An Adaptive Approach on the Carrier Sensing Range of CSMA/CA Multi-hop Wireless Networks

RUAN, Sichao

A Thesis Submitted in Partial Fulfilment
of the Requirements for the Degree of
Master of Philosophy
in
Information Engineering

August 2008

Acknowledgement

I spend two years on the M.Phil. study in the Chinese University of Hong Kong. This is a fruitful and rewarding experience, which I will treat as a lifetime treasure.

I would like to express my deepest gratitude towards my supervisor Prof. Lee, Tony Tong for his patience, for his invaluable advice, and most importantly, for being a true teacher to me. His passions for research and teaching evoke my respect and admiration. This work cannot be finished without his continuous support.

I would much appreciate the people who have worked with me during this two years' period. I would like to thank Mr. Deng Yun, Mr. Choy Man-Ting and Mr. Wang Cong for their discussions and comments on my work. Finally, I am grateful to my parents for morally supporting during all these years.

摘要

多跳自組無線網路(Multihop Ad-hoc Wireless Network)最初是為軍事應用而設計的，現在已經有了更為廣泛的應用。然而，隱藏節點(Hidden Node)和暴露節點(Exposed Node)的問題嚴重限制了多跳無線網路的擴展性。隱藏節點的定義為那些影響文件包接收而發射結點卻無法檢測到的節點，暴露節點指的是在其它節點傳輸過程不必要地被禁止行動的節點。研究者們已經針對這兩個問題提出了大量的處理方法。在 IEEE 802.11 DCF[8]——多跳無線網路的標準中，“載波檢測多路存取/碰撞避免(Carrier Sensing Multiple Access/Collision Avoidance, CSMA/CA)”媒體存取控制(Media Access Control, MAC)協議採用了載波檢測的方法來探測一些活動的節點，並且使用 RTS/CTS 包來通知在發射點和接收點附近的節點保持靜止。因此，一些隱藏節點被去掉了。但是，在[17]中，作者證明了這個標準並不能完全消除所有的隱藏節點，更引入了一系列的暴露節點。作者進一步證明了通過增加載波檢測多路存取協議的檢測範圍，所有的隱藏節點都可以被消除，但同時會造成大量的暴露節點。這一關係暗示了在隱藏和暴露節點之間存在著交換關係。這種交換關係在其他用於解決隱藏節點的方法中也同樣存在。

在此篇論文中，我們首先研究了幾種處理隱藏和暴露節點問題的方法，並對兩個問題之間的交換關係做了細緻的研究。然後，我們導出了一條函數曲線，這

條曲線詮釋了在非持續(non-persistent)載波檢測多路存取/碰撞避免協議中載波檢測範圍和單跳通過量(one-hop throughput)之間的關係。這份分析告訴了我們載波檢測範圍在移除隱藏節點中的效果。由這些分析結果，我們在傳輸控制協議(TCP Protocol)中的擁塞控制視窗(Congestion Control Window)和載波檢測範圍之間建立了一個模型，這樣檢測範圍可以以相類似的方式適時自我調節。基於這個模型，我們提出了兩種媒體存取控制方案，分別叫做 LDMI(線性減少倍數增加, Linear Decrease Multiplicative Increase)和 Tahoe 控制方案。為了評測兩種方案的性能，我們在一個實用的模型中對方案進行了仿真，結果顯示這兩種方案與 IEEE 802.11 比較起來可以提高網路性能。一系列比較包括通過量，節點之間公平性和通過量收斂速度的比較。這份工作顯示了一種平衡隱藏和暴露節點問題，和提高多跳自組無線網路擴展性可行的方法。

Abstract

Multi-hop Ad-hoc wireless networks, which were originally developed for military, now have a much wider range of applications. The hidden and exposed node problems, however, severely limit the scalability of multi-hop wireless networks. The hidden node is defined as the node that interferes the packet reception while the transmitter cannot detect, on other hand, the exposed node is referred to the node that is unnecessarily forced to keep silent during others' transmission. Researchers have proposed numerous schemes to solve these problems. In the IEEE 802.11 DCF [9]—the standard for multi-hop networks, the CSMA/CA (Carrier Sensing Multiple Access with Collision Avoidance) uses physical carrier sensing to detect some active nodes and the RTS/CTS frames to notify nodes in the vicinity of the transmitter and receiver to keep silent. Hence, some hidden nodes are removed. However, in [18], the authors have demonstrated that this standard cannot eliminate all the hidden nodes, and moreover, it defines a set of exposed nodes. They further argued that by increasing the carrier sensing range of CSMA, the hidden nodes can be eliminated, but this results in a large number of exposed nodes. This implies a tradeoff between the hidden and exposed nodes. And this tradeoff also appears in other schemes which are aimed at solving the hidden node problem.

In the thesis, we firstly investigated several schemes for the hidden and exposed node problems to have a detailed study of the tradeoff between these two problems. Then, we derived a function curve, which characterizes the relationship between carrier sensing range and *one-hop* throughput in the *non-persistent* CSMA/CA. This gives us a clear picture of the effect of carrier sensing range in removing the hidden nodes. In the sight of the analysis results, we establish a model between carrier sensing range

and congestion control window in TCP protocols so that the sensing range can be adaptively adjusted in a similar manner. Based on the model, we propose two MAC schemes called as *LDMI* (Linear Decrease Multiplicative Increase) and *Tahoe* Control Schemes. To evaluate the performance, we simulated the schemes in a practical model and the results show that these scheme can improve the performance compared with IEEE 802.11. The comparison includes the throughput, terminal fairness and the throughput convergence speed. This work shows a feasible way to balance the hidden and exposed nodes and improve the scalability of multi-hop Ad-hoc wireless networks.

Contents

1 Introduction 1

1.1 Multihop Ad Hoc Wireless Networks 1

1.1.1 Introduction to Multihop Ad Hoc Networks 2

1.1.2 Scalability of Ad Hoc Wireless Networks 3

1.2 Hidden Terminal Problem 3

1.3 Exposed Terminal Problem 5

1.4 Overview of the Thesis 6

2 Background 8

2.1 MAC Protocols for Wireless Networks 8

2.1.1 Aloha 8

2.1.2 CSMA/CA 9

2.1.3 IEEE 802.11 DCF Standard 10

2.2 Related Work 12

2.2.1 Schemes for Hidden Node Problem 12

2.2.2 Schemes for Exposed Node Problem 13

2.3 Tradeoff between Hidden and Exposed Nodes 14

2.4 The Effect of Carrier Sensing Range 17

3 Analysis on Carrier Sensing Range **18**

3.1 Analysis Model 18

3.1.1 Terminal Configurations 18

3.1.2 Timing/Packet Parameters 19

3.1.3 Protocol Approximation 20

3.1.4 Throughput Measurement 21

3.2 Derivation of Throughput 21

3.2.1 Channel Modeling 22

3.2.2 Actual Transmission Rate 24

3.2.3 Case One 24

3.2.4 Case Two 26

3.2.5 Mathematical Form of Throughput 28

3.2.6 Analysis Results 30

3.3 Implications 31

3.3.1 Value of Sensing Range in CSMA/CA 31

3.3.2 Need for New MAC Protocols 32

4 MAC Protocols by Congestion Control **34**

4.1 Motivations and Principles 34

4.1.1 Balancing Hidden and Exposed Nodes 35

4.1.2 Controlling Carrier Sensing Range 36

4.1.3 Non-homogenous Sensing Range 36

4.2 Algorithm Descriptions 38

4.2.1 Core Concept 38

4.2.2 LDMI Control Scheme 40

4.2.3 Tahoe Control Scheme 41

5 Simulation Analysis 44

5.1 Simulation Configurations 44

5.1.1 Geometric Burst Traffic Model 45

5.1.2 Network Topology 46

5.1.3 Simulation Parameters 47

5.2 Throughput Comparisons 48

5.3 Fairness Comparisons 50

5.3.1 Situation of Unfairness 50

5.3.2 Fairness Measurement 52

5.4 Convergence Comparisons 54

5.5 Summary of Performance Comparison 55

6 Conclusions 56

A Categories of CSMA/CA 58

A.1 1-*persistent* CSMA/CA 58

A.2 *non-persistent* CSMA/CA 58

A.3 *p-persistent* CSMA/CA 59

B Backoff Schemes 60

B.1 Constant Window Backoff Scheme 60

B.2 Geometric Backoff Scheme 60

B.3 Binary Exponential Backoff Scheme 61

Bibliography 62

List of Figures

1.1 Hidden Terminals in CSMA/CA Protocol 5

1.2 Exposed Terminals in CSMA/CA Protocol 6

2.1 The Process of RTS/CTS Handshake 11

2.2 Hidden and Exposed Node in CSMA/CA 14

2.3 Hidden and Exposed Nodes in CSMA/CA with RTS/CTS 15

2.4 Carrier Sensing Range Covering the Whole Interference Range 16

2.5 Tradeoff between Hidden and Exposed Terminals 16

3.1 Diagram for Timing/Packet Parameters 20

3.2 States Experienced by Node A 21

3.3 Markov Chain of the Channel State 22

3.4 Illustration of Case One 25

3.5 Successful Transmission Timing Diagram for Case One 25

3.6 Illustration of Case Two 26

3.7 Successful Transmission Timing Diagram for Case Two 27

3.8 Carrier Sensing Range vs. Throughput 30

3.9 The Effect of Large Carrier Sensing Range 32

4.1 Carrier Sensing Range Coordination 37

4.2 Modeling R_{CS} to Congestion Window 39
4.3 Track of Carrier Sensing Range in LDMI 41
4.4 Track of Carrier Sensing Range in Tahoe 43

5.1 Illustration of Geometric Burst Traffic Model 45
5.2 Network Topology in the Simulation 46
5.3 Throughput Comparisons 49
5.4 Unfairness in Channel Resources Allocation 51
5.5 The Comparison of Terminal Fairness 52
5.6 Speed of Throughput Convergence 54

List of Tables

5.1 Simulation Parameters 47

5.2 The Sample of Terminal Throughputs in *Tahoe Controlling Scheme* . . 53

5.3 Overview of Performance Comparison 55

Chapter 1

Introduction

Wireless networks has now become a mature area of network technology. The wireless Ad Hoc network, a category of wireless networks, is widely used in commercial and military applications. However, the hidden and exposed node problems still limit the progress of Ad Hoc network development. This thesis will provide a study on the MAC layer of Ad Hoc networks and propose some enhancement schemes on the two problems. In this chapter, we will present a description to Ad Hoc networks and the two problems. An overview of the thesis is included in the last section of this chapter.

1.1 Multihop Ad Hoc Wireless Networks

Multihop Ad Hoc Wireless Network was originally developed for military purpose in the 1970s [1]. With the development of the past few decades, it now enjoys a wide range of deployment. We will provide a description of Ad Hoc networks in this section.

1.1.1 Introduction to Multihop Ad Hoc Networks

From the word "Ad Hoc", the Ad Hoc wireless networks should be *self-organizing* and *adaptive*. We can define the network as follows [2].

Definition 1 *An Ad Hoc wireless network is a decentralized network of two or more devices equipped with wireless communications capability. Such devices can communicate with another node that is immediately within their radio range or one that is outside their radio range via relays or forwards.*

The Ad Hoc wireless network can take different forms. Moreover, various kinds of Ad Hoc devices can be deployed in the network, such as, laptop, PDA, mobile phone, palmtop and etc. With the protocol specifications, Ad Hoc devices can detect the presence of neighboring terminals/nodes, therefore the Ad Hoc network itself is *infrastructure-less*. There is no need for any fixed radio base stations, wires or fixed routers to perform overall or partial centralized control. All the nodes are auto-connected and the path links are auto-maintained. These have highlighted the flexibility, reliability and low cost features of Ad Hoc networks [3].

Routing protocols and MAC (Medium Access Control) protocols are the main contributers that make the wireless network "*Ad Hoc*". Many protocols have been proposed. For the network layer, *AODV* (Ad Hoc On-Demand Distance Vector Routing) [4] and *DSR*(Dynamic Source Routing) [5] are now widely accepted routing protocols. For the MAC layer, CSMA/CA [6], CSMA/CA with RTS /CTS [9], BTMA [7] and etc. have been designed. A brief description of some common MAC protocols is provided in Chapter 2. This thesis will focus on the MAC protocol analysis and design to improve the performance of Ad Hoc networks.

1.1.2 Scalability of Ad Hoc Wireless Networks

One of the major challenges in wireless Ad Hoc networks is the scalability problem [2] When the network scale or terminal density increases, the Ad Hoc network performance decreases quickly. This is because most MAC protocols fail to coordinate the terminals efficiently in large-scale networks.

The main causes to this are the notorious hidden [7] and exposed node problems. Hidden nodes are basically a category of interference nodes that may cause packet collisions at the receiver. Hence, the transmission time has been wasted and the transmitter has to perform retransmissions. With the network scale increased, the probability of packet collisions is larger. The exposed node problem often appears in pairs with the hidden node problem. There are various causes to the exposed node problem depending on the MAC protocol specifications. This problem results in network resource waste. The waste is especially obvious when the terminal density is large. A description of hidden and exposed node problem is given in the next section. Thus, because of these two problems, the network performance is severely influenced.

The key to the scalability problem is the coordination of the terminals so that the network can avoid suffering from the hidden and exposed node problems. This thesis will present a detailed study on the coordination issue.

1.2 Hidden Terminal Problem

Hidden Terminal Problem, or Hidden Node Problem was first discovered by Tobagi and Kleinrock in [6] when they proposed the CSMA/CA MAC protocol in [7]. The problem is known to be the main cause of packet collisions in wireless network. The definition of *Hidden Node* is given as follows.

Definition 2 *Hidden terminals are the terminals that are invisible to the transmitter and receiver of the ongoing transmission, and therefore, may cause collisions to the packet reception.*

To decode packets correctly, the received packet signal should have an *SNR* larger than the threshold denoted as SNR_{Th}. In wireless channel, the signal power attenuates with the distance with a *Path Loss Factor* α [8], that is,

$$\frac{P(d_0)}{P(d_1)} = \left(\frac{d_1}{d_0}\right)^{\alpha} \tag{1.1}$$

where $P(d_1)$ means the detected power at distance of d_1 from the source. With this property, there exists a range around the receiver within which the active interference node may cause packet collisions. Assuming the transmitted power is P_t, we have the following equation,

$$SNR = \frac{P_t}{d^{\alpha}} / \frac{P_t}{{D_i}^{\alpha}} \geq SNR_{Th} \tag{1.2}$$

where d is the distance between transmitter and receiver; D_i is the distance of the interference node to the receiver. Therefore, to guarantee the ongoing transmission, it is necessary that,

$$D_I \geq \sqrt[\alpha]{SNR_{Th}}d \tag{1.3}$$

Thus, we denote $R_I = \sqrt[\alpha]{SNR_{Th}}d$ as the interference range of the receiver. The active nodes within this range may become hidden nodes. Fig. 1.1 illustrates the situation that hidden node problem occurs in CSMA/CA (An explanation of CSMA/CA is given in Chapter 2). The terminal A is transmitting to B. The terminal C, D and E are within the interference range R_I. Hence, they are hidden terminals and may cause packet collision at terminal B.

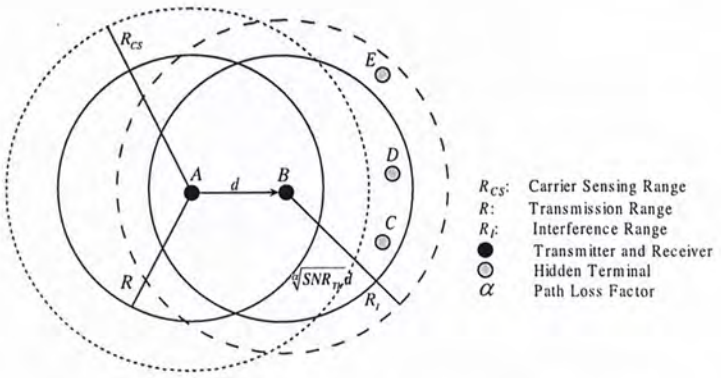


Figure 1.1: Hidden Terminals in CSMA/CA Protocol

Besides CSMA/CA, most MAC protocols, such as Aloha [10] and CSMA/CA with RTS/CTS suffer from the hidden node problem. This problem severely limits the network throughput and scalability. Hence, it has become one of the hot research areas in Ad Hoc networks.

1.3 Exposed Terminal Problem

When researchers developed various MAC protocols, attempting to reduce the packet collision and mitigate the hidden nodes, another problem called Exposed Terminal Problem, or Exposed Node Problem appeared. This has also become a bottleneck in improving the performance of wireless networks. The exposed terminals are defined as follows.

Definition 3 *Exposed terminals are the terminals that are unnecessarily kept inactive because of the exposure to the neighboring transmitter during the ongoing transmission.*

There are various causes of exposed terminal problem, which are related to the MAC protocol specifications. Fig. 1.2 shows an example of exposed in the CSMA/CA protocol. Terminal C is beyond the interference range of the receiver terminal B, hence

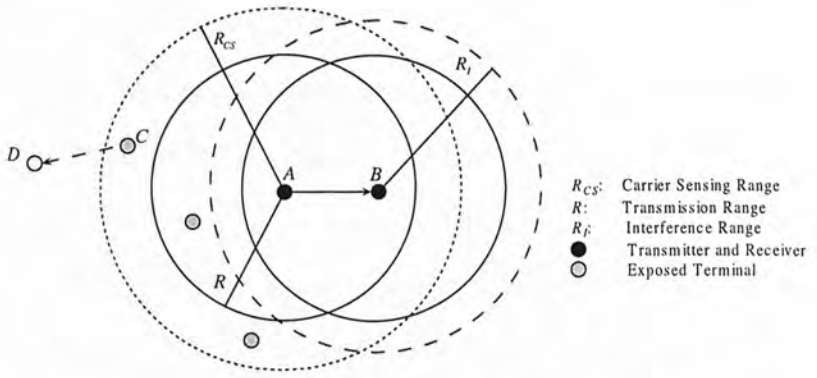


Figure 1.2: Exposed Terminals in CSMA/CA Protocol

its transmission will not affect the packet reception. However, C is within the sensing range of the transmitter A, or it is exposed to terminal A specifically in CSMA/CA. Hereby, terminal C will detect the transmission from A, and thus unnecessarily keep silent during the whole transmission process (C cannot transmit to terminal D). This problem results in *Spatial Reuse Waste* [23].

Other MAC protocols may also have the exposed terminal problem. It is interesting that the exposed terminal problem does not exist in the simplest MAC protocol, say, Aloha. It comes with the people's attempt to solve hidden terminal problem. We will look into this phenomena in further details in the later chapters.

Both hidden and exposed node problems have drawn much research attention in the past decade. In [11], it has been listed as one of the *Top Ten* challenges in the future wireless networks. This thesis intends to reduce the influence of the two problems on the network performance.

1.4 Overview of the Thesis

In the thesis, we will investigate hidden and exposed node problem in depth. According to the analysis results, we will present the mathematical analysis and two MAC

protocols in the aspect of two problems.

In Chapter 2, some background information will be provided in this area including some MAC protocols and related works. In the end of the Chapter 2, we will point out the relationship between these two problems. There actually exists a tradeoff between these two problems. In Chapter 3, mathematical analysis on the influence of carrier sensing range is presented. We will derive the relationship between carrier sensing range and *one-hop* throughput of the network. This analysis provides some implications on coordinating the two problems.

Based on the tradeoff and the analysis of carrier sensing range, we will propose two MAC protocols in Chapter 4. We find the similarity between the carrier sensing range of CSMA/CA and the *window size* in TCP Congestion Control. Hence, a model of these two concepts is established. With reference to this model, two protocols are presented, which utilize the concept of TCP Congestion Control to the MAC layer and try to balance two problems instead of tackling both of them.

To verify the performance of the proposed protocols, Chapter 5 is dedicated to the simulation analysis. We will construct a random topology and compare the proposed protocols with the original CSMA/CA. The terminals in the network deploy a *Burst Traffic Model* we proposed so that the traffic can emulate the real network traffic. Our comparisons include *one-hop* throughput, terminal fairness and throughput convergence. These analyses have demonstrated the superiority of the proposed protocols.

Chapter 2

Background

In this chapter, we will first provide some information on the MAC protocols for single channel wireless Ad Hoc networks, like Aloha and CSMA/CA. Afterwards, an introduction on the related research work will be provided. In the late section of this chapter, we will show that there exists a tradeoff between hidden and exposed nodes.

2.1 MAC Protocols for Wireless Networks

For single channel wireless networks, the MAC protocols widely used in applications now include Aloha and CSMA/CA. IEEE 802.11 DCF [9] implements the CSMA/CA with the optional RTS/CTS frames and is the widely accepted standard. We will briefly describe these MAC protocols in this section.

2.1.1 Aloha

In 1970s, Aloha was originally developed in the University of Haiwaii for use with satellite communication systems in the Pacific [10]. This protocol applies the simple communication scheme.

The terminals will transmit packets immediately whenever they have a packet waiting. If the transmission is successful, the terminal will transmit the next packet or waits for the next arrival. If the frame does not reach the receiver, it will transmit the packet again after a random backoff. Therefore, the terminals behave in an uncoordinated manner in Aloha protocol. There are two categories of Aloha protocol, *pure* Aloha and *slotted* Aloha. In pure Aloha, the terminal may initiate transmission at any time. In slotted Aloha, a synchronous system, the time has been divided into time slots and the terminal will only start transmission at the beginning of a time slot.

Assuming the Poisson traffic, the slotted Aloha system can achieve a theoretical maximum throughput of 0.368 [13] in the single-hop network. However, when the network traffic increases, the throughput decreases. Neither can the scheme work well in multi-hop wireless network. As the terminals transmit packets blindly, Aloha greatly suffers from the hidden node problem, making the network inefficient.

2.1.2 CSMA/CA

Having realized the problem of Aloha, researchers developed CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) for performance improvement. This is a modification of *Pure* CSMA [12], which is originally used in wired network.

Unlike Aloha, CSMA/CA deploys so called 'Listening before Talking' scheme. The antenna of the transmitter measures the local channel power (*RSSI*, Received Signal Strength Index) and compares the value with a threshold. If the *RSSI* is larger than the threshold, the transmitter will assume a busy channel and experience a random backoff time. Otherwise, the transmitter judges an idle channel status and start transmission. This is the basic mechanism of CSMA/CA. CSMA/CA has several variations, including 1-*persistent*, *non-persistent* and *p-persistent* CSMA/CA [8]. A brief description of these

is given in Appendix A for reference.

In the wireless channel, the signal strength attenuates the power of distance, that is,

$$P_r(d) \propto \frac{1}{d^{\alpha}} \tag{2.1}$$

Therefore, the value of threshold in CSMA/CA determines a range inside which the active nodes will be detected by the transmitter. This range is named as *Carrier Sensing Range*, R_{CS}. Assuming the homogeneous case, all the terminals have the same threshold, i.e, the same carrier sensing range. This determines an inactive area within the R_{CS} of the transmitter, as the terminals within this range will detect the ongoing transmission, and thus backoff the potential transmission. This makes it possible for the transmitter to filter out some hidden nodes.

The threshold is a software-defined parameter, so it is tunable and influences the size of Carrier Sensing Range. This value has an important impact on the network performance which will be explored in details in the later chapters.

2.1.3 IEEE 802.11 DCF Standard

IEEE 802.11 is now the standard for wireless networks. It has two categories, PCF(Point Coordination Function) and DCF (Distributed Coordination Function), where IEEE 802.11 DCF is widely accepted as the standard for Ad Hoc Networks. In the MAC design, IEEE 802.11 DCF employs CSMA/CA with optional RTS/CTS frames, or *Virtual Carrier Sensing*. This is basically a further attempt to mitigate the hidden node problem.

With the RTS/CTS frames implemented, the transmitter initiates an RTS frame (*Ready To Send*) to the receiver when it finishes the channel sensing process. Thus, the receiver replies with a CTS frame (*Clear To Send*). Afterwards, the transmitter starts

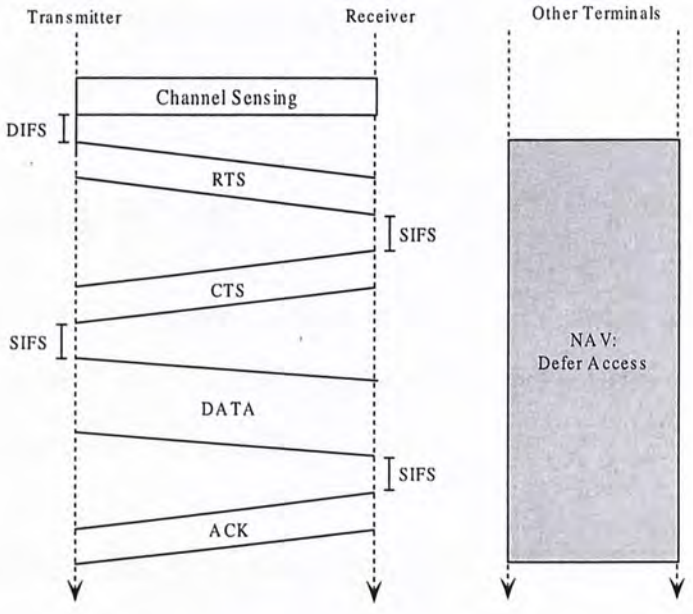


Figure 2.1: The Process of RTS/CTS Handshake

the real data frame transmission. In addition to the handshaking function, RTS/CTS frames will also inform the recipients of keeping inactive during the incoming transmission period. The frames do this by updating *NAV* (Network Allocation Vector) of the terminals, specifying the duration they need to keep silent. Thereby, the terminals in the transmission range of transmitter and receiver will keep silent within the predetermined period. This helps to ensure the incoming transmission. When the packet is received successfully, the receiver will reply with an ACK. Otherwise, if the ACK times out, the transmitter will assume a failed transmission and schedule a retransmission after a random backoff. IEEE 802.11 DCF applies *BEB* (Binary Exponential Backoff) Scheme. This together with other backoff schemes are described in Appendix B. Fig. 2.1 illustrates the whole process of transmission using IEEE 802.11 DCF.

The RTS/CTS handshake, or *Virtual Carrier Sensing* reduces the packet collisions to some extent. However, one problem of this scheme is the extra overheads it involves. This will become especially obvious when the traffic loading is high or the network

density is large. Moreover, it cannot completely remove all the hidden nodes. This will be explored in the following sections of this chapter.

2.2 Related Work

Hidden and exposed node problems have always been drawing researhers' attetention. Hereby, much research work has been performed to tackle these two problems. We will discussion some of these works in this section.

2.2.1 Schemes for Hidden Node Problem

For the hidden terminal problem, the CSMA/CA is one of the early attempts to reduce packet interferences. But, this protocol cannot remove the hidden terminal thoroughly. *BTMA* (Busy Tone Multiple Access) was proposed in [7]. A separated channel is applied to signal the transmission process. However, this protocol was basically designed for station-based networks, where a centralized base station serves several mobile hosts. Hence, it is not suitable for distributed Ad Hoc networks.

Zygmunt Haas developed a protocol called *DBTMA* [14] (Dual Busy Tone Multiple Access) based on *BTMA*. This protocol can be applied on the Ad Hoc network. Simulation work performed by the proposer shows the superiority to the original RTS/CTS MAC schemes. Nevertheless, it requires two separated channels in addition to the data transmission channel. This design involves extra cost.

In [18], the authors also proposed a scheme to eliminate the hidden nodes. The protocol is based on CSMA/CA with RTS/CTS and limits the distance between transmitter and receiver to $d \leq \frac{1}{\sqrt[\alpha]{SNR_{Th}}} R$. From Eq. 1.1, the interference range $R_I \leq R$, so the CTS frame can cover the whole interference range and eliminates the hidden terminals. The protocol limits the distance by power control, that is, only if the re-

ceived power of RTS is higher than a threshold (indicating the distance is small than $\frac{1}{\sqrt[\alpha]{SNR_{Th}}}R$) will the receiver reply a CTS frame. One problem is that the power attenuation can hardly be that accurate in practical applications. And another problem is that the reduced connectivity may result in multihop transmission, and thus more overheads are involved. Moreover, more exposed nodes will appear because of the numerous RTS/CTS frames.

2.2.2 Schemes for Exposed Node Problem

For the exposed terminal problem, one approach is to apply directional antennae [15] [16] so that protocols can selectively notify the terminals to keep silent. The obvious disadvantage of this is the extra hardware implementation cost. Another problem is the complex algorithms are needed to enable the transmitter make the right selection.

In [19], the authors suggest dealing with exposed terminal problem by timing control. In the proposed scheme, an exposed node is allowed to transmit if the transmission time needed for the head of line packet in the backlog is smaller than the remaining time of the ongoing transmission. The terminal can recognize itself as an exposed node by the sequence of packets it received, i.e., RTS followed by DATA frame.

The scheme does improve the channel utilization to some extent, but it also has potential problems. This scheme requires time synchronization, which is relatively hard to achieve in distributed Ad Hoc networks. Moreover, it is, as the proposer stated, an opportunistic algorithm. The channel utilization can be increased only when the exposed terminal happens to have packets that satisfy the above requirements.

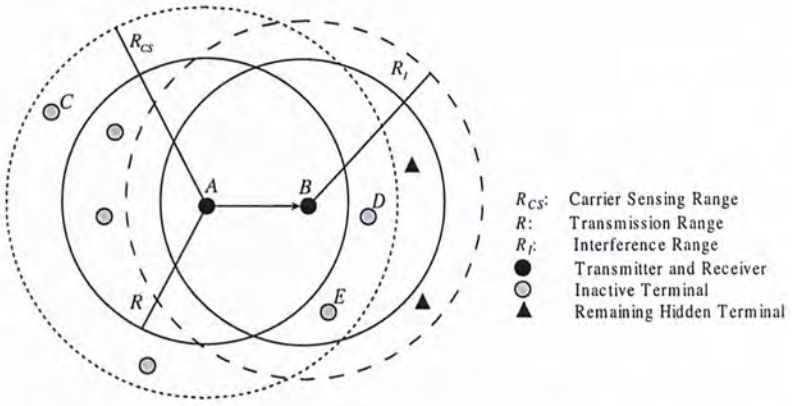


Figure 2.2: Hidden and Exposed Node in CSMA/CA

2.3 Tradeoff between Hidden and Exposed Nodes

In the last section, we have shown several schemes aimed at solving the hidden and exposed nodes. However, we can observe that most of these schemes usually solve one of the two problems, but making the other one worse or sacrificing other aspects of the network, such as, simplicity, connectivity and etc. This indicates a tradeoff between hidden and exposed node problem. In this section, we will explore the tradeoff.

In Aloha, all the terminals will not care the status of other terminals and will transmit the packets immediately whenever they have backlog. All the terminals are hidden to each other [22]. On the other hand, as there is no collision avoidance mechanism, no nodes are required to keep silent. As a result, in Aloha, there are lots of hidden nodes although no exposed terminal exists.

When CSMA/CA is developed, the carrier sensing range defines an inactive area in the homogeneous case (the terminals have the same R_{CS}), and thus mitigates some hidden terminals, e.g., terminal D, E. Albeit, some exposed terminals appears due to the R_{CS}. As shown in Fig. 2.2, some original hidden nodes have become inactive nodes. However, terminal C is beyond the inference range of the receiver B, but is

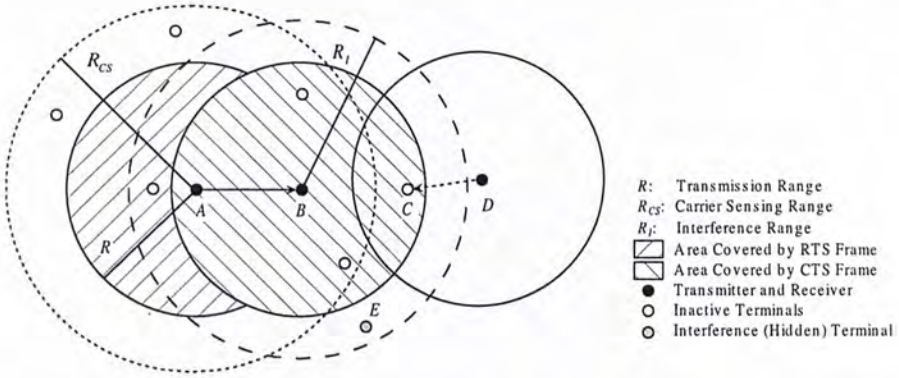


Figure 2.3: Hidden and Exposed Nodes in CSMA/CA with RTS/CTS

forced to keep silent. Hereby, it has become an exposed node and resulted in spatial wastes. Therefore, CSMA/CA brings in exposed nodes while removing some hidden nodes.

CSMA/CA was optionally implemented with RTS/CTS frames in IEEE 802.11 DCF standard. The RTS/CTS handshake keeps the terminals in the vicinity of transmitter and receiver silent to ensure the ongoing transmission. However, this mechanism still fails to eliminate the hidden node. Moreover, it involves more exposed nodes due to the CTS frames. This has been illustrated in Fig. 2.3. As the CTS frame is initiated by the receiver, it can only cover the transmission range R of the receiver. Some hidden node for example, terminal E, may remain in the interference range. Meanwhile, terminal C is an exposed node due to the CTS frame, as it cannot receive the transmission from terminal D for the moment.

In [18], the author shows that the hidden nodes can be completely eliminated by a large R_{CS} in the homogeneous case. That is, the R_{CS} covers the whole interference range, then we have,

$$R_{CS} = R + \sqrt[\alpha]{SNR_{Th}}R \tag{2.2}$$

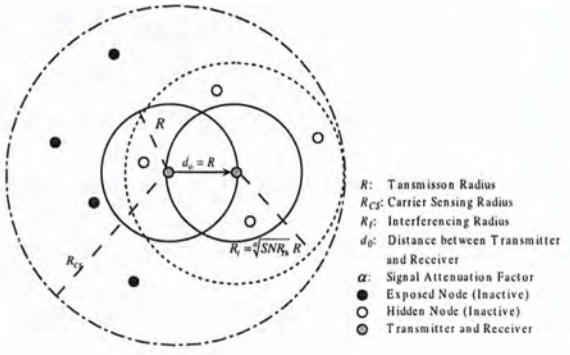


Figure 2.4: Carrier Sensing Range Covering the Whole Interference Range

This has been illustrated in Fig. 2.4. The whole interference range has been covered, thereby, there is no hidden terminal. On the other hand, we can observe that lots of exposed terminals come into existence due to the large inactive area. In summary, the CSMA/CA with large R_{CS} has a poor spatial reuse despite its effect in eliminating hidden nodes.

Therefore, there is an obvious tradeoff between hidden and exposed terminals on the track of MAC protocol development. Researchers are trying to solve the hidden hidden whilst the exposed terminal problem is becoming more severe. This process can be summarized by Fig. 2.5.

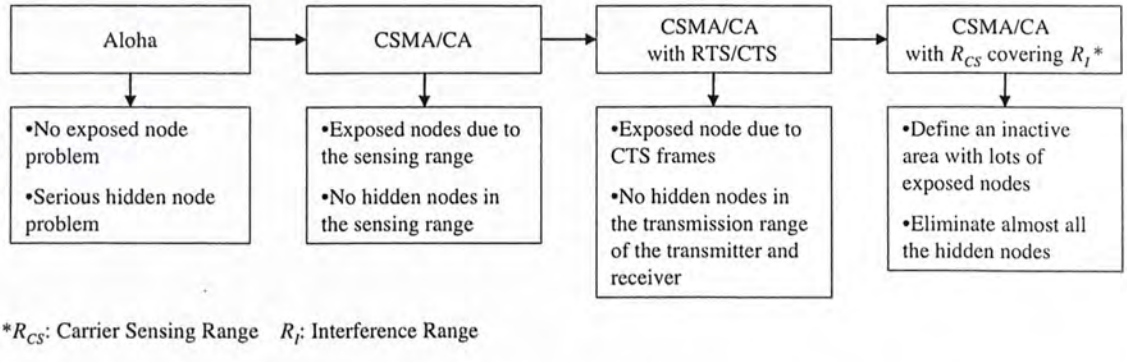


Figure 2.5: Tradeoff between Hidden and Exposed Terminals

2.4 The Effect of Carrier Sensing Range

In the last section, we have observed that the large R_{CS} (covering the whole interference range) can be used to completely eliminate the hidden nodes despite the exposed terminals. On the other hand, in Aloha, no exposed terminal exists and all the terminals are hidden to each other. In this case, the terminals have no sensing range, i.e., $R_{CS} = 0$. Obviously, the value of R_{CS} can play a critical role in balancing the two problems.

Assuming the uniform density of the terminal distribution, the expected number of inactive terminals is proportional to ${R_{CS}}^2$. There can be either potential interference terminals to the ongoing transmission or normal terminals among these terminals. By making the interference terminals inactive, the hidden nodes are removed while by making the normal terminals inactive, the exposed node problem becomes worse. In this point of view, the larger the carrier sensing range, the less hidden nodes and the more exposed nodes there will be and vice versa. This factor gives the idea to balance hidden and exposed problem using carrier sensing range coordination. Two schemes have been proposed in this thesis, which will be presented in Chapter 4.

Both hidden and exposed nodes can have an influence on the throughput of the network. In Chapter 3, we will present a mathematical analysis on the effect of carrier sensing range in CSMA/CA in terms of the relationship between throughput and carrier sensing range.

Chapter 3

Analysis on Carrier Sensing Range

In this chapter, we will deal with the analysis of carrier sensing range, especially its influence on the terminal throughput. In view of the analytical results, we will discuss the need of new MAC schemes in the later sections of this chapter.

3.1 Analysis Model

Before the detailed derivation, the analysis model is presented in this section, which is based on [20]. In the model, the terminals apply *non-persistent* CSMA/CA with *Geometric Backoff*. The model description includes four aspects: terminal configurations, timing/packet parameters, protocol approximation and throughput measurement.

3.1.1 Terminal Configurations

We assume the terminals in the network are homogenous, hence they all have the same transmission power P_t, transmission range R and carrier sensing range R_{CS}. The packet decoding SNR threshold, SNR_{Th} is $10dB$. To ensure the packet reception, we

can have,

$$SNR = \frac{P_t}{r^\alpha} / \frac{P_t}{{D_I}^\alpha} \geq SNR_{Th} = 10dB \tag{3.1}$$

where $\alpha = 4$ is the *path loss factor*; r is the distance between transmitter and receiver and D_I is the distance of the receiver from the interference node. Therefore, we get $D_I \geq 1.778r$, where $R_I = 1.778r$ is the interference range for receivers. The active nodes within this range may affect the packet reception. Obviously, the maximum value for R_I is $1.778R$ when $r = R$.

The network is located on an infinite plane and the terminals are distributed according to *Spatial Poisson Process* with the density $\lambda(nodes/m^2)$. Thus, $P_A(i)$, the probability of finding i nodes in an area of A is given by,

$$P_A(i) = \frac{e^{-\lambda A}(\lambda A)^{-i}}{i!} \tag{3.2}$$

Further, $N = \lambda \pi R^2$ is the expected number of nodes within the transmission range of a certain node.

3.1.2 Timing/Packet Parameters

The time slot length is represented by T which is a unit time length. We also define a concept called *mini slot*, a, as the propagation delay. It approximately equals the time needed for the signal to propagate from the transmitter to the margin of R_{CS}. It is a very small value and has been normalized by T, particularly, we take $a = 0.001T$ in the analysis.

We assume all the packets transmitted have the same length. It takes four time slots, i.e., $4T$ to process a packet. The timing/packet parameters can be illustrated by Fig. 3.1.

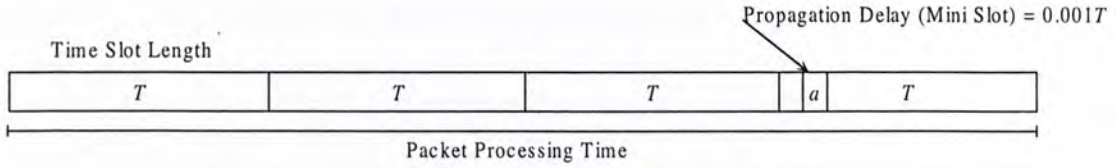


Figure 3.1: Diagram for Timing/Packet Parameters

3.1.3 Protocol Approximation

We approximate the *non-persistent* CSMA/CA with *Geometric Backoff* in the analysis. The terminals are assumed to have the same traffic loading. We confine the following configurations to approximate the protocol

- Each terminal senses the channel with probability $p_0 \leq 1$ at the beginning of a mini slot a, attempting to transmit packets.
- On average, a terminal senses the channel m times in a time slot T.
- $m = \frac{p_0 T}{a}$ is the channel sensing rate $(times/slot)$.
- A terminal starts to transmit only when it senses an idle channel state.
- Let $p_0' \leq 1$ denote the probability that a terminal starts real transmission at the beginning of mini slot, then,

$$\begin{aligned} p_0' &= Pr\{\text{A Terminal Starts Actual Transmission}\} \\ &= Pr\{\text{Senses the Channel}\} Pr\{\text{Idle Channel State}\} \\ &= p_0 P_I \end{aligned} \tag{3.3}$$

- Similarly, $m_0 = \frac{p_0' T}{a}$ is the actual transmission rate $(times/slot)$.
- The sender knows the transmission result immediately (success or failure).

- After a transmission, the transmitter is requested to keep silent for a mini slot.

The timing diagram in Fig. 3.2 illustrates the channel states experienced by a certain terminal, A, which is within the sensing range of the transmitter, during a successful packet transmission. Suppose terminal A is always listening. This diagram helps specify the protocol approximation in the analytical model.

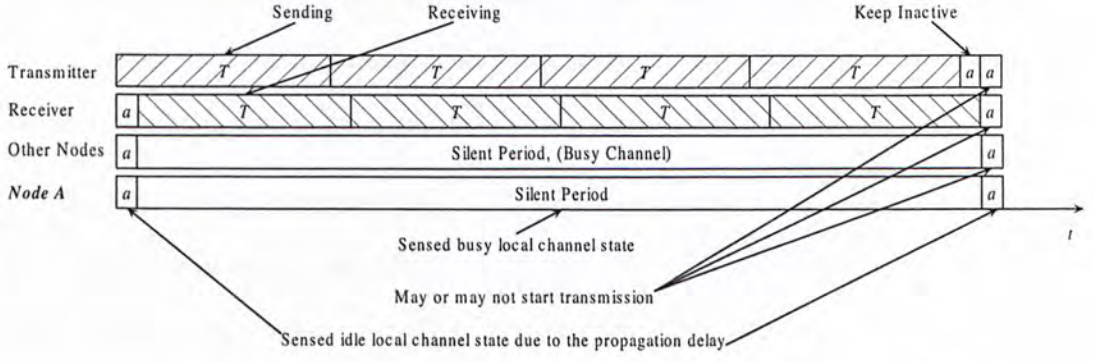


Figure 3.2: States Experienced by Node A

3.1.4 Throughput Measurement

A terminal is equally likely to send packets to the other terminals within the transmission range R, i.e., the nodes that are directly connected to the transmitter. Based on this assumption, we derive the average *one-hop* throughput. It is defined as [20] the average number of *successful* transmissions per time slot T of a terminal.

3.2 Derivation of Throughput

In this section, we derive the relationship between *one-hop* throughput and carrier sensing range based on the model presented. In CSMA/CA, the terminal only starts to transmit when it senses idle channel state, hereby we will calculate the idle channel

probability by channel modeling and then find out the successful fraction of transmitted packets.

3.2.1 Channel Modeling

The local channel state of a certain terminal basically includes the busy and idle states [21] when it keeps sensing the channel. '*Busy*' indicates it senses some terminal is transmitting and '*Idle*' means the local channel power is lower than the threshold. These two states are approximated by a *Markov Chain* shown in Fig. 3.3.

The idle channel probability is, hence, the limiting probability of *Idle* state P_I. According to protocol specification in section 3.1.3, the transmitter is requested to keep silent for a mini slot a after the transmission finishes. Hence, we can get the transition probability $P_{BI} = 1$. In the idle state, if no terminals within R_{CS} starts transmission in current mini slot, then the next mini slot is still in idle. Otherwise, the channel enters the busy state. As the terminals are distributed according to *Spatial Poisson Process* in the plane and the actual transmission probability in a mini slot is p'_0, we can get,

$$P_{II} = Pr\{\text{No nodes within } R_{CS} \text{ start transmission in this mini slot}\}$$

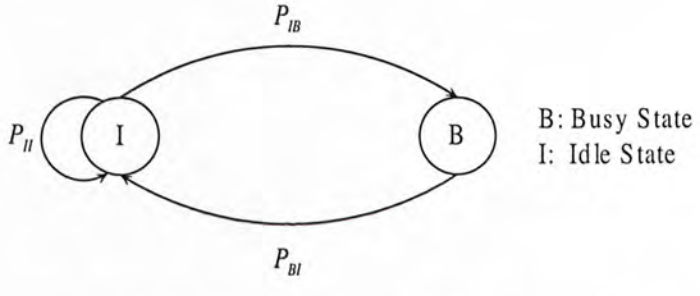


Figure 3.3: Markov Chain of the Channel State

$$
\begin{aligned}
&= \sum_{i=0}^{+\infty} Pr\{\text{No nodes start transmission}|i \text{ nodes in } R_{CS}\} Pr\{i \text{ nodes in } R_{CS}\} \\
&= \sum_{i=0}^{+\infty} (1-p_0')^i \cdot \frac{e^{-\lambda\pi {R_{CS}}^2} (\lambda\pi {R_{CS}}^2)^i}{i!} \\
&= e^{-p_0'\lambda\pi {R_{CS}}^2} \qquad (3.4)
\end{aligned}
$$

And,

$$P_{IB} = 1 - P_{II} = 1 - e^{-p_0'\lambda\pi {R_{CS}}^2} \qquad (3.5)$$

With the knowledge of transition probabilities P_{BI}, P_{II} and P_{BI}, we can derive the expected time in state B and I and in turns, the limiting probability P_I.

From Fig. 3.2, we know the expected time in B is $E[B] = 4T$. For $E[I]$, it can be calculated by,

$$
\begin{aligned}
E[I] &= \sum_{k=1}^{+\infty} (k \text{ idle mini slots}) \cdot Pr\{\text{idle for } k \text{ mini slots}\} \\
&= \sum_{k=1}^{+\infty} ka \cdot (P_{II})^{(k-1)} P_{IB} \qquad (3.6)
\end{aligned}
$$

Substitute with Eq. 3.4 and 3.5, we obtain,

$$E[I] = \frac{a}{1 - e^{-p_0'\lambda\pi {R_{CS}}^2}} \qquad (3.7)$$

Therefore, the limiting probability is given by,

$$P_I = \frac{E[I]}{E[I] + E[B]} = \frac{a}{a + 4T(1 - e^{-p_0'\lambda\pi {R_{CS}}^2})} \qquad (3.8)$$

3.2.2 Actual Transmission Rate

We have obtained the limiting probability of *idle* state. The next step is to derive the average number of transmissions of a terminal in each time slot T. This is defined as m_0 in section 3.1.3. By Eq. 3.3, the actual transmission probability p_0' is,

$$p_0' = p_0 P_I = \frac{a p_0}{a + 4T(1 - e^{-p_0' \lambda \pi {R_{CS}}^2})} \tag{3.9}$$

We know $p_0 = \frac{am}{T}$, $p_0' = \frac{am_0}{T}$ and a is very small. Hence, when $a \to 0$, approximately,

$$m_0 = m P_I = \lim_{a \to 0} \frac{am/T}{a + 4T(1 - e^{-a\lambda\pi {R_{CS}}^2 m_0/T})} \tag{3.10}$$

By some manipulations,

$$m_0 = \frac{\sqrt{T^2 + 16T\lambda\pi {R_{CS}}^2 m} - T}{8T\lambda\pi {R_{CS}}^2} \tag{3.11}$$

This equation relates the actual transmission rate m_0 with the channel sensing rate m and represents the average number of transmissions of a terminal within a time slot T. The *one-hop* throughput is, thus, the successful fraction of m_0. That is, we need to derive the successful transmission probability P_s.

3.2.3 Case One

The successful transmission probability p_s is dependent on the value of R_{CS} and r, the distance between transmitter and receiver, as they determine the existence of hidden nodes. The first case is that R_{CS} has covered the whole interference range. In this case,

$$0 < r < \frac{R_{CS}}{1 + (SNR_{Th})^{1/\alpha}} \tag{3.12}$$

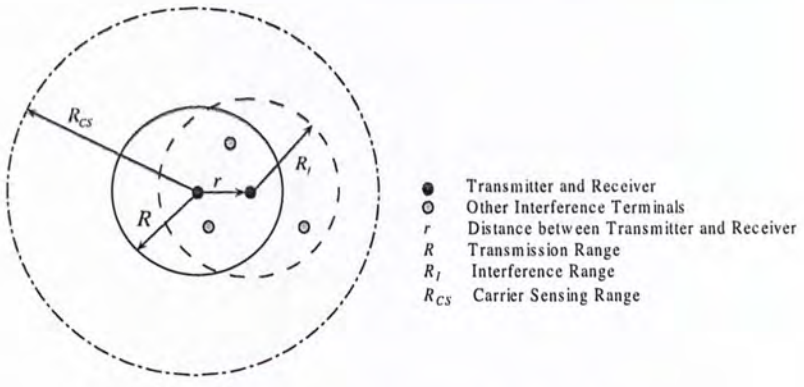


Figure 3.4: Illustration of Case One

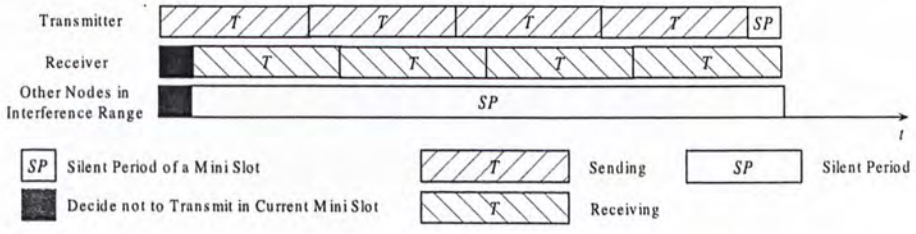


Figure 3.5: Successful Transmission Timing Diagram for Case One

where $SNR_{Th} = 10dB$. And this can be illustrated by Fig. 3.4. In this situation, all the interference nodes have been covered by carrier sensing range. No hidden nodes exist, so the packets will not be corrupted during transmitting process.

The timing diagram shown in Fig. 3.5. describes the situation when the packet transmission is successful in case one. From this diagram, the conditional successful transmission probability under case one is,

$$p_s = Pr\{\text{successful transmission}\} = P_1 \cdot P_2 \tag{3.13}$$

where,

P_1 = $Pr\{$the receiver does not start transmission in current mini slot$\}$

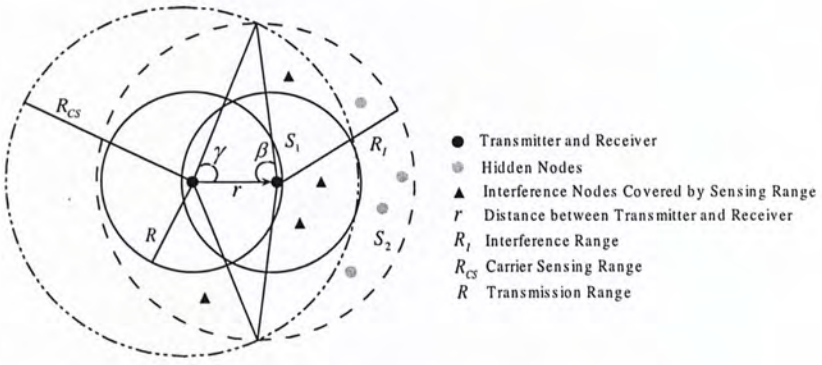


Figure 3.6: Illustration of Case Two

$$= 1 - p_0' \tag{3.14}$$

$$\begin{aligned} P_2 &= Pr\{\text{no other nodes within } R_I \text{ start transmission in current mini slot}\} \\ &= \sum_{i=0}^{+\infty} Pr\{\text{No nodes start transmission}|i \text{ nodes in } R_I\} Pr\{i \text{ nodes in } R_I\} \\ &= e^{-p_0' \lambda \pi {R_I}^2} \end{aligned} \tag{3.15}$$

In summary, the successful transmission probability for case one is,

$$p_s = (1 - p_0') e^{-p_0' \lambda \pi {R_I}^2} \tag{3.16}$$

3.2.4 Case Two

The second case happens when some hidden nodes exist during the transmission. Meanwhile, R_{CS} covers only part of the interference range. That is,

$$r \geq \frac{R_{CS}}{1 + (SNR_{Th})^{1/\alpha}} \tag{3.17}$$

Fig. 3.6 shows this situation. We denote the part of interference range that has been covered by R_{CS} as $S_1(r)$ and other part as $S_2(r)$. Both area sizes are the functions of

r. By *Geometry* calculations,

$$S_1(r) = \beta {R_I}^2 + \gamma {R_{CS}}^2 - R_I r \sin\beta \tag{3.18}$$

$$S_2(r) = \pi {R_I}^2 - S_1(r) \tag{3.19}$$

where,

$$\beta = \arccos\left(\frac{r^2 + {R_I}^2 - {R_{CS}}^2}{2rR_I}\right) \quad \text{and} \quad \gamma = \arccos\left(\frac{r^2 + {R_{CS}}^2 - {R_I}^2}{2rR_{CS}}\right)$$

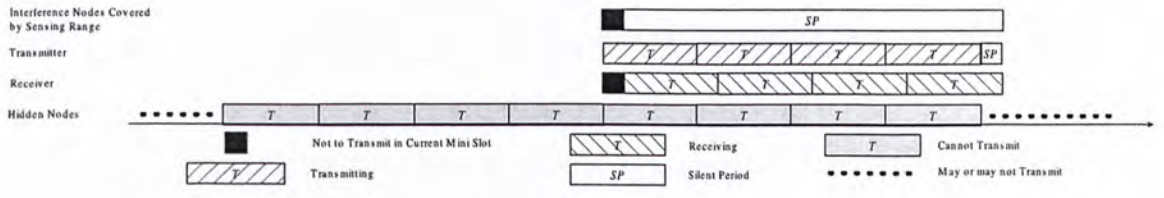


Figure 3.7: Successful Transmission Timing Diagram for Case Two

In $S_1(r)$, the interference nodes will keep inactive during the transmission as in case one. On the other hand, the nodes in $S_2(r)$ may initiate transmissions and corrupt the packet reception. Therefore, those nodes are hidden nodes. To ensure the current transmission successful, these nodes cannot transmit in the previous and following $4T$ of the current transmission starting time. The timing diagram in Fig. 3.7 further explains this, showing the condition of successful transmission. Under case two, the conditional successful transmission probability can be derived by,

$$p_s = Pr\{\text{Successful Transmission}\} = P_A P_B P_C \tag{3.20}$$

And,

$$\begin{aligned} P_A &= Pr\{\text{The receiver does not initiate transmission in this mini slot}\} \\ P_B &= Pr\{\text{Other nodes in } S_1(r) \text{ does not start to transmit in this mini slot}\} \\ P_C &= Pr\{\text{Nodes in } S_2(r) \text{ does not transmit in previous and following } 4T\} \end{aligned}$$

P_A is easy to get. P_B and P_C can be calculated by the property of *Spatial Poisson Process*. Hence, we can get,

$$P_A = 1 - p_0' \qquad P_B = e^{-\lambda S_1(r) p_0'} \qquad P_C = e^{-8\lambda p_0' S_2(r) \frac{T}{a}} \tag{3.21}$$

Combining them together, the successful transmission probability of case two is obtained, which is shown as follows.

$$p_s = P_A \cdot P_B \cdot P_C = (1 - p_0')\, e^{-\lambda S_1(r) p_0'} e^{-8\lambda p_0' S_2(r) \frac{T}{a}} \tag{3.22}$$

3.2.5 Mathematical Form of Throughput

Given the successful transmission probability in the last two sections, we will derive the mathematical form of *one-hop* throughput in this section. The throughput is represented in terms of packets per time slot, which has the length of T.

According to the previous analysis, the successful transmission probability is conditioning on r, the distance between transmitter and receiver. Therefore, the overall probability P_s should be dependent of the distribution of r. To derive this, we need to

have the cumulative distribution function $F(r)$ of r.

$$F(r) = Pr\{\text{Distance} < r\} = Pr\{\text{Select a node within range } r\}$$

From the *Spatial Poisson Distribution* of the terminals,

$$F(r) = \frac{E[\text{Select a node within range } r]}{E[\text{Select a node within transmission range } R]} = \frac{\lambda\pi r^2}{\lambda\pi R^2} = \frac{r^2}{R^2} \tag{3.23}$$

where $0 \leq r \leq R$ The probability density function $f(r)$ of r is the first order differentiation of $F(r)$.

$$f(r) = \frac{dF(r)}{dr} = \frac{2r}{R^2} \qquad 0 \leq r \leq R \tag{3.24}$$

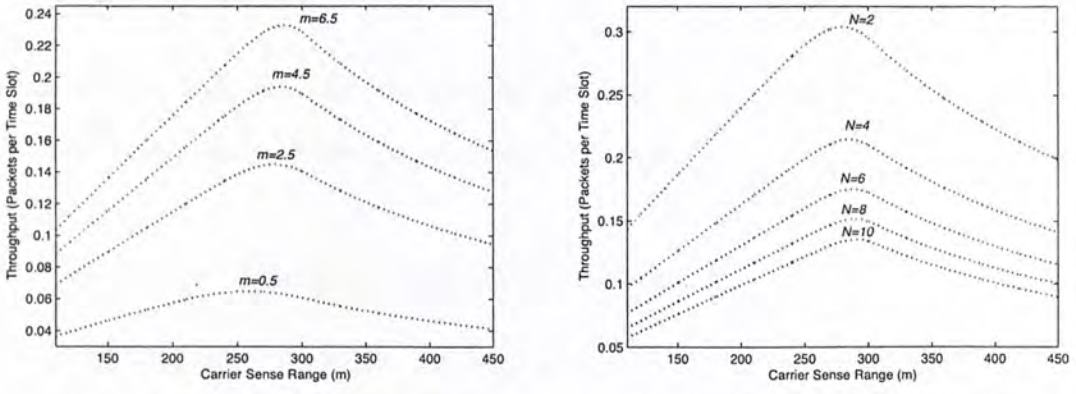
With the PDF of r, we can obtain the successful fraction of m_0, actual transmitted packets per time slot. This is exactly the *one-hop* throughput, ρ.

$$\begin{aligned} \rho &= m_0 \cdot P_s \\ &= m_0 \int_0^R f(r) p_s dr \end{aligned} \tag{3.25}$$

Substitute with Eq. 3.16, 3.22 and 3.24, the final form of ρ is,

$$\rho = \frac{m_0}{R^2}\left(\int_0^{\frac{R_{CS}}{1+10^{1/\alpha}}} 2r(1-p_0')e^{-p_0'\lambda\pi {R_I}^2} dr + \int_{\frac{R_{CS}}{1+10^{1/\alpha}}}^{R} 2r(1-p_0')e^{-\lambda S_1(r)p_0'} e^{-8\lambda p_0' S_2(r)\frac{T}{\alpha}} dr\right) \tag{3.26}$$

This gives the non-closed mathematical form of throughput. Using this equation, we can derive the relationship between carrier sensing range and *one hop* throughput.



(a) Under Different Sensing Rate (b) Under Different Node Density

Figure 3.8: Carrier Sensing Range vs. Throughput

3.2.6 Analysis Results

The Eq. 3.26 is not a closed form integration, but the numerical results can be obtained with the aid of computers. When $R = 110m$, $\alpha = 4$ and $T = 1$, the curves of the relationship between R_{CS} and ρ are plotted in Fig. 3.8.

Fig. 3.8(a) shows the relationship under different sensing rate m $(times/slot)$, where N the node density—expected number of terminals within the transmission range is 4. Fig. 3.8(b) represents the cases of different node densities and $m = 5.5$ in this figure. From both figures, we can find the result basically agrees with the intuitions. With homogeneous node assumptions, the *one-hop* throughput first increases as R_{CS} is increasing and keeps removing the hidden nodes. And then, the throughput begins to decrease when the more and more exposed nodes appears. This indicates the existence of an optimal sensing range R_{CS}. Besides, other factors like sensing rate, node density and etc., also affect the optimal R_{CS}. In summary, this analysis gives a direct reference on the relationship between carrier sensing range and throughput in CSMA/CA MAC protocol.

3.3 Implications

In this section, we will show the implications of the previous analysis on MAC protocol and discuss the necessity of new MAC protocol designs.

3.3.1 Value of Sensing Range in CSMA/CA

In [18], it is suggested that the hidden nodes can be removed by large R_{CS} in CSMA/CA. Nevertheless, the previous analysis demonstrated that the optimal performance cannot be achieved by this approach.

Fig. 3.8 indicates that there exists an optimal carrier sensing range under the homogenous terminal assumption. Referring to the figure, we find that the optimal R_{CS} are less than $300m$ despite some minor factors that may affect this value. On the other hand, the interference range R_I is $\sqrt[\alpha]{SNR_{Th}}r$ where r is the distance between transmitter and receiver. Hence, to ensure the hidden nodes are eliminated, we should have, ($R = 110m$, $\alpha = 4$ and $SNR_{Th} = 10dB$)

$$R_{CS} = R + \sqrt[\alpha]{SNR_{Th}}R = 305.58m \tag{3.27}$$

This value is larger than the optimal R_{CS} shown in Fig. 3.8. This is because too many exposed nodes have appeared and resulted in a poor spatial reuse when all the hidden nodes are removed by R_{CS}. The issue can be illustrated by Fig. 3.9, where we can observe lots of exposed nodes due to the large R_{CS}.

Therefore, the key issue here is to balance the hidden and exposed terminals instead of eliminating the hidden terminals. In conclusion, in CSMA/CA, the desirable performance can be achieved with the existence of hidden terminals.

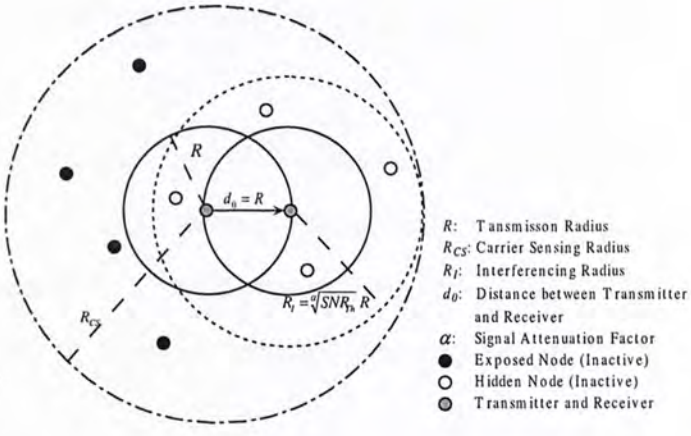


Figure 3.9: The Effect of Large Carrier Sensing Range

3.3.2 Need for New MAC Protocols

The theoretical analysis suggests that the average good performance can be achieved by properly adjusting sensing range of CSMA/CA. However, the terminals are assumed to be homogenous in this analysis. This can hardly be the case in practice.

In the analysis model, all the terminals have the same traffic loading with the same transmitted packet size. And the terminals have the same CSMA/CA channel sensing rate. These assumptions can help to simplify the theoretical analysis, but it cannot happen in real application. Both the loadings and packet size of terminals can vary depending on the specific applications.

Moreover, the terminals in the network have unified distribution density λ in the network. This usually cannot hold in general cases. The uneven terminal density indicates the expected numbers of interference terminals faced by various transmitters are different. Other phenomena can also affect the local channel conditions of each terminal, like channel fading, mulit-path effect [8] and etc. Hence, the optimal sensing range derived in uniform density case may not apply here. In other words, we cannot apply the same configurations to all the terminals regardless the local conditions of them.

Nevertheless, the unified configurations have been adopted by most MAC protocols in use now.

Therefore, new schemes are needed to effectively coordinate the terminals in the network in practice. The MAC schemes should take the various local conditions into account. In the Chapter 4, we will propose two new MAC schemes to perform the terminal coordinations by adjusting the carrier sensing range.

Chapter 4

MAC Protocols by Congestion Control

We have performed the analysis on carrier sensing range and mentioned some issues regarding new MAC protocol design in the last chapter. In this chapter, we will propose two MAC schemes. The schemes adopt the congestion control mechanism to achieve fair channel resource allocation in the MAC layer.

4.1 Motivations and Principles

In this section, we will introduce the motivations and basic principle of the proposed MAC protocols. Our algorithms are the modifications of IEEE 802.11 DCF, but as the cases in most applications, they do not adopt the RTS/CTS frames . They are based on adjusting the threshold (sensitivity) of CSMA/CA.

4.1.1 Balancing Hidden and Exposed Nodes

The tradeoff between hidden and exposed nodes, as addressed in Chapter 2, indicates that it is difficult to mitigate two problems at the same time. Tons of researches have been performed to solve them, but according to our knowledge, there exists no elegant solutions to these problems. Most schemes to these problems, like [18], [22], [23] and etc.,usually solve only one of the two problems, but either making the other problem worse or sacrificing some other aspects of the network, such as, connectivity, simplicity and etc. Therefore, the key to the coordination is to balance them.

Among the basic parameters of IEEE 802.11 DCF, the carrier sensing range R_{CS} of CSMA/CA is a tunable parameter. In the CSMA/CA, the antenna will compare the local channel power with a threshold (or sensitivity) to decide whether the channel status is busy or idle. Hence, by adjusting this threshold, the carrier sensing range can be modified. A study on the carrier sensing range in balancing the hidden the exposed nodes has been performed in [18]. This work shows the effect of sensing range in balancing the hidden and exposed nodes.

Moreover, the theoretical analysis in the last chapter address the influence of carrier sensing range on *one-hop* throughput in details. The work shows there can exist an optimal R_{CS} under the homogenous assumption. These issues motivates us to use R_{CS} in CSMA/CA as the critical parameter to balance hidden and exposed nodes.

Based on this, we propose two MAC schemes with *self-adjusting* R_{CS}. The terminals with the schemes learn local channel condition to find a (sub)optimal R_{CS} and achieve better channel resource allocation.

4.1.2 Controlling Carrier Sensing Range

In CSMA/CA, the antenna compares the local channel power to a threshold to determine the channel status. The transmitted power attenuates with the distance in the wireless channel. The measured power P_r is particularly modeled by [8],

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^\alpha} \tag{4.1}$$

α is the path loss factor. d is the distance from the transmitter. P_t is the transmitted power. G_t and G_r are the antenna gains of the transmitter and receiver respectively. λ is the wavelength. When $P_r(d) \geq P_{th}$, the CSMA/CA threshold, the power will be detected by the antenna and the transmitter will be blocked. In other words, the R_{CS} can be given by,

$$R_{CS} = \sqrt[\alpha]{\frac{P_t G_t G_r \lambda^2}{P_{th}(4\pi)^2}} \tag{4.2}$$

This means that with the threshold P_{th}, the transmitting terminal at a distance of R_{CS} with power P_t will be detected by the local terminal. Hence, this equation defines the corespondency between the sensing range R_{CS} and the threshold P_{th}. The smaller the threshold is, the larger the sensing range will be.

4.1.3 Non-homogenous Sensing Range

In the theoretical analysis in the last chapter, all the terminals are assumed to have the same R_{CS}. However, in our the proposed MAC schemes, the terminals will adjust the R_{CS} according to their local environment. Therefore, the sensing range, in this case, are non-homogenous.

If the terminals are allowed to have different R_{CS}, the optimal R_{CS} will become case dependent. For example, in Fig. 4.1, to ensure the current transmission, the nodes

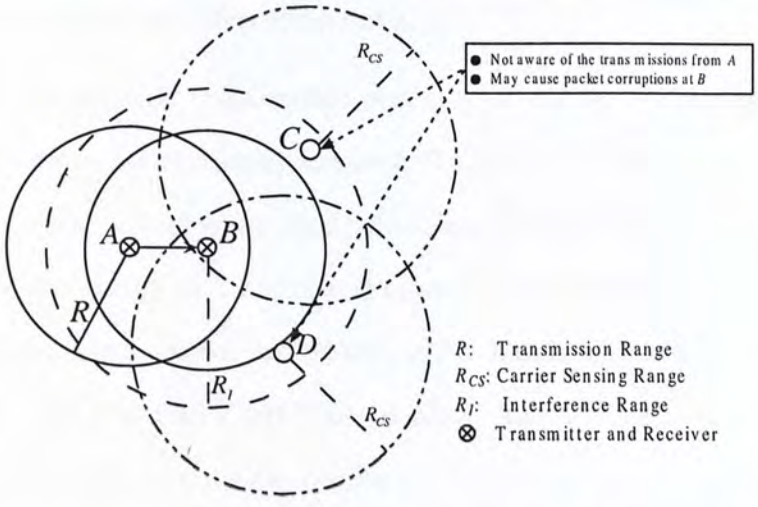


Figure 4.1: Carrier Sensing Range Coordination

C,D have to increase their sensing range to just cover the transmitter A. Clearly, the optimal R_{CS} depends on many factors, such as, relative location of the hidden nodes, the distance between transmitter, nearby terminal density and etc. If the sensing ranges are simultaneously optimized for each pair of transmitter and receiver, the hidden and exposed nodes can be ideally balanced.

The centralized control can be one option to coordinate the sensing ranges. In [24] and [25], the authors suggested using *GPS* (Global Positioning System) systems for coordination. However, this will cause high computation complexity and poor network scalability, not to mention the extra hardware cost involved.

An alternative approach is to apply distributed adaptive control, that is, each node adjusts the R_{CS} itself according to the current environment so as to find a (sub)optimal range. This approach can effectively reduce the algorithm complexity and enhance the network scalability. The two MAC protocols proposed in the thesis are based on this approach. A linear adaptive scheme was proposed in [31], but we will show this scheme does not work well in general cases in Chapter 5. This indicates that the simple

adaptive schemes are not effective enough.

We have investigated the tunable property of carrier sensing range in depth and found that there exists similarity between the sensing range and window size in TCP congestion control. Hereby, we model the R_{CS} as the congestion window and adaptively control the range in a manner similar to congestion control algorithms. These algorithms have been shown to achieve good bandwidth allocation in TCP protocols [26] [27]. And it turns out that in MAC layer, they also perform well, which is to be proven by the simulation results in Chapter 5.

4.2 Algorithm Descriptions

In this section, we will describe the algorithms for the MAC layer proposed in this thesis. The core concept is the modeling of R_{CS} to congestion window. Hereby, we propose *LDMI* (Linear Decreasing Multiplicative Increase) and *Tahoe* Controlling MAC protocols.

4.2.1 Core Concept

In CSMA/CA, the R_{CS} determines how conservative a terminal will behave. Assuming the uniform density of the network, a terminal with a larger sensing range will behave more conservative, as it has to , on average, take care of more nodes within the R_{CS}, and vice versa.

This is similar to that of TCP congestion control. In congestion control, each flow maintains a window size, which can be regarded as the transmitting rate. The larger the window size, the more aggressive it is. The flow will keep on increasing the window size when the transmitted packets are acknowledged. Once a transmission fails or traffic congestion occurs, the windows size will decrease (usually in a multiplicative

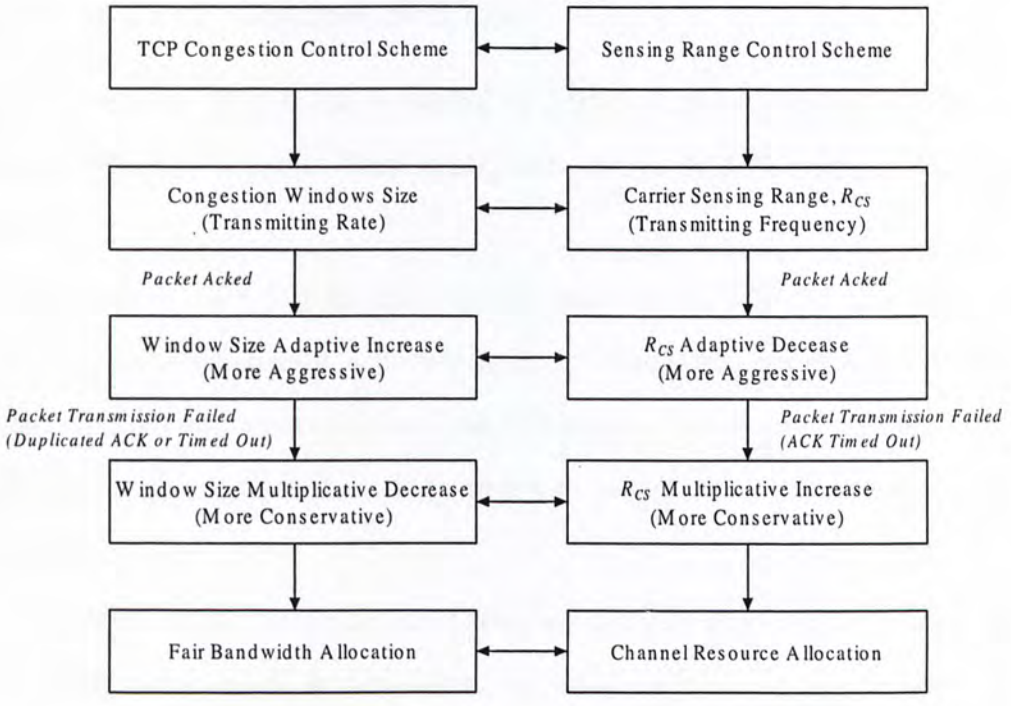


Figure 4.2: Modeling R_{CS} to Congestion Window

manner). The flow, thus, becomes conservative. This process performs iteratively and gradually realize the fair bandwidth allocation among the traffic flows. Some famous TCP congestion control schemes include *AIMD* [26] (Additive Increase and Multiplicative Decrease), TCP Tahoe [28],TCP Vegas [32] and etc.

In CSMA/CA, the same mechanism can be applied to achieve fair channel resource allocation. When the node is experiencing successful transmissions, it will reduce the sensing range, making the node more aggressive. As a packet failure occurs, it will increase the sensing range and behave more conservatively. So on and so forth, the terminal tries to adaptively determine a (sub)optimal R_{CS} with regard to the local condition. In this way, the overall fair channel resource allocation can be achieved. The modeling to R_{CS} can be summarized in Fig. 4.2.

4.2.2 LDMI Control Scheme

The first scheme we propose is named as *LDMI* (Linear Decrease and Multiplicative Increase) *Control Scheme*. This corresponds to the *AIMD* scheme in TCP congestion control.

All the flows start with the minimum window size$-1MSS$ (Maximum Segmentation Size [12]). For each packet acknowledged, the congestion window size is increased by a fixed step depending on the local configurations. This is known as additive increase. On the other hand, the congestion window is halved in case a transmission failure has occurred.

In *LDMI*, all the terminals start with a relatively large sensing range, denoted as R_{Top}. After a successful transmission, i.e., ACK received for the previous packet, the R_{CS} is decreased by δ. Once ACK is timed out, i.e., transmission failure, the sensing range R_{CS} will be increased by $(R_{Top} - R_{CS})/2$ which resemble halving the window size in TCP congestion control. In mathematical representation, let R_i denote the carrier sensing range after the ith transmission of a terminal, we can have For $i = 0$,

$$R_0 = R_{Top} \tag{4.3}$$

and for $i \geq 1$,

$$R_i = \begin{cases} R_{i-1} - \delta & \text{Previous Packet } ACK\text{ed} \\ \frac{R_{i-1}+R_{Top}}{2} & \text{ACK Packet Timed Out} \end{cases} \tag{4.4}$$

A track of R_{CS} in the terminal using *LDMI* is provided in Fig. 4.3 where $R_{Top} = 180.58m$ and $\delta = 15m$. The *LDMI Control Scheme* gives a proper modeling of R_{CS} to the *AIMD* mechanism.

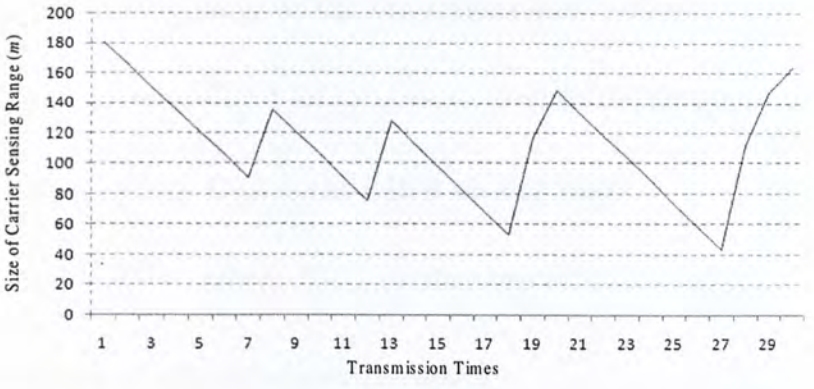


Figure 4.3: Track of Carrier Sensing Range in LDMI

4.2.3 Tahoe Control Scheme

Another famous congestion control scheme was proposed in [28], called *TCP Tahoe*. We have also imported it to the MAC layer and developed *Tahoe Control Scheme*.

In *TCP Tahoe*, the expansion of congestion window has two phases [28]. In phase I−slow start, the window goes through an exponential increase. When the size is larger than a threshold, it enters phase II−congestion avoidance, where additive increase is applied. Once a failure occurrs, the threshold becomes the half of the current window size while the window size is reduced to the minimum ($1MSS$). Afterwards, the flow applies the phase I again until the windows size is over the new threshold.

Similarly, we have two phases, exponential decreasing and linear decreasing, when R_{CS} is decreasing in *Tahoe Control Scheme*. In exponential decreasing, the terminal will reach the high share of channel resources quickly. When it enters the linear decreasing, it tries to stay on that high share as long as possible. The description is given as follows.

- Let R_i^k denote the sensing range of the ith consecutive successful transmission after the kth transmission failure.

- R^k is the sensing range at the kth transmission failure.
- Hereby, k increases by 1 and i is set to 0 when the transmission failure occurs.
- $R_0^k = R_{Top}$, where R_{Top} is the initial sensing range.
- $R_{Thres} = \frac{R^k + R_{Top}}{2}$, where R_{Thres} is the threshold.

During the series of successful transmissions,

$$R_i^k = \begin{cases} R_{Top} - \beta^i & 1 \leq i < \lceil log_\beta(R_{Top} - R_{Thres}) \rceil \\ R_{i-1}^k - \delta & i \geq \lceil log_\beta(R_{Top} - R_{Thres}) \rceil \\ 0 & R_{Top} - \beta^i < 0 \text{ or } R_{i-1} - \delta < 0 \end{cases} \tag{4.5}$$

where β is the exponential factor and δ is the linear decreasing step.

When transmission failure occurs,

$$R_0^{k+1} = R_{Top} \tag{4.6}$$

and the new threshold becomes,

$$R_{Thres} = \frac{R^{k+1} + R_{Top}}{2} \tag{4.7}$$

We have also provided a track of R_{CS} in *Tahoe Control Scheme* ($R_{Top} = 180.58m$, $\beta = 3$ and $\delta = 5m$) in Fig. 4.4 , where the two phases of sensing range decrease can be observed.

Both protocols are based on the modeling between carrier sensing range and TCP congestion control window. There can be other variations of these two MAC protocols just like the cases in TCP congestion control, such as TCP New Reno [29], TCP Hybia [30] and etc. The best TCP congestion control scheme has not appeared yet. Similarly,

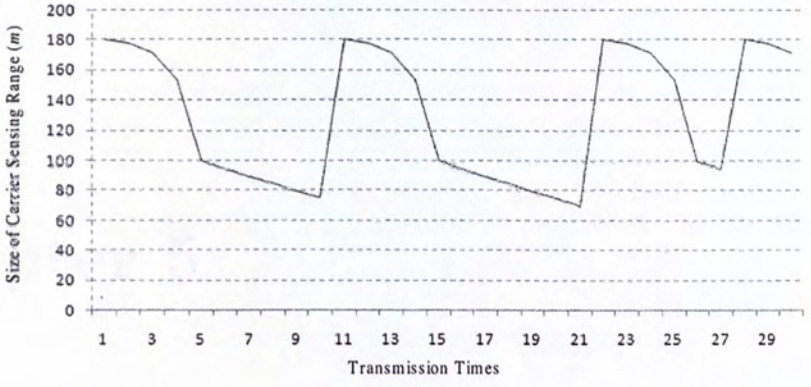


Figure 4.4: Track of Carrier Sensing Range in Tahoe

the optimal MAC protocol using this approach is yet to be discoverd. Nonetheless, the simulation analyses presented in the next chapter have already demonstrated the superiority of these two protocols, *LDMI* and *Tahoe*.

Chapter 5

Simulation Analysis

We have presented two MAC schemes by congestion control algorithms in the last chapter. In this chapter, we will demonstrate the superiority in the performance of these two via simulations. We perform this by the comparisons with the CSMA/CA in IEEE 802.11 DCF standard. The comparisons include *one-hop* throughput, fairness and throughput convergence speed.

5.1 Simulation Configurations

We conduct experiments on IEEE 802.11 DCF standard without RTS/CTS frames using *OMNet++* [33] and its *Mobility Framework* [34]. *OMNet++* is an open source discrete event simulator. It provides extensive models defined by C++ language and support of MAC layer protocols. Furthermore, the access to the model modifications provides the ease of new protocol implementations.

5.1.1 Geometric Burst Traffic Model

One of the critical issues in simulations is to make the model realistic. In practice, the traffic flows in the network usually appear in terms of traffic burst, that is, the generated traffic rate remains the same within a certain duration depending on the application. And then, the rate will alter after this burst ends. To emulate this network traffic characteristic, we propose a *Geometric Burst Traffic Model* in this section. The specification of the model is given as follows.

- The packets arrive at MAC layer in terms of bursts.
- During each burst, a packet is generated with probability p_0 in an application time slot, where we refer p_0 as the *traffic loading*.
- The packet will randomly choose a terminal within the transmission range as the destination.
- The terminals have the fixed packet destination, traffic loading and packet size within a burst.
- The burst length (in application layer time slots) is followed by a *Geometric* distribution with p, thus $1/p$ is the expected burst length.
- A different traffic burst will begin immediately after the current one ends.

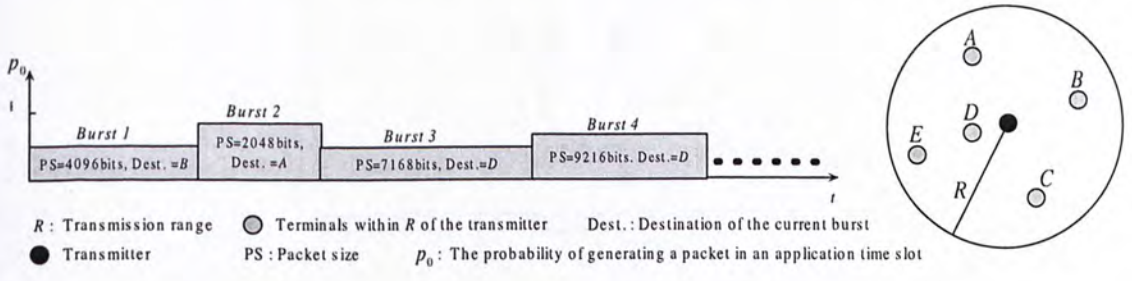


Figure 5.1: Illustration of Geometric Burst Traffic Model

Fig. 5.1 illustrates the traffic generated by this model. It helps generate traffic stream as in the real applications, and hence makes the simulation more practical. We will test the proposed schemes under this model.

5.1.2 Network Topology

For the network topology, the network is located on a $1000 \times 1000m^2$ playground, in the center of which we place 16 *Target Nodes* in a 4 by 4 grid-shape manner. The *Manhattan Distance* between targets nodes is set to be larger than the transmission range. The target nodes apply fixed traffic loading (say, generating a packet with fixed probability p' in each application time slot) and packet size (8192bits) in each run of the simulations. We then measure the average *one-hop* throughput of these 16 target nodes.

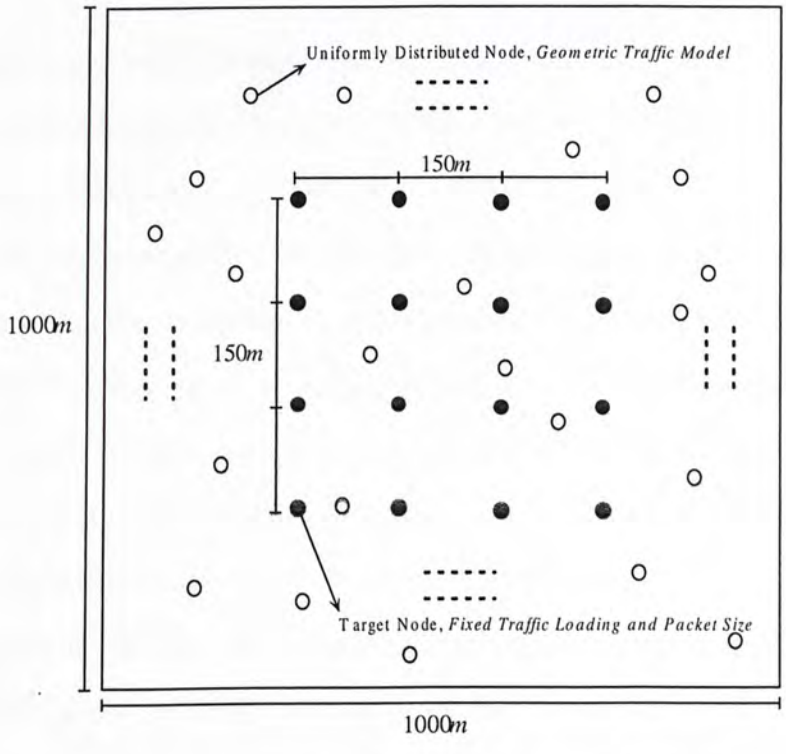


Figure 5.2: Network Topology in the Simulation

figurations, we will compare the performance of our schemes with the CSMA/CA in IEEE 802.11 DCF Standard.

5.2 Throughput Comparisons

We compared the *one-hop* throughput [20] of different MAC schemes in our simulations, that is, the average number of successful transmissions to the destination (a random terminal within the transmission range) in a second.

The first result is on *Linear Control Scheme*, which is described as follows.

$$R_i = \begin{cases} R_{i-1} - \delta & \text{Packet ACKed} \\ R_{i+1} + \delta & \text{ACK Timed Out} \\ 0 & \text{If } R_{i-1} - \delta \leq 0 \end{cases} \tag{5.1}$$

where R_i is the carrier sensing range after ith transmission. Hereby, R_{CS} will decrease or increase by a fixed value δ, depending on the success or failure of the transmission. This is a simple self-adjusting mechanism

According to the experimental results shown in Fig. 5.3(a) ($\delta = 15m$), the throughput performance is fairly unstable. At some loadings, the throughput exceeds that of the original CSMA/CA while at other loadings, it presents a poor performance. In the next section, we will see the cause of this situation is related to the fairness of channel resource allocation among the terminals. In a word, the *Linear Control Scheme* shows an unsatisfactory performance in the random topology.

Now, we present the throughput performance of the algorithms proposed in this paper. The throughput of *LDMI* is illustrated in Fig. 5.3(b) In the simulation, the *LDMI* algorithms has been specified by Eq. (4.3) and (4.4), where $R_{Top} = 180.58m$ and $\delta = 15m$. This time, the performance is stable at all the loadings, plus the throughput

In the surrounding of the target nodes, there are 190 nodes randomly distributed in the playground according to the *uniform* distribution. In the simulation, these terminals apply *Geometric Burst Traffic Model*, thus this creates a realistic and varying traffic environment. We will observe how well the target nodes perform using the proposed schemes under this condition. Fig. 5.2 gives the illustration of the network topology.

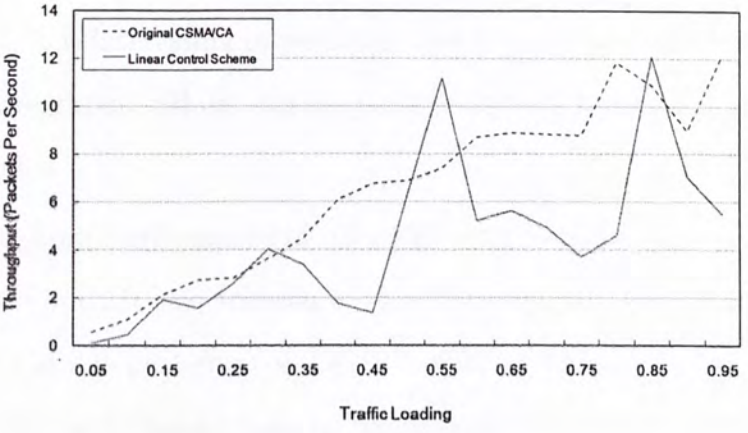
5.1.3 Simulation Parameters

The acknowledge mechanism and the backoff scheme are exactly the same as the CSMA/CA in IEEE 802.11 DCF. Other simulation parameters are summarized in Table 5.1

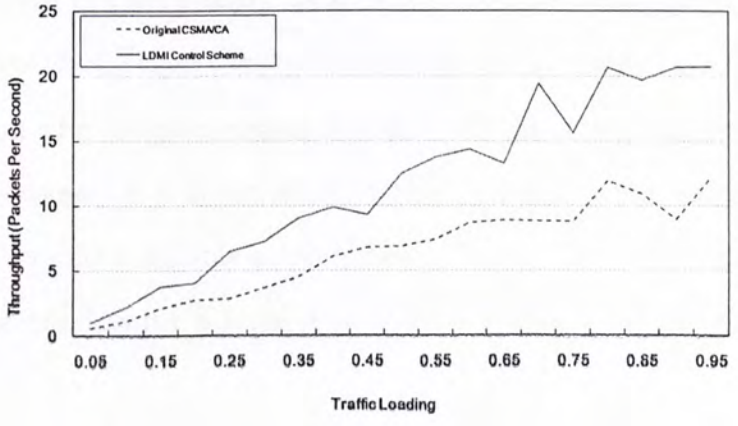
Playground Size	$1000 \times 1000m^2$
Number of Random Distributed Nodes	190
Number of Target Nodes	16
Manhattan Distance between Target Nodes	$150m$
Target Node Packet Size	$8192bits$
Path Loss Factor, α	4
SNR Decoding Threshold	$10dB$
Bit Rate	$11Mbps$
MAC Layer Time Slot Length	$20\mu s$
MAC Layer Header Size	$272bits$
Transmission Power	$3mW$
Transmission Range	$110m$
Initial Carrier Sensing Range	$180.58m$
Application Layer Time Slot Length	$2ms$
Average Burst Length	$8s$
Simulation Time	$900s$

Table 5.1: Simulation Parameters

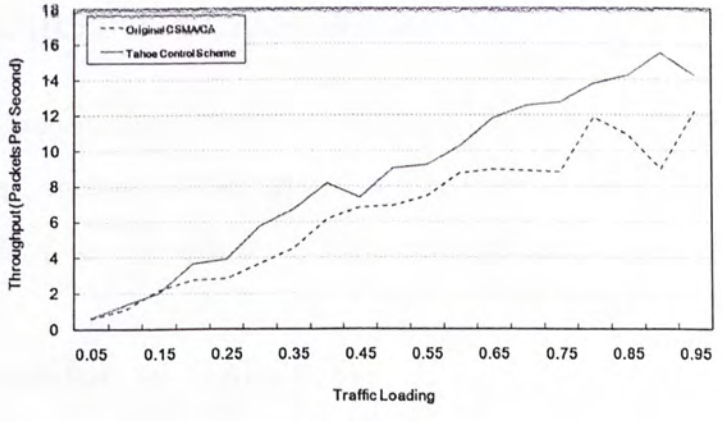
Note that the traffic loading is defined with reference to the application layer time slot, so the loading is not very high to the MAC layers. Using these simulation con-



(a) Linear



(b) LDMI



(c) Tahoe

Figure 5.3: Throughput Comparisons

is higher than the original CSMA/CA. This has demonstrated a great throughput improvement. It is interesting to point out that if we tweak the parameter δ to a larger value, the throughput will on average become higher. However, the performance will become unstable.

The throughput performance of *Tahoe Control Scheme* is presented in Fig. 5.3(c) ($\beta = 3$ and $\delta = 5m$). It also achieves a higher throughput than the original CSMA/CA and presents a stable performance, i.e., it has higher throughput at all loadings in our simulation. This is desirable, however, compared with *LDMI*, the throughput is a bit lower. This does not necessarily mean *Tahoe* is worse than *LDMI*. We will show the unique advantage of *Tahoe Control Scheme* in the following sections.

In addition, the two parameters, β and δ, will also affect the performance of *Tahoe Controlling Scheme*. If β is increased to large value, it will become more difficult for the terminal to find a feasible sensing range. Hence, the throughput will be lowered. On the other hand, with a large δ value, the throughput performance will become unstable.

5.3 Fairness Comparisons

In the last section, we have seen the unstable performance of *Linear Control Scheme*. This is, in fact, related to the fairness among the terminals. In this section, we will compare the fairness of terminals in the network of different MAC schemes

5.3.1 Situation of Unfairness

For each terminal in the network, the chances to access the channel and transmit packets can be regarded as the obtained channel resources. Therefore, the fairness of this allocation becomes a critical issue in MAC scheme designing. Fig. 5.4 illustrates

one possible situation that may result in unfairness under *Linear Control Scheme.*

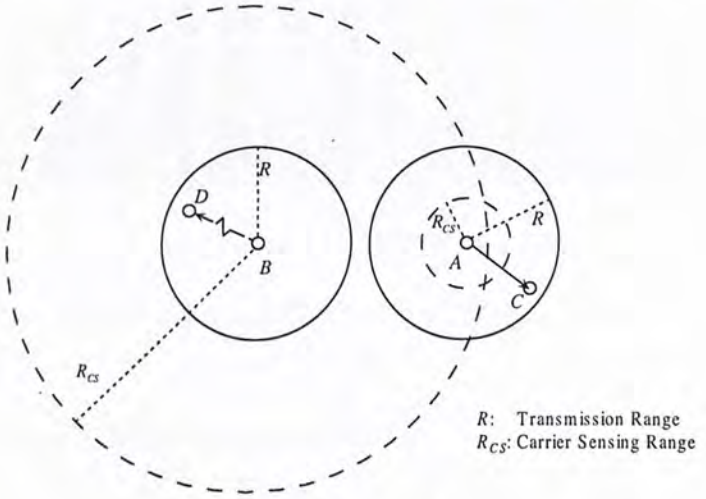


Figure 5.4: Unfairness in Channel Resources Allocation

After a series of transmission, the sensing range, R_{CS} of terminal B may become very large due to the consecutive transmission failures while the successful transmissions gives a very small R_{CS} to terminal A. Therefore, B can be aware of the transmission from A. On the other hand, A even does not know the existence of B and keeps on transmitting to C aggressively. Even if A occasionally experiences an ACK time out, it will not change the situation too much. As the penalty in *Linear Control Scheme* is small, the R_{CS} will only increase by δ ($15m$ in the simulations). As long as the next transmission is acknowledged, the R_{CS} will decrease again and it still cannot notice B. As a result, B can hardly have chance to transmit to D. Therefore, this causes the unfairness of channel resource allocation between terminal A and B.

Fig. 5.4 only shows one possible case. There are other situations that may induce the unfairness. Hereby, in Fig. 5.3(a), the target nodes we are measuring may happen to obtain a high share of channel resources at some loadings, and thus, exceed the original throughput. However, at other loadings, they may fail to achieve so.

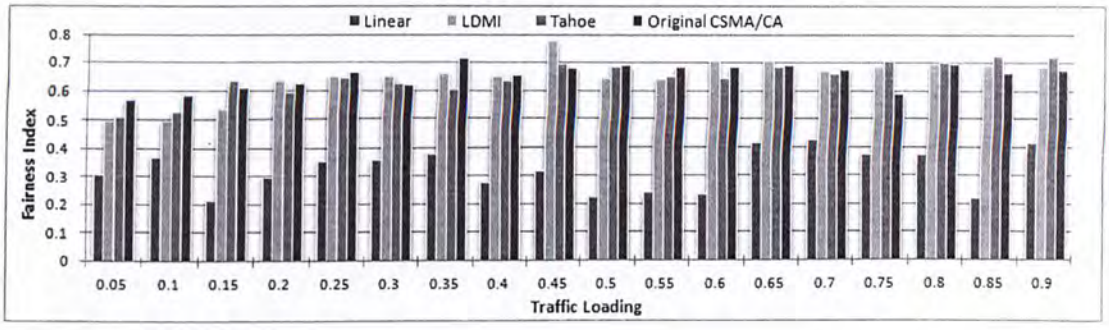


Figure 5.5: The Comparison of Terminal Fairness

5.3.2 Fairness Measurement

To quantify the fairness, we adopt the index introduced in [35], which is originally used to measure the fairness of bandwidth allocation in TCP congestion control. It is given by the following equation,

$$F(x) = \frac{(\sum_i x_i)^2}{n(\sum_i x_i^2)} \tag{5.2}$$

where x_i denotes the *one-hop* throughput of terminal i. $F(x)$ ranges from 0 to 1 and monotonically increases with the fairness. Different from the simulations of throughput comparisons, we apply the same traffic loading (the same packet size, $1024bytes$, and the same sending rate) to all the terminals in the network. That is, we do not apply the *Geometric Burst Traffic Model*. By using the index, Fig. 5.5 shows the fairness comparisons of different schemes.

We can observe that *Linear Control Scheme* shows a poor fairness performance. This agrees with our previous analysis and is the cause of unstable performance in throughput. However, both*LDMI* and *Tahoe* achieve the same level of fairness as the original CSMA/CA. At the lower loadings, they perform a bit worse than CSMA/CA, but exceeds it at higher loadings. On average, the fairness over all the loadings of the original CSMA/CA is 0.658 while that of *LDMI* is 0.653 and 0.654 for *Tahoe*.

Although the fairness value of all these three schemes are not very high, around 0.65, we did find any terminal starving in *LDMI* and *Tahoe* by observation. Nevertheless, there exists variance among the terminal *one-hop* throughputs, as shown in Table 5.2 (*Tahoe*, Traffic Loading= 0.8). In this sense, the two schemes do not have the improvement in terms of fairness. After all, they have achieved the same level fairness as the original CSMA/CA.

Terminal	Throughput (*packets/sec*)	Terminal	Throughput (*packets/sec*)
Host 148	19.394	Host 167	3.250
Host 149	11.218	Host 168	9.594
Host 150	5.833	Host 169	13.453
Host 151	4.023	Host 170	3.454
Host 152	6.914	Host 171	5.494
Host 153	3.016	Host 172	13.141
Host 154	9.218	Host 173	10.569
Host 155	3.934	Host 174	14.007
Host 156	2.122	Host 175	8.329
Host 157	6.959	Host 176	8.329
Host 158	16.941	Host 177	4.732
Host 159	12.485	Host 178	23.938
Host 160	10.531	Host 179	8.737
Host 161	13.984	Host 180	10.864
Host 162	7.030	Host 181	36.732
Host 163	13.653	Host 182	12.178
Host 164	12.644	Host 183	15.619
Host 165	5.719	Host 184	5.984
Host 166	8.601	Host 185	9.549

Table 5.2: The Sample of Terminal Throughputs in *Tahoe Controlling Scheme*

By this token, both *LDMI* and *Tahoe* show a desirable performance. As they have much higher throughput as well as the same level of fairness, most terminals in the networks will get a better share of the channel resources, i.e., more chances to access the channel and transmit. Therefore, *LDMI* and *Tahoe* perform better in terminal coordination than the original CSMA/CA.

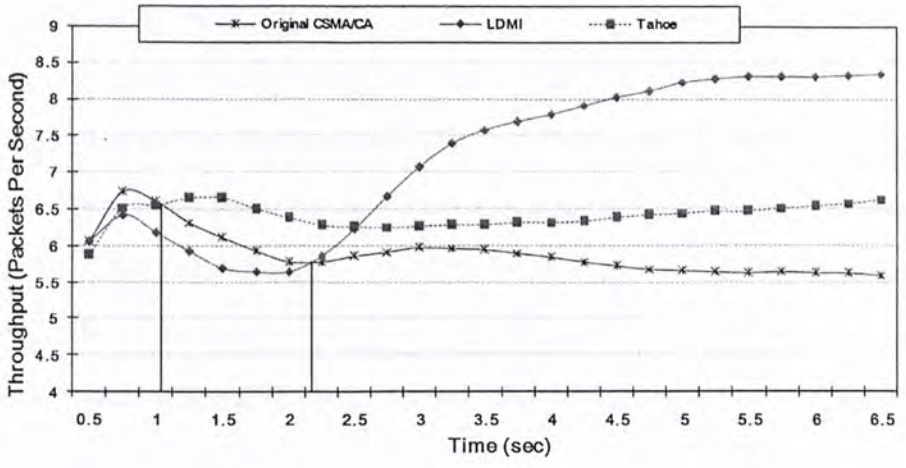


Figure 5.6: Speed of Throughput Convergence

5.4 Convergence Comparisons

We have compared the throughput and fairness of the four schemes, and concluded that *LDMI* and *Tahoe* present the satisfactory performance. But, from Fig. 5.3(b) and 5.3(c), it can be observed that *Tahoe* has lower throughput than *LDMI*. So, in this section, we will explore the superiority of *Tahoe Control Scheme* in terms of the speed of throughput convergence.

According to the configurations in Section 5.1, the average burst length adopted is 8 seconds in the simulations. Now, we will observe how the throughput varies within this 8 seconds. We apply the traffic loading of 0.35 to a terminal inside the network. It is located in the center of the topology show in Fig. 5.2, thus the surrounding nodes are randomly distributed around it. They apply the *Geometric Burst Traffic Model*. We observe the *one-hop* throughput of this terminal from the beginning of a new burst of the surrounding nodes under different MAC schemes. The result is shown in Fig. 5.6.

Although *LDMI* has achieved the highest throughput in the end, the throughput

of *Tahoe* exceeds the CSMA/CA earlier at around 1.2second which is almost half of *LDMI*, 2.25second. Both control schemes can outperform the CSMA/CA within 8 seconds, but this may not be the case when the burst length is shorter. For example, if the burst length becomes 2 seconds, then the throughput of *LDMI* may even be lower than CSMA/CA. This indicates that *Tahoe* can find a better or optimal R_{CS} more quickly than *LDMI*. In summary, *Tahoe Control Scheme* is more suitable in dynamic traffic condition where the traffic of the surrounding terminals varies more frequently.

5.5 Summary of Performance Comparison

The simulation analyses present a set of performance comparisons of the two MAC protocols, *LDMI* and *Tahoe*. The results can be summarized by the Table 5.3.

Protocols	Better → Worse
Throughput	*LDMI* → *Tahoe* → CSMA/CA
Terminal Fairness	Same level of fairness
Convergence Speed	*Tahoe* → *LDMI*

Table 5.3: Overview of Performance Comparison

From this table, we can observe both *LDMI* and *Tahoe* have their own advantages in different aspects. Hereby, the selection should be made based on the practical situation. On the whole, the modeling of sensing range to the *congestion control window* have made the two MAC protocols superior to the original CSMA/CA.

Chapter 6

Conclusions

This thesis provides a comprehensive study on the MAC layer of Ad Hoc wireless networks by analyzing the hidden and exposed node problems. This is a practical research area that enjoys wide applications.

By studying on the hidden and exposed node problems themselves and previous research work, we showed the tradeoff between two problems. One problem may become worse when the efforts are being made to solve the other problem. This indicates the difficulties of solving the two problem at the same time.

We further performed a theoretical study on the carrier sensing range of CSMA/CA. A mathematical derivation has given a curve that characterizes the relationship between the *one-hop* throughput of the network and the carrier sensing range. Although approximation has been taken, the analysis implies that the size of carrier sensing range plays an important role in the tradeoff between hidden and exposed nodes in CSMA/CA when the terminals are homogeneous.

Based on these works, we found the key issue is to balance the two problems instead of tackling both of them. We have utilized the concept of TCP congestion control to MAC layer of Ad Hoc networks and proposed two distributed MAC schemes, *LDMI*

and *Tahoe* control. The simulation analyses have proven that these two schemes present satisfactory performance in terms of throughput and terminal fairness. Particularly, *Tahoe* is also suitable in dynamic traffic conditions.

The optimal MAC scheme is not discovered in the thesis, but the modeling between congestion control and carrier sensing control presents a feasible approach to improve the MAC layer performance of Ad Hoc networks.

Appendix A

Categories of CSMA/CA

There are several variations of the CSMA depending on the 'Channel Listening' strategy. The variations are 1-*persistent*, *non-persistent* and *p-persistent* CSMA/CA [8]. In the analysis of Chapter 3, we approximated the *non-persistent* CSMA/CA with Geometric Backoff.

A.1 1-*persistent* CSMA/CA

With this strategy, the terminal always keeps listening to the channel and waits for the end of the transmission. As soon as the channel is idle, the terminal transmits its message with probability one.

A.2 *non-persistent* CSMA/CA

In this category of CSMA/CA, if busy channel is encountered or the transmission fails, the terminal waits a random time before the retransmission of a packet. Here, the random time is known as *backoff* time. Several backoff schemes are described in Appendix B.

A.3 *p-persistent* CSMA/CA

This is a generalization of the above two schemes. It can be described as follows [36].

- If the channel is idle, the terminal begins transmission with probability p in this (mini)slot.
- In idle channel, the terminal repeats the above process in each (mini)slot until the transmission is initiated or the channel becomes busy.
- If the channel is busy, the terminal keeps sensing the channel until it becomes idle.

Appendix B

Backoff Schemes

In most MAC protocols, the terminal will apply a random *backoff* time before the next action if it encounters contentions, like busy channel or transmission failure. If the next action still fails, the terminal will go through another backoff. There are many backoff algorithms, some of which are described here for reference.

B.1 Constant Window Backoff Scheme

This is the most basic backoff scheme. A contention window with fixed size is maintained in terms of (mini)slots, for example, $[0, CW-1]$, where CW stands for *contention window* and specifies the maximum possible time of backoff. When backoff is needed, a random value W is selected uniformly from $[0, CW-1]$. Hereby, the terminal will experience a backoff of W (mini)slots.

B.2 Geometric Backoff Scheme

Under this scheme, the length of backoff time follows the *Geometric* Distribution. During the backoff, the terminal ends the backoff with a probability p in each (mini)slot.

Therefore, the expected backoff time is $1/p$ (mini)slots under this scheme. This scheme is adopted in the analysis of Chapter 3.

B.3 Binary Exponential Backoff Scheme

Binary Exponential Backoff (BEB) is the scheme that IEEE 802.11 DCF standard implements. Each terminal will also maintain a contention window. During the first backoff, the initial window size is $[0, CW_0 - 1]$. A random value will be randomly selected as the backoff (mini)slots. In case the next transmission still fails, another backoff is launched and the window size is updated to $[0, CW_1 - 1]$, where $CW_1 = 2CW_0$. This process repeats if the transmission failure continues. Therefore, the contention window will goes through a binary exponential expanding. The maximum contention window is defined as $[0, CW_{max} - 1]$. In IEEE 802.11 standard, one common configuration is that the minimum window size CW_{min} is $CW_{min} = CW_0 = 2^5$ and the maximum window size is $CW_{max} = 2^{10}$ [9].

Bibliography

[1] M. Gerla, "Guest Editorial Wireless Ad Hoc Networks", *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8. Aug 1999.

[2] C. K. Toh, *Ad Hoc Mobile Wireless Network: Protocols and Systems*, Prentice Hall, New Jersey, 2002.

[3] E. Hossain and K. K. Leung, *Wirless Mesh Networks: Architectures and Protocols*, Springer, New York, 2008.

[4] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing", *WMCSA '99*, pp. 90-100, Feb. 2008.

[5] D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts". *Proceedings of WMCSA '94*, pp. 158-163, Dec. 1994.

[6] F. A. Tobagi and L. Kleinrock, "Packet Switching in Radio Channels: Part I–Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics", *IEEE Trans. Communications.*, vol. 23, pp. 1400-1416, Dec. 1975.

[7] F. A. Tobagi and L. Kleinrock, "Packet switching in radio channels: Part II—The hidden terminal problem in carrier sense multiple-access and the busy-tone solution". *IEEE Trans. Communications.*, vol. 23, pp. 1417-1433, Dec. 1975.

[8] T. Rappaport, *Wireless Communications: Principles and Practice, 2nd Edition*, Prentice Hall, Dec. 2001.

[9] IEEE 802.11 Standards, "Wireless LAN Medium Access Control and Physical Layer Specifications", *IEEE Standards Association*, 2007.

[10] F. F. Kuo, *"The ALOHA system" in Computer Networks.*, Prentice-Hall, 1973.

[11] M. W. Ritter, "The Future of WLAN", *ACM Queue.*, vol. 2, No. 3, pp. 18-27, May 2003.

[12] J. F.Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, Pearson Education, Amherst, 2003.

[13] D. Raychaundhuri and K. Joseph, "Performance evaluation of slotted ALOHA with generalised retransmission backoff", *IEEE Trans. on Communications.*, vol. 38, pp. 117-122, Jan. 1990.

[14] Z. J. Haas and J. Deng, "Dual Busy Tone Multiple Access (DBTMA)A Multiple Access Control Scheme for Ad Hoc Networks",*IEEE Trans. on Communications*, vol. 50, no. 6, pp. 975-985, Jun. 2002.

[15] Y. Ko, V. Shankarkumar, and N.H. Vaidya, "Medium access control protocols using directional antennas in ad hoc networks, *INFOCOM 2000*, pp.1321, 2000.

[16] C. N. Kang, D. Y. Yang and J. W. Jwa, "A Dual-Channel MAC Protocol with Directional Antennas for Mobile Ad-Hoc Networks", *IEICE Trans. on Commun.* vol. E90-B, no. 11, pp. 3266-3270, Nov. 2007.

[17] F. Ye, S. Yi and B. Sikdar, "Improving spatial reuse of IEEE 802.11 based ad hoc networks", *IEEE GLOBECOM' 03*, vol. 2, pp. 1013-1017, Dec. 2003.

[18] K. Xu, M. Gerla and S. Bae, "How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks", *IEEE GlOBECOM' 02*, vol. 1, pp. 72-76, Nov. 2002.

[19] D. Shukla, L. Wadia and S. Lyer, "Mitigating the exposed node problem in IEEE 802.11 ad hoc networks", *ICCCN. 2003 Proceedings*, pp. 157-162, Oct. 2003.

[20] H. Takagi and L. Kleinrock, "Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals", *IEEE Trans. on Commun.* vol. 32, no. 3, pp. 246-257, Mar. 1984.

[21] R. Rom and M. Sidi, *Multiple Access Protocols: Performance and Analysis*, Springer-Verlag, New York, 1990.

[22] L. Jian and S. C. Liew, "Removing hidden nodes in IEEE 802.11 wireless networks", *Vehicular Technology Conference, 2005*, vol. 2, pp. 1127-1131, Sept. 2005.

[23] Bharghavan et al, "MACAW: A Media Access Protocol for Wireless LAN's". *Proc. of ACM SIGCOMM '94*, pp. 212-215, Aug. 1993.

[24] K. Yukinari, N. Tomotaka, K. Mori and H. Kobayashi, "An advanced CSMA inter-vehicle communication system using packet transmission timing control decided by the vehicle position", *IEIC Technical Report*, vol. 103, No. 86, pp. 11-16, 2003.

[25] T. You, C. Yeh and H. Hassanein, "CSMA/IC: a new class of collision-free MAC protocols for ad hoc wireless networks", *8th IEEE International Symposium on Computers and Commun.*, vol. 2, pp. 843-848, July 2003.

[26] D. Chiu, R. Jain, "Analysis of the Increase/Decrease Algorithms for Congestion Avoidance in Computer Networks", *Journal of Computer Networks and ISDN*, 17(1), June 1989.

[27] O. Ait-Hellal and E. Altman, "Analysis of TCP Vegas and TCP Reno", *ICC '97*, vol. 1. pp. 495-499, Montreal, Jun 1997

[28] V. Jacobson, and M. J. Karels, "Congestion Avoidance and Control", *Symposium Proceedings on Commun. Acrhitectures and Protocols*, pp. 314-329, 1988.

[29] V. Jacobson, "Modified TCP congestion avoidance algorithm," *note sent to end2end-interest mailing list*, 1990.

[30] C. Caini and R. Firrincieli, "TCP Hybla: a TCP enhancement for heterogeneous networks", *Int. J. Satell. Commun. Network.*, vol. 22., pp. 547-566, 2004.

[31] J. Zhu, X. Guo, L. Yang, W. Conner, S. Roy and M. Hazra, "Adapting physical carrier sensing to maximize spatial reuse in 802.11 mesh networks", *Wireless Commun. & Mobile Computing*, vol. 4, pp. 933-946, Dec. 2004.

[32] L. S. Brakmo, S W. O'Malley and L. L. Peterson, "TCP Vegas: New Techniques for Congestion Detection and Avoidance", *Proceedings of SIGCOMM '94*, pp. 24-35, 1994.

[33] Omnet++, http://www.omnetpp.org

[34] W. Drytkiewicz, S. Sroka, V. Handziski, A. Kpke and H. Karl, *A Mobility Framework for Omnet++*, Technische Universitat Berlin, Jan. 2003.

[35] R. Jain, D. Chiu and H. Hawe, "A Quantitative Measure of Fairness and Discrimination for Resource Allocation in Shared Systems", *Techical Report DEC-TR-301, Digital Equipment Coporation*, 1984.

[36] T. Suda and T. Nakano, "Multiple Radio Access", *CS232 Internet Lecture Notes*, U.C. Irvine, 2007.