. For example, in Figure 4.8, the first transmitter prohibition subslot consists of 8 unit slots.

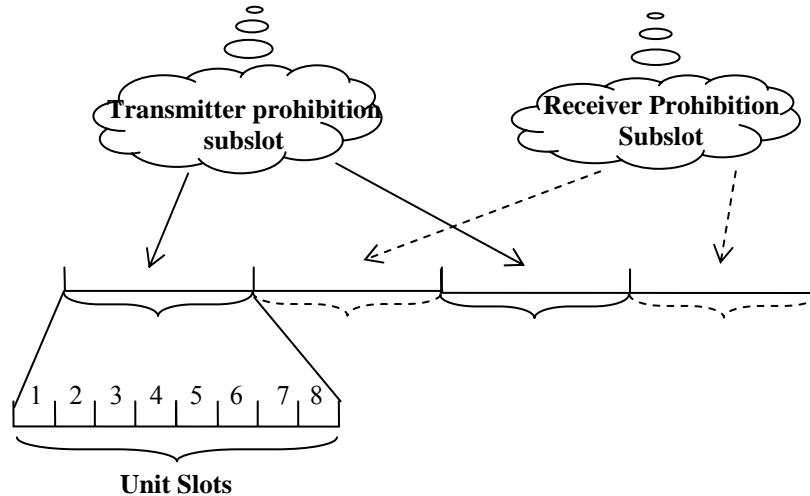


Figure 4.8 Structure of transmitter/receiver subslots.

Figure 4.9 shows the simulation result. We found that the achieved maximum throughput for DPMA decreases as the unit slot length is increased from $0.1 \mu s$ to $3.0 \mu s$. The reason is that, for longer unit slot duration, the time period of contention phase becomes longer. Therefore, the overhead for accessing the medium is increased considerably, which results in lower network throughput. From this figure, we also see that, for different cases of BCNs, the effect of unit slot length on network throughput is the same. This fact implies that larger control channel bandwidth will lead to better system performance. Comparing the performance of DPMA and CSMA/CA shown in Figure 4.9, we can see that DPMA obtains higher maximum throughput than CSMA/CA when the unit slot length is less than around $0.5 \mu s$. As the unit slot length increases, the performance of DPMA degrades quickly and becomes even worse than that of CSMA/CA.

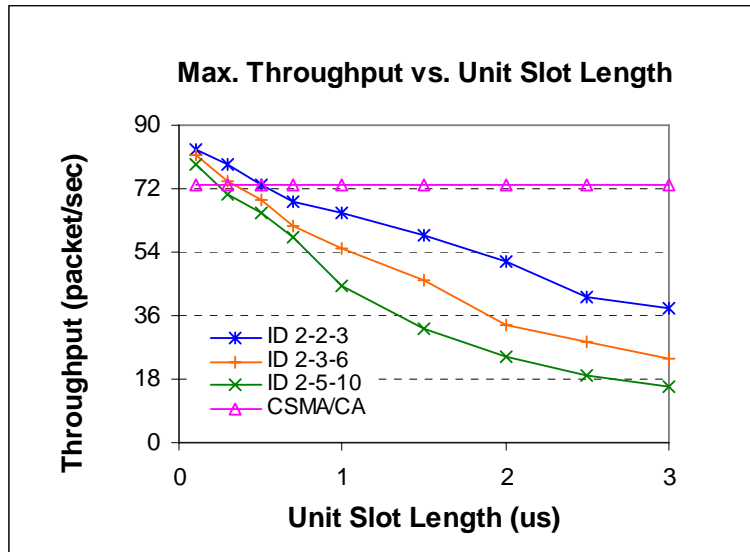


Figure 4.9 Experiment on the effect of unit slot length in DPMA.

4.2.3 Effect of Safe Margin

In DPMA, safe margin is used to mitigate the additive prohibiting signal strength problem. The intended receivers send prohibiting signals according to their remaining allowed interference, i.e.,

$$\text{Prohibiting signal strength} = \frac{1}{\text{Remaining allowed interference}}$$

The competing transmitters measure the received additive prohibiting signals sent by receivers in their vicinity and then decide that it survives in this receiver prohibiting subslot or not. In this experiment, we change receivers' prohibiting signal strength by adding a safe margin factor into above equation, which becomes

$$\text{Prohibiting signal strength} = \frac{1 * \text{Safe_Margin}}{\text{Remaining allowed interference}}$$

The simulation results in Figure 4.10 show the effect of using safe margin on the system performance. We can see that, for different cases of BCNs, the system has the highest maximum throughput when safe margin factor is equal to 2, which means double the strength of prohibiting signals sent by receivers, the system obtains the optimized performance. The reason behind this result is that when we enlarge the safe margin factor to increase the prohibiting signal power level, the strength of received additive signals at transmitters is increased. However, the threshold for transmitters to be killed in the competition is also increased. Therefore, these two factors affect the network performance in the opposite way and the network achieves the best performance when safe margin factor is 2.

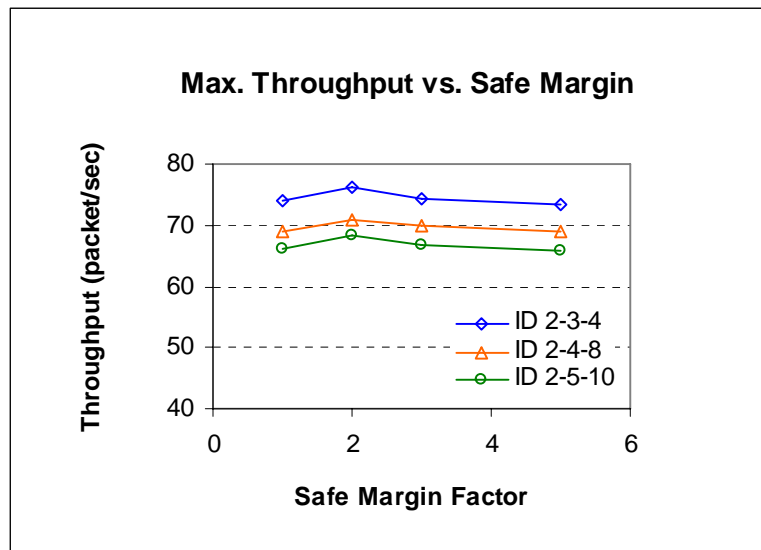


Figure 4.10 The effect of safe margin on network performance.

4.2.4 QoS Differentiation Capability of DPMA

In this section, we demonstrate the capability of DPMA for QoS Differentiation through simulations. Figure 4.11 depicts differentiated throughput for DPMA with four priority classes (priority 1, 2, 3, and 4). The network density $D = 10$. The unit slot length is equal to $0.1 \lambda \mu s$. The BCN used by each mobile node is in the form of ID 2-3-4, which means 2 bits for the priority number part, 3 bits for the random number part, 4 bits for the station ID part. The arrival rates for the four differentiated packets are the same, which is equal to one quarter of the mean aggregated packet arrival rate λ . The arrival rate for CSMA/CA is also equal to $\lambda/4$. Note that no DiffServ is implemented in the CSMA/CA protocol.

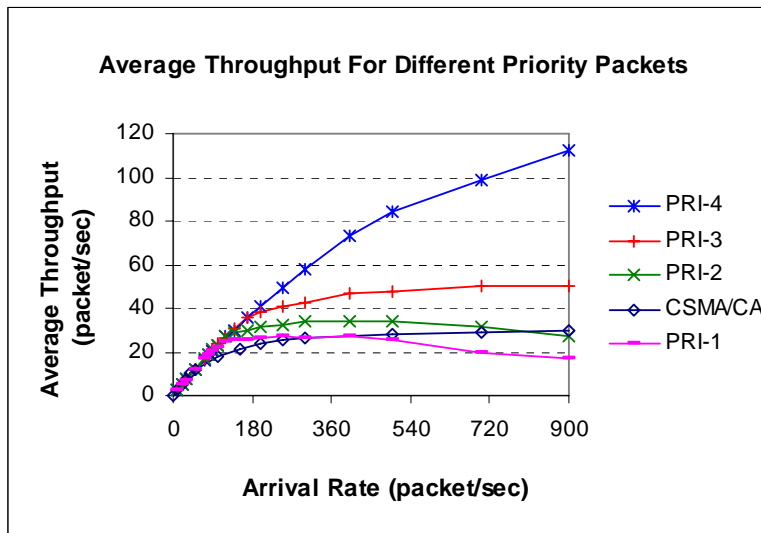


Figure 4.11 Differentiated throughput vs. arrival rate for DPMA

From Figure 4.11, we find that the system throughput is similar for the four priorities when the traffic load is low (i.e., $\lambda \leq 100$). When the traffic load becomes higher (i.e., $\lambda \geq 500$), we can see that the throughput of lower priority packets of PRI_1 and PRI_2 begin to decrease, while the throughput of the highest priority packets (i.e., Pri_4) still continue to

increase. Therefore, it demonstrates that the four priority packets are differentiated effectively in DPMA. The reason behind this fact is that packets with higher priority can always beat lower priority packets during the contention process by assigning the priority number part of BCNs in DPMA. More detailed reasons have been explained in the Section 3.2.4.

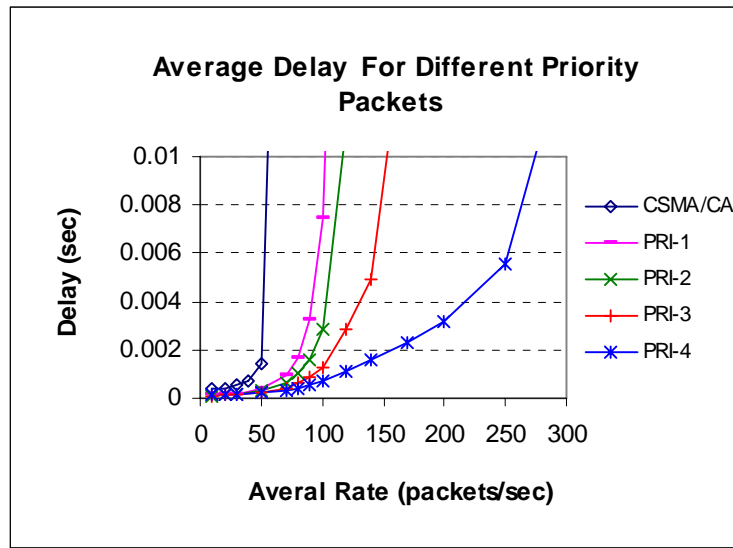


Figure 4.12 Differentiated delay vs. arrival rate for DPMA

For further comparison, Figure 4.12 illustrates the average delay for different priority packets. Similarly, we can see that all the four priority packets have similar average delay as the traffic load is low ($\lambda \leq 50$). When the traffic load gets higher ($\lambda \geq 50$), we find that, as the traffic load increases, the highest priority packets remain a very small average delay while the average delays of lower priority packets (such as PRI_1 and PRI_2) increase quickly. Therefore, for delay-sensitive applications, such as voice and video, DPMA can

provide relatively small end-to-end delay by assigning higher priority to the voice and video packets.

4.2.5 Performance Comparisons for DPMA and CSMA/CA

In the following series of experiments, the performance of DPMA is compared with CSMA/CA. We set the BCN in DPMA as ID 2-4-8, which means 2 bits for the priority number part, 4 bits for the random number part, 8 bits for the station ID part. The unit slot length is $1\mu s$. Figures 4.13 and Figure 4.14 show the average throughput of DPMA and CSMA/CA for Density = 10 and Density = 20, respectively.

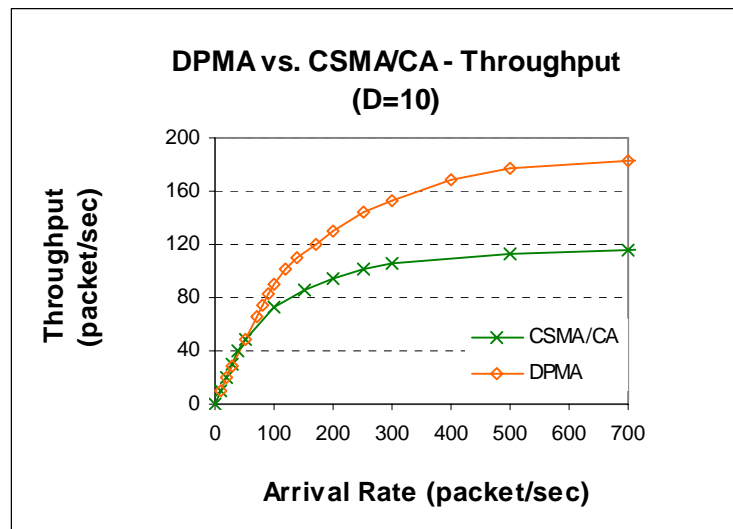


Figure 4.13 Throughput comparison between DPMA and CSMA/CA (Density = 10).

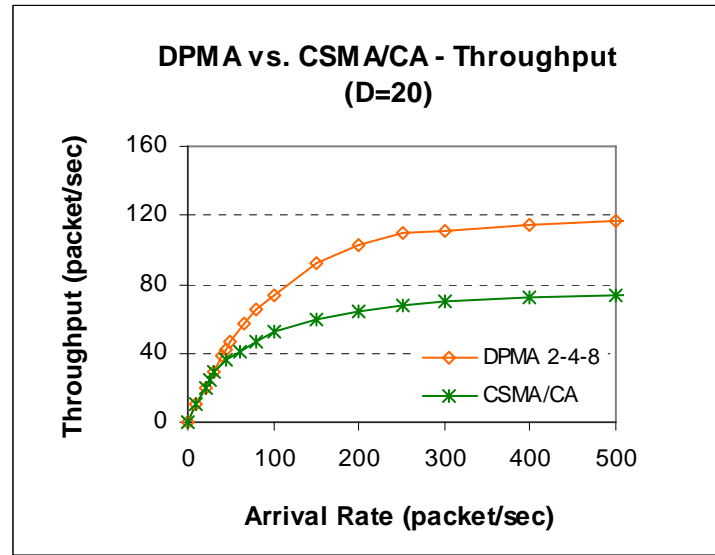


Figure 4.14 Throughput comparison between DPMA and CSMA/CA (Density = 20).

In Figure 4.13, we see that the system that implements CSMA/CA saturates at around $\lambda = 300$ packets/sec, while the system that implements DPMA saturates at around $\lambda = 500$ packets/sec. Also, the maximum throughput achieved by DPMA is 58.9% higher than CSMA/CA. When we increase the network density from 10 to 20, both protocols saturate at lower traffic load, i.e., at arrival rate of 300 packets/sec for DPMA and 200 packets/sec for CSMA/CA. We can conclude that, in terms of network throughput, the DPMA protocol outperforms CSMA/CA in both high and low density network environment. The reason is that, CSMA/CA MAC protocol suffers from more serious hidden/exposed terminal problems. Therefore, either nodes are blocked from transmission unnecessarily or data packets are collided by hidden terminals, which results in lower throughput, especially in high density networks. However, in DPMA, power control and collision avoidance mechanisms are employed to enable more concurrent data transmissions with low

collisions, even under high density network. As a result, DPMA can dynamically adapt to the status of the medium, and maximize the utilization of the network resources, which makes it outperform the CSMA/CA MAC protocol. This can also be demonstrated from the simulation results of the average packet delay, the collision rate and the blocking rate shown in Figure 4.15 – Figure 4.20.

In Figures 4.15 and Figure 4.16, the average packet delay for CSMA/CA and DPMA is shown under Density = 10 and Density = 20, respectively.

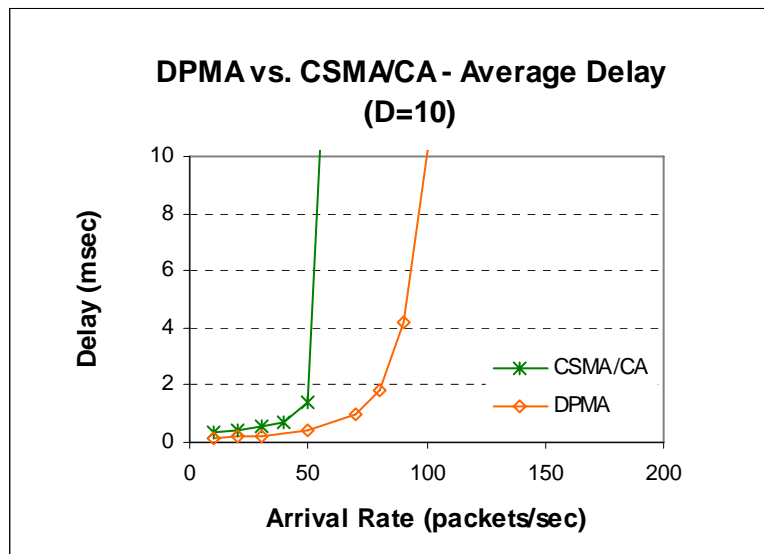


Figure 4.15 Average delay comparison between DPMA and CSMA/CA (Density = 10).

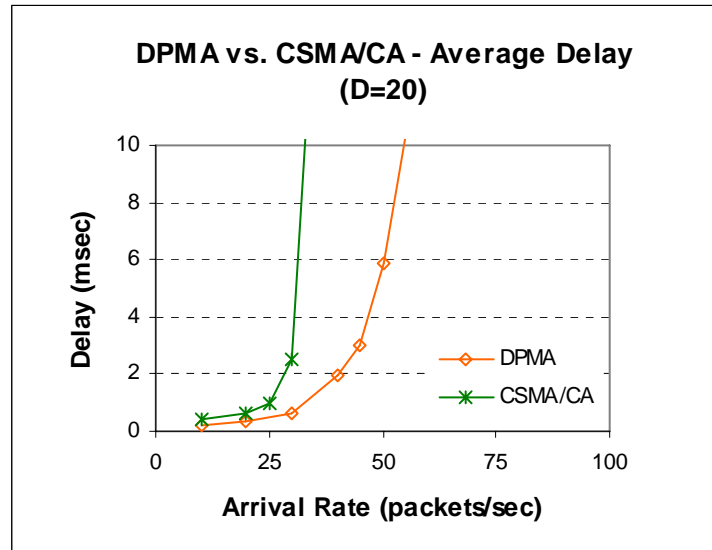


Figure 4.16 Average delay comparison between DPMA and CSMA/CA (Density = 20).

We observe that, at $\lambda = 30$ packets/sec, the average delay for CSMA/CA increases 0.5sec to 2.5sec when network density is double, while the average delay for DPMA only increases from 0.2sec to 0.6sec. This is because the exposed terminal problem gets more serious in CSMA/CA as density increases. Mobile stations are blocked from transmission and spend longer time on waiting in the queue. However, in DPMA, by incorporating the power control mechanism with the dual prohibition mechanism, relatively smaller number of nodes will be interfered/prohibited by prohibiting signals or by data transmissions. That is, DPMA greatly alleviates the exposed terminal problem. Therefore, density has little effect on DPMA because it can dynamically adapt to the status of the medium.

In Figures 4.17 and Figure 4.18, the collision rate for CSMA/CA and DPMA is studied for density = 10 and density =20, respectively.

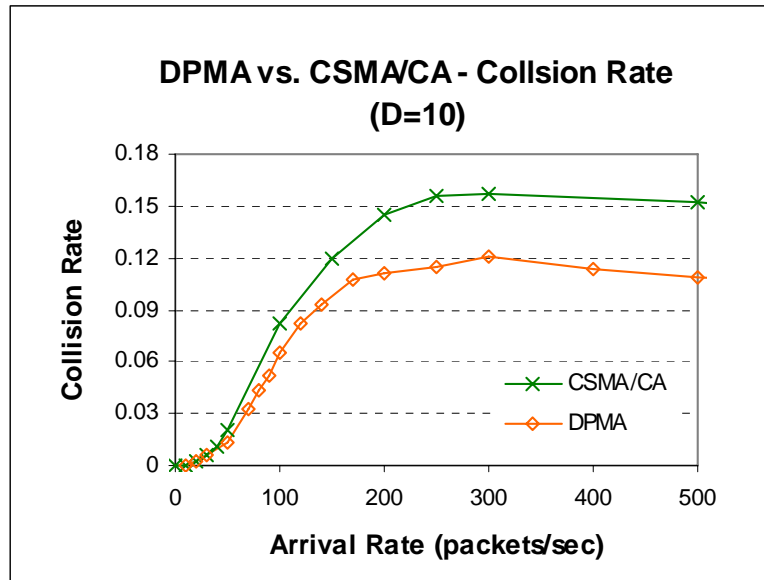


Figure 4.17 Collision rate comparison between DPMA and CSMA/CA (Density = 10).

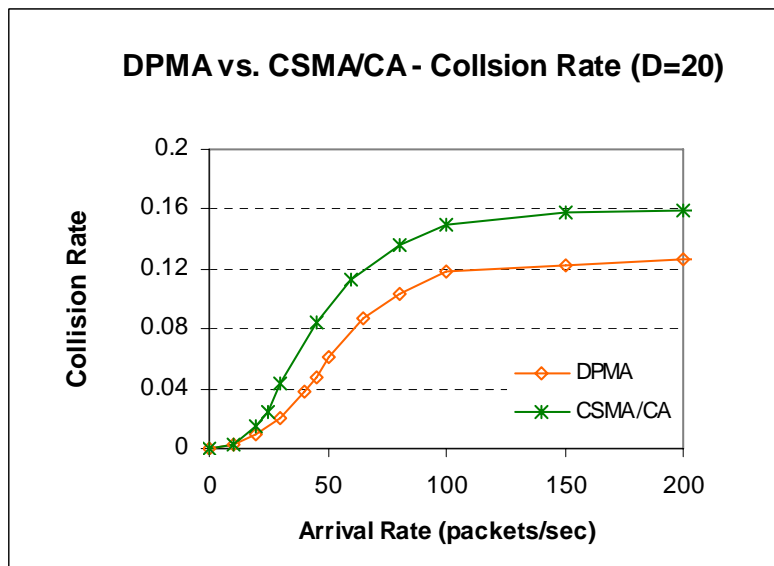


Figure 4.18 Collision rate comparison between DPMA and CSMA/CA (Density = 20).

From Figure 4.17 and Figure 4.18 we find that the collision rate of CSMA/CA is higher than that of DPMA in both low and high density network. The reasons are as follows:

First, the control messages (RTS/CTS) in CSMA/CA are collision-prone, while the busy-tone like prohibiting signals in DPMA do not suffer from collisions. Secondly, CSMA/CA does not take the additive interference problem into account, which causes the high collision rate. DPMA implements the additive interference control mechanism, which leads to much lower collision rate.

The interference caused by transmissions with properly controlled transmission power in DPMA is much smaller than the interference caused by transmissions with fixed transmission power in CSMA/CA. That is to say, the power control in DPMA incurs less interference to surrounding nodes, and thus reduces the probability of packet collision. Furthermore, with the aid of the additive interference mechanism, all nodes keep measuring the additive interference caused by the on-going and the upcoming transmissions. It implies that all nodes update MAP properly to avoid possible data collisions. As a result, it greatly reduces the probability of data collisions even though the density increases.

In Figures 4.19 and Figure 4.20, we compare the blocking rate of DPMA and CSMA/CA. We can see that under both low and high density environments, the CSMA/CA MAC protocol has higher blocking rate than DPMA for both light and heavy traffic load.

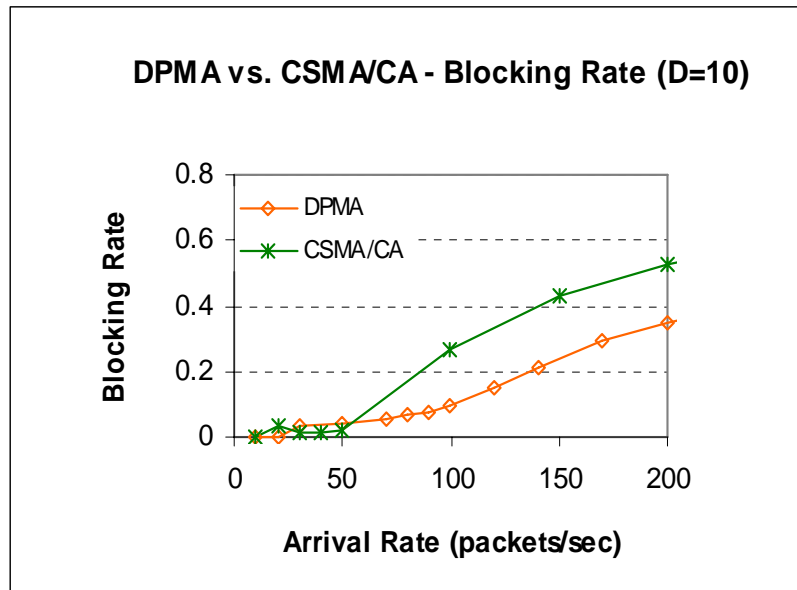


Figure 4.19 Blocking rate comparison between DPMA and CSMA/CA (Density = 10).

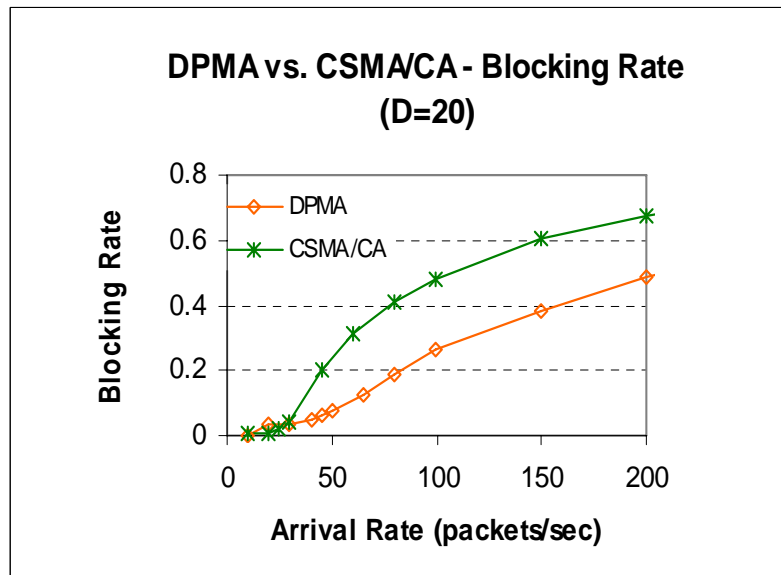


Figure 4.20 Blocking rate comparison between DPMA and CSMA/CA (Density = 20).

In the following figures, i.e., Figure 4.21 – Figure 4.26, we compare CSMA/CA with DPMA with different system parameter settings. In Figure 4.21 – Figure 4.23, we change the unit slot length in DPMA to compare its performance with CSMA/CA. We find that DPMA with slot length (SL) = $1\mu s$ and SL = $1.5\mu s$ has higher throughput and lower delay than CSMA/CA (see Figure 4.21 and Figure 4.22). However, when SL is increased to $2.5\mu s$, the performance of DPMA degrades considerably and is even worse than CSMA/CA. The reason is that longer unit slot length results in larger contention overhead. In Figure 4.23, we can see that DPMA has lower collision rate than CSMA/CA for different unit slot lengths. Furthermore, the longer unit slot length, the lower collision rate.

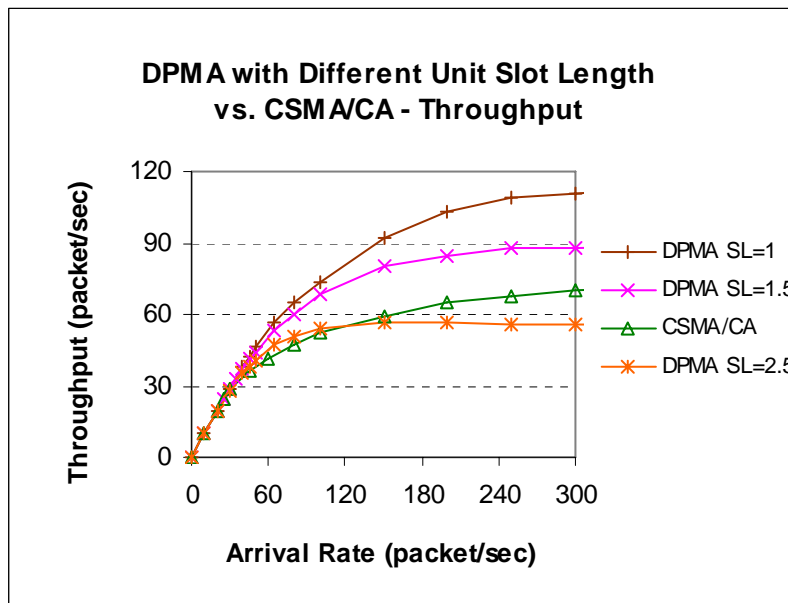


Figure 4.21 Throughput comparison between CSMA/CA and DPMA with different unit slot lengths.

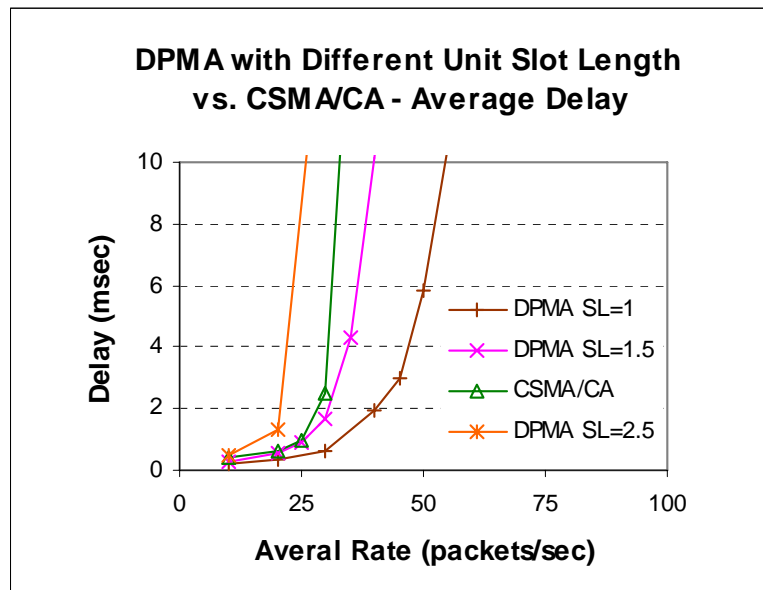


Figure 4.22 Average delay comparison between CSMA/CA and DPMA with different unit slot lengths.

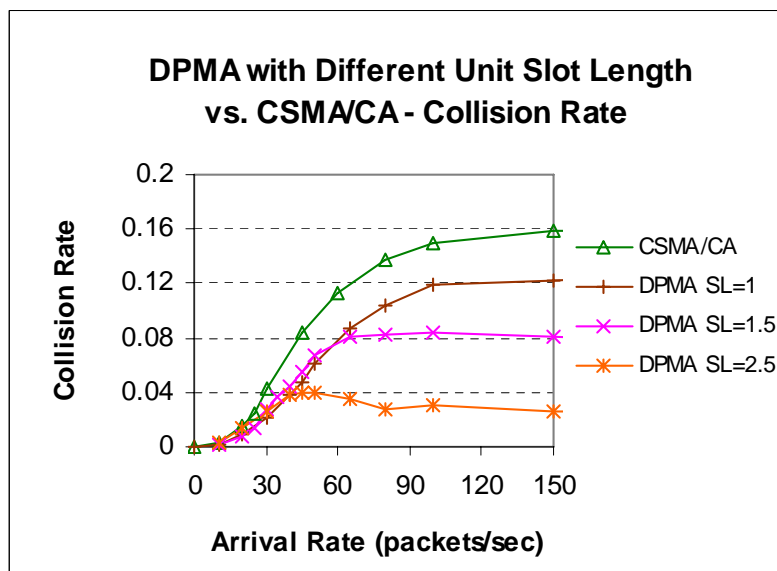


Figure 4.23 Collision rate comparison between CSMA/CA and DPMA with different unit slot lengths.

In Figure 4.24 – Figure 4.26, we apply different BCNs in DPMA to compare the performance of it with CSMA/CA. We can see that for all cases of BCNs, the network system employing DPMA obtains better performance than CSMA/CA in terms of system throughput and average packet delay, although the collision rate of DPMA with BCN 2-2-3 is much greater than that of CSMA/CA.

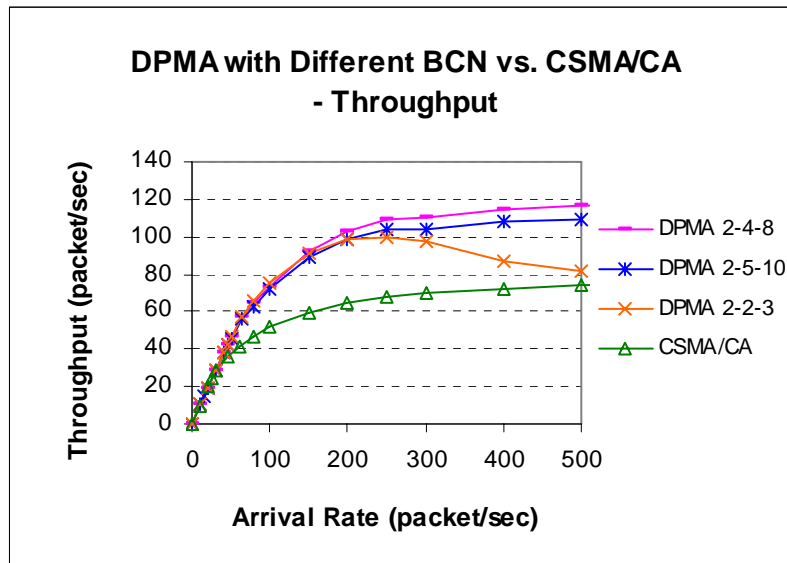


Figure 4.24 Throughput comparison between CSMA/CA and DPMA with different BCNs.

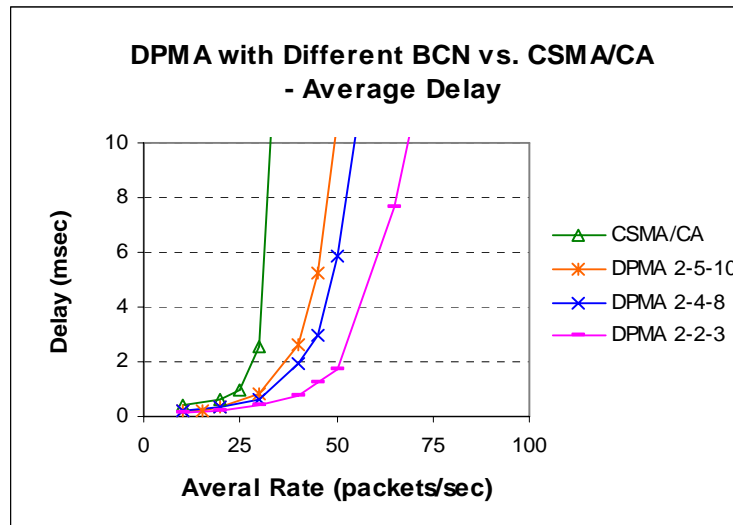


Figure 4.25 Average delay comparison between CSMA/CA and DPMA with different BCNs.

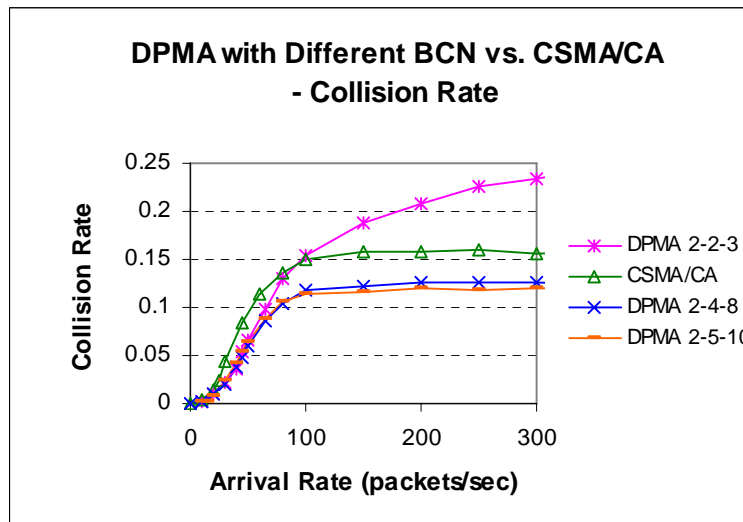


Figure 4.26 Collision rate comparison between CSMA/CA and DPMA with different BCNs.

We conclude that DPMA outperforms CSMA/CA significantly in both low and high density network environment if BCN and unit slot length are appropriately set. The performance of CSMA/CA degrades fast as the traffic load and number of stations increase. DPMA can provide much higher average throughput, smaller average packet delay and lower collision rate compared to the legacy CSMA/CA. Furthermore, in DPMA, the spatial utilization can be maximized and the collision rate is controlled to a very low level. As a result, DPMA significantly improves the overall network performance as compared to CSMA/CA, especially under heavy traffic load and large network density.

4.3 Summary

In this chapter we evaluated the performance of the DPMA protocol through a realistic simulation model by taking the additive interference into account. Moreover, the performance of DPMA is compared to CSMA/CA in terms of average system throughput, end-to-end average packet delay, and collision rate. The simulation results show that the network system achieves different performance when different ID lengths, different unit slot lengths or different safe margins are applied in the DPMA protocol. Specifically, with ID 2-4-8 is used, the system obtains the highest throughput and lowest average delay compared to the cases of using ID 2-3-4 and ID 2-5-10. That is to say, in terms of ID length, the system achieves better performance with using ID 2-4-8. The simulation results also show that the shorter the unit slot length, the higher throughput and lower average delay. Furthermore, the simulation results demonstrate that with properly assigned binary

IDs, DPMA is able to provide strong differentiation capability in terms of throughput and delay.

In addition, DPMA protocol is compared with CSMA/CA protocol. When unit slot length = $1\mu s$ and using ID 2-4-8, DPMA has higher throughput, lower delay and lower collision rate than CSMA/CA. However, when unit slot length increases to $2.5\mu s$, the performance of DPMA degrades considerably and becomes even worse than that of CSMA/CA. Therefore, in DPMA, larger control channel bandwidth leads to better system performance. When we change the ID length from ID 2-2-3 to ID 2-4-8 and finally ID 2-5-10, we found that for these three cases, DPMA has higher throughput and lower average delay than CSMA/CA. However, DPMA with ID 2-2-3 has higher collision rate than CSMA/CA.

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

Due to the great flexibility to support the communication of mobile users, mobile ad hoc networks have become very popular in the research community in recent years. The MAC protocol is used to coordinate mobile nodes to resolve contentions when accessing the shared wireless medium. Due to the characteristics of the wireless ad hoc network --- fast deployable, self-organizing without central control, it is a challenging task to design an efficient MAC protocol to avoid packet collisions, increase the spatial reuse, maximize the system throughput, and at the same time guarantee QoS. A decade ago, the CSMA/CA scheme was standardized in the most popular IEEE 802.11 DCF, and is now commonly used in wireless ad hoc networks. However, RTS/CTS based MAC protocols do not eliminate the hidden terminal problems or the exposed terminal problems in the ad hoc environment. Moreover, the collisions between RTS, CTS, and Data are unavoidable in the shared wireless medium.

In this thesis, a dual prohibition multiple access (DPMA) protocol is described in detail in Chapter 3. In Chapter 4, the performance of the DPMA protocol is well studied and compared to the CSMA/CA MAC protocol through the event-driven simulator developed by using the C programming language.

In DPMA, to prevent the collisions of the RTS/CTS control messages, busy-tone like signals (dual prohibiting signals) are applied for preventing data packet collisions. Meanwhile, the DPMA protocol utilizes the dual channels for control signals and data signals, respectively. Therefore, the collisions between control and data packets are naturally avoided.

Due to the unique feature of the dual prohibiting signals, power control can be easily implemented in the DPMA protocol by controlling the power level of the prohibiting signal, declaring signal and the data packet signal during the “contention round” and the data transmission round. By combining the power control mechanism with the core dual prohibition mechanism in DPMA, it not only increases the spatial reuse, but also reduces the interference to the neighboring nodes. Consequently, the network throughput can be improved and energy is saved.

By simply setting the appropriate values for the priority number part and the random number part in the BCN, DPMA is able to support DiffServ and maintain fairness at the same time.

We have conducted comprehensive simulations to study various effects on network performance by changing the parameters of BCN, unit slot length, safe margin and network density. We also did experiments on comparing DPMA with the CSMA/CA MAC protocol. Simulations results show that DPMA can achieve better performance than CSMA/CA MAC protocol when the control channel is assigned with enough bandwidth and an optimal ID combination is selected. The reason behind the fact is that, combining various mechanisms in DPMA (e.g., dual prohibition, dual channels, additive interference control, and power control), leads to efficient interference control, collision avoidance and spatial reuse.

The performance improvements of DPMA are achieved at the expense of some extra overhead and complexity. In particular, separate control channels are required for binary countdown competition. Hardware for such competition including sending and detection of prohibition signals is required. The protocol also leads to some extra complexity for handling such a mechanism. Moreover, the version of DPMA presented in this thesis requires synchronization, which is not easy to implement. Some supporting mechanisms for power control, interference engineering, assignment of IDs, and concurrent competition for sender and receiver are omitted in this thesis. Finally, the performance of DPMA is not always better than CSMA/CA, for example, when the propagation delay is relatively large, leading to large unit slot duration.

5.2 Future Work

Our future research work can be conducted in several directions. First, in the DPMA protocol, only one data channel is implemented for data transmission. To further improve the system capacity and increase bandwidth utilization, a version of DPMA that can utilize multiple data channels can be developed. Secondly, comparison with other MAC protocols should be conducted, especially those with more complicated and advanced mechanisms for power control and QoS supports, and MAC protocols with separate control channels. Thirdly, in our simulation, we use a simple free-space channel model. More realistic models that take into account pathloss, fading and shadowing factors may be used. Finally, cross-layer design can be incorporated into future versions of DPMA.

BIBLIOGRAPHY

- [1] J. Sheu; S. Wu; C. Lin; Y-C Tseng, "A new multi-channel MAC protocol with on-demand channel assignment for multi-hop mobile ad hoc networks," in *Parallel Architectures, Algorithms and Networks*, 2000, pp. 232 - 237.

- [2] L. Kleinrock; F. Tobagi, "Packet Switching in Radio Channels: Part I--Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics," *Communications, IEEE Transactions*, vol. 23, pp. 1417 - 1433 Dec 1975.

- [3] L. Kleinrock; F. Tobagi, "Packet Switching in Radio Channels: Part II--The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution," *IEEE TRANSACTIONS ON COMMUNICATIONS*, vol. 23, pp. 1417 - 1433 Dec 1975.

- [4] L. Zhang; V. Bharghavan; A. Demers; S. Shenker, "MACAW: A Media Access Protocol for Wireless LAN's," in *Proceedings ACM SIGCOMM*, 1994, pp. 210 - 225.

-
- [5] P. Karn, "MACA – a New Channel Access Method for Packet Radio," in *Proceedings ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, New York, 1990.
- [6] J.J. Garcia-Luna-Aceves; C. L. Fullmer;, "Solutions to Hidden Terminal Problems in Wireless Networks," in *Proceedings ACM SIGCOMM, Cannes, France*, 1997.
- [7] "Wireless LAN Medium Access Control (MAC and Physical Layer (PHY) specifications," *Draft Standard IEEE 802.11*, 1997.
- [8] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE Standard 802.11," 1999.
- [9] Z.J. Haas; J. Deng, "Dual busy tone multiple access (DBTMA)-a multiple access control scheme for ad hoc networks," *IEEE Transactions On Communications*, vol. 50, pp. 975 - 985 June 2002.
- [10] T. Saadawi; S. Xu, "Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks?," in *IEEE Commun.* vol. 39, 2001, pp. 130–137.
- [11] J.J. Garcia-Luna-Aceves; Y. Wang, "Collision avoidance in multihop ad hoc networks," in *Proc. of the IEEE/ACM MASCOT'02*, Texas, U.S.A., 2002.

-
- [12] S. Choi et al., "IEEE 802.11e Contention-Based Channel Access (EDCF) Performance Evaluation," in *Proc. IEEE ICC 2003*, 2003.
- [13] Q. Zeng; Y. Chen, "Performance evaluation for IEEE 802.11e enhanced distributed coordination function," in *Wireless Communications and Mobile Computing*, 2004, pp. 639–653.
- [14] N.H. Vaidya; E.S. Jung, "A Power Control MAC protocol for ad hoc networks," in *ACM International Conference Mobile Computing and Networking (MOBICOM)*, 2002.
- [15] J. P. Monks; V. Bharghavan; W.-M. W. Hwu, "A power controlled multiple access protocol for wireless packet networks," in *4th Annual IEEE International Conference on Computer Communication (INFOCOM)*, 2001, pp. 219-228.
- [16] J. Gomez; A. T. Campbell; M. Naghshineh; C. Bisdikian, "Conserving transmission power in wireless ad hoc networks," in *Proceedings of 9th IEEE International Conference in Network Protocols (ICNP)*, Riverside, California, 2001, pp. 11-14.
- [17] C. K. Toh, "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks," in *IEEE Communications Magazine*. vol. 39, 2001, pp. 138-147.

- [18] S. Agarwal; S. Krishnamurthy; R. H. Katz; S. K. Dao, "Distributed power control in ad-hoc wireless networks," in *IEEE International Symposium on Personal and Indoor Mobile Radio Communication (PIMRC)*, 2001, pp. 59-66.
- [19] X. Qiu;, Y. Gu; L. Shen, "A dual-channel MAC protocol for multi-hop ad hoc networks," in *Communications, Circuits and Systems, 2005. Proceedings.*, 2005, pp. 308 - 313.
- [20] J. Zhu; Roy, S., "A 802.11 Based Slotted Dual-Channel Reservation MAC Protocol for In-Building Multi-Hop Networks," *Mobile Networks and Applications*, vol. 10, pp. 593-606, Oct 2005.
- [21] H. Zhai; J. Wang; Y. Fang, "DUCHA: A New Dual-channel MAC Protocol for Multihop Ad Hoc Networks," *IEEE TRANSACTION ON WIRELESS COMMUNICATIONS*, 2006.
- [22] Y. Chen; S. Leng; L. Zhang, "IEEE 802.11 MAC protocol enhanced by busy tones," in *Communications, 2005. ICC 2005.* , 2005, pp. 2969 - 2973.
- [23] J. Sheu; S. Wu; Y. Tseng, "Intelligent medium access for mobile ad hoc networks with busy tones and power control," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 18, pp. 1647 - 1657 Sep 2000.

-
- [24] A. Nasipuri; J. Mondhe, "Multi-channel MAC with Dynamic Channel Selection for Ad Hoc Networks " 2004.
- [25] B. Ji, "Asynchronous busy-tone multiple access with acknowledgement (ABTMA/ACK) for ad hoc wireless networks," in *GLOBECOM '05*, 2005.
- [26] H. Wu; J. Zhai; Y. Wang; D. Fang, "A dual-channel MAC protocol for mobile ad hoc networks," in *Global Telecommunications Conference Workshops, 2004.*, 2004, pp. 27 - 32
- [27] V.O.K. Li; C. Wu, "Receiver-initiated busy-tone multiple access in packet radio networks," in *Proc. ACM SIGCOMM'87*, 1987, pp. 336-342.
- [28] Y. Yuan; H. Chen; M. Jia; X. Chen, "A New Multi-channel MAC Protocol with Power Control for Ad hoc Networks," in *Advanced Information Networking and Applications.*, 2006, pp. 143 - 146.
- [29] C.S. Raghavendra; S. Singh, "Power-Efficient MAC Protocol for Multihop Radio Networks," in *9th IEEE Int'l. Symp. Personal, Indoor and Mobile Radio Commun.*, 1998.

- [30] J. Sheu; Y. Tseng; S. Wu; C. Lin, "A multi-channel MAC protocol with power control for multi-hop mobile ad hoc networks," in *Distributed Computing Systems Workshop*, 2001.
- [31] S.L. Wu; C.Y. Lin; Y.C. Tseng; J.P. Sheu, " A new multichannel MAC protocol with on-demand channel assignment for multi-hop mobile ad hoc networks," in *Proceedings of the IEEE WCNC*, Chicago, 2000.
- [32] Z. Huang; C. Shen; C. Srisathapornphat; C. Jaikaeo, "A busy-tone based directional MAC protocol for ad hoc networks," in *MILCOM 2002.*, 2002, pp. 1233 - 1238.
- [33] R.R. Choudhury; X. Yang; R. Ramanathan; N.H. Vaidya, "On designing MAC protocols for wireless networks using directional antennas," *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 5, pp. 477 - 491 May 2006.
- [34] A.G. Ruzzelli; G. O'Hare; R. Jurdak; R. Tynan, "Advantages of Dual Channel MAC for Wireless Sensor Networks," in *Communication System Software and Middleware, 2006*, 2006, pp. 1- 3.
- [35] A.S. Tanenbaum, *Computer Networks*, forth ed. New Jersey: Prentice Hall, 2002.
- [36] B. Bensaou; Y. Wang; C. Ko, "Fair medium access in 802.11 based wireless ad-hoc networks," in *MobiHOC. 2000*, 2000, pp. 99-106.

- [37] S.F. Midkiff; R.O. Baldwin; N.J. Davis, "A real-time Medium Access Control protocol for ad hoc wireless local area networks," in *Mobile Comput. Commun.*, 1999, pp. 20–27.
- [38] C-H. Yeh, "The heterogeneous hidden/exposed terminal problem for power-controlled ad hoc MAC protocols and its solutions," in *2004 IEEE 59th Vehicular Technology Conference*, 2004, pp. 2548- 2554.
- [39] M. Wenig; A. Schmitz, "The effect of the radio wave propagation model in mobile ad hoc networks," in *Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems*, 2006.
- [40] C.-H. Yeh; H. Zhou, "A new class of collision-free MAC protocols for ad hoc wireless networks," Proc. Int'l Conf. Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet, Jan. 2002.
- [41] C.-H. Yeh, "Medium access control with differentiated adaptation for QoS management in wireless networks," Proc. IEEE Int'l Conf. Mobile and Wireless Communication Networks, 208-219, 2001.
- [42] C.-H. Yeh, "ROAD: A class of variable-radius MAC protocols for ad hoc wireless networks," Proc. IEEE Vehicular Technology Conf. (VTC'02 Spring), 2002.

-
- [43] A. S. Tanenbaum, *Computer Networks*, 3rd Edition, Prentice Hall, N.J., 1996.
- [44] S. Xu; T. Saadawi, "Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks?" *IEEE Communications Magazine*, vol. 39, no. 6, June 2001.
- [45] C.-H. Yeh, "A Collision-controlled MAC Protocol for Mobile Ad Hoc Networks and Multihop Wireless LANs", *IEEE Globecom* 2004.
- [46] X. D. Wang; C. Demiroglu, "A TDMA/TDD MAC protocol for wireless multimedia local area networks," *Proc. IEEE GLOBECOM'01*, vol. 3, pp. 1898 - 1902, 2001.
- [47] R. Garces; J. J. Garcia-Luna-Aceves, "Collision avoidance and resolution multiple access with transmission queues." *ACM Wireless Networks Journal*, 1998.
- [48] E.-S. Jung; N. H. Vaidya, "An energy efficient MAC protocol for wireless LANs," *Proc. IEEE INFOCOM* 2002, vol. 3, pp. 1756 -1764, 2002.
- [49] N. Sivamok; L. Wuttisittikulkij; A. Charoenpanitkit, "New channel reservation techniques for media access control protocol in high bit-rate wireless

- communication systems,” Proc. IEEE GLOBECOM’01, vol. 6, pp. 3558-3562, 2001.
- [50] J.-W Wan; X.-C. Lu, “QoS level-based bandwidth split-level adaptation, J. Software, vol.11, No. 10, Oct. 2000, pp.1375-1381.
- [51] R. Cusani; F. Delli; M. Torregiani, “A novel MAC and scheduling strategy to guarantee QoS for-the new-generation WIND-FLEX wireless LAN,” IEEE Wireless Communications, vol. 9, no. 3, June 2002.

APPENDIX

CONFIDENCE INTERVALS

Confidence intervals can be used to indicate the accuracy of the simulation results. Since it is not possible to get a perfect estimate of the actual mean μ from any finite number of finite size samples, the best we can do is to get probabilistic bounds. Thus, we may be able to get two bounds, for instance, c_1 and c_2 , such that there is a high probability, $1-\alpha$, that the actual mean is in the interval (c_1, c_2) :

$$\text{Probability } [c_1 \leq \mu \leq c_2] = 1 - \alpha \quad (\text{B.1})$$

The interval (c_1, c_2) is called the confidence interval for the actual mean, $100(1-\alpha)$ is called the called the confidence level.

Suppose the sample $[x_1, x_2, \dots, x_n]$ is got from statistically independent simulation runs of the same simulation program and the sample mean is \bar{x} :

$$\bar{x} = \frac{\sum_{i=1}^n x_i}{n} \quad (\text{B.2})$$

The standard deviation of the sample is s and given by:

$$s^2 = \frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n-1} \quad (\text{B.3})$$

For small number of samples, the sample mean is approximately t -distributed with mean \bar{x} and standard deviation s/\sqrt{n} . The $100(1-\alpha)$ confidence interval is given by

$$\left(\bar{x} - t_{[1-\alpha/2; n-1]} \frac{s}{\sqrt{n}}, \bar{x} + t_{[1-\alpha/2; n-1]} \frac{s}{\sqrt{n}} \right) \quad (\text{B.4})$$

Here, $t_{[1-\alpha/2; n-1]}$ is the $(1-\alpha/2)$ -quantile of a t -variate with $n-1$ degrees of freedom.

The following is an example. If the sample mean is $\bar{x} = 3.90$, the standard deviation $s = 0.95$ and $n = 15$, 90% confidence interval for the mean = $3.90 \pm (1.761) * (0.95) / \sqrt{15} = (3.47, 4.33)$. Then we can state with 90% confidence that the actual mean is between 3.47 and 4.33.