AD HOC ASSISTED HANDOFF IN IEEE 802.11 INFRASTRUCTURE WLANS

AD HOC ASSISTED HANDOFF IN IEEE 802.11 INFRASTRUCTURE WLANS

By

MING HE, B. ENG., M. ENG.

A Thesis
Submitted to the School of Graduate Studies
in Partial Fulfilment of the Requirements for the degree of

Master of Applied Science
Department of Electrical and Computer Engineering
McMaster University

MASTER OF APPLIED SCIENCE (2004)
(Electrical and Computer Engineering)

McMaster University
Hamilton, Ontario

TITLE:
Ad Hoc Assisted Handoff in IEEE 802.11 Infrastructure WLANs

AUTHOR: Ming He, B. Eng., M. Eng.
(Xidian University, P.R.China)

SUPERVISORS: Dr. Terence D. Todd and Dr. Dongmei Zhao

NUMBER OF PAGERS: xviii, 87

Abstract

IEEE 802.11 wireless local area networks (WLANs) are increasingly used to support real-time services such as voice and video. Reliable and portable operation, however, is often difficult due to factors such as imperfect customer access point (AP) installation, unpredictable WLAN coverage, and unexpected co-channel interference.

There has been much recent activity that considers the combination of ad hoc relaying and infrastructure wireless networks as alternative solutions to coverage extension. In this thesis, we propose and further investigate the use of IEEE 802.11 Ad Hoc Assisted Handoff (AAHO). In AAHO, an additional ad hoc hop may be used by a mobile station (MS) to obtain the range extension or channel quality needed to maintain its real-time voice connection. An MS that is currently not carrying active traffic may offer itself as a potential relay station (RS). Three versions of IEEE 802.11 AAHO are discussed in this thesis. In the case of Backward Ad Hoc Assisted Handoff (BAAHO), the additional hop uses a relay station which already has an IEEE 802.11 association with the AP that the MS is using. In the case of Forward Ad Hoc Assisted Handoff (FAAHO), however, the additional hop uses a relay station whose AP is different from the one that the MS is currently using. Hybrid Ad Hoc Assisted Handoff (HAAHO) is a combination of these two concepts that allows an MS to perform in either BAAHO or FAAHO mode. The proposed AAHO schemes are backward compatible to existing IEEE 802.11 infrastructure. They can be implemented as a transparent overlay across existing IEEE 802.11 deployments. Two implementation options for achieving this compatibility are proposed. A criterion in selecting relay station is introduced, which permits mobile stations to control real-time relaying of voice packets. Our simulation results show that AAHO can greatly improve performance in many realistic situations.

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my thesis supervisors, Dr. Terry Todd and Dr. Dongmei Zhao, for their consistent guidance and support in the process of this thesis work. Their passion for research and knowledgeable suggestions have greatly enhanced my interest of research, and significantly improved the end results. Without their encouragement and invaluable insights, this thesis would not have been possible. Secondly, I would like to acknowledge Dr. Steve Hranilovic and Dr. Shahram Shirani for their time in reviewing this thesis and valuable comments. I would also like to appreciate Craig Thornton for his time and patience in reviewing this thesis and his valued suggestions.

It is my pleasure to have the opportunity stay with members of wireless networking laboratory in the past two years. I would like to give them my very much appreciation for their help and friendship. I would also like to thank the administrative staff of the department in making my study and stay here easy.

Last but not the least, I would like to thank my parents for their continual encouragement and support. My special thanks gives to my wife for her love, understanding, and patience.

Contents

Abstract iii

Acknowledgements v

List of Abbreviations xv

1 Introduction 1

1.1 Introduction to IEEE 802.11 WLAN 1

1.2 Multihop Relaying 4

1.3 Overview of Proposed Work 8

1.4 Thesis Organization 10

2 Background 13

2.1 IEEE 802.11 MAC Protocol 14

2.1.1 IEEE 802.11 Legacy MAC Protocol 14

2.1.2 IEEE 802.11 MAC Extension 20

2.2 Management Operations in Infrastructure IEEE 802.11 WLAN 25

2.2.1 Scanning 25

2.2.2 Authentication 28

2.2.3 Association 28

2.2.4 Power Management 30

2.2.5 Synchronization 32

2.3 Mobility Management 33

2.4 Relaying in IEEE 802.11 Infrastructure Networks 39

3 Ad Hoc Assisted Handoff (AAHO) in IEEE 802.11 Infrastructure WLANs 43

3.1 System Architecture 44

3.2 Ad Hoc Assisted Handoff (AAHO) 46

3.3 IEEE 802.11 MAC Protocol Extensions 51

3.4 Link Maintenance and Handoff 56

3.5 Relay Station Selection Criterion 57

3.6 Compatible Implementation Options 59

4 Simulation Results and Performance Analysis 63

4.1 Simulation Model 63

4.2 Mobility Model 64

4.3 Simulation Environment and Parameters Settings 66

4.4 Numerical Results and Performance of AAHO 70

4.4.1 Comparison of AAHO Schemes 71

4.4.2 Impact of the Number of Mobile Stations 73

4.4.3 Impact of Mobile Station Moving Speed 75

4.4.4 Impact of Relay Station Selection Criteria 77

5 Conclusions and Future Work 79

List of Figures

1.1 Independent BSS and Infrastructure BSS 3

2.1 IEEE 802.11 DCF Channel Access Mechanism 15

2.2 Hidden Station and RTS/CTS Procedure Illustration 16

2.3 DCF Channel Access Mechanism with RTS/CTS Exchange . . . 17

2.4 IEEE 802.11 PCF Channel Access Mechanism 18

2.5 Channel Access Entities for EDCA 23

2.6 Example of IEEE 802.11e HCCA Channel Access 24

2.7 Passive Scanning Procedure 26

2.8 Active Scanning Procedure and Medium Access 27

2.9 Frame Exchange during Authentication 28

2.10 Association Procedure 29

2.11 PS-Poll and Buffered Frames Retrieval Process 31

2.12 Handoff in IEEE 802.11 Infrastructure WLAN 35

2.13 Illuatration of Handoff Algorithms 35

2.14 Handoff Procedures in IEEE 802.11 Infrastructure WLAN . . . 38

2.15 Example of WLAN coverage area 40

3.1 IEEE 802.11 Infrastructure Network 44
3.2 Forward and Backward Ad Hoc Assisted Handoff 46
3.3 Example of BAAHO 48
3.4 Example of FAAHO 49
3.5 Example of HAAHO 50
3.6 Relay Station Probing Procecss 53
3.7 Relay Station Operation During AAHO 54
3.8 Example of Relay Station Selection in MRSS 59
3.9 Infrastructure Anchor for Ad Hoc Assisted Handoff 61

4.1 Simulation System Configuration 65
4.2 Illustration of Extension Coverage Area, $R = 65$ m 66
4.3 Illustration of Extension Coverage Area, $R = 90.5$ m 67
4.4 New Call Blocking/Handoff Call Dropping Rate, $R = 65$m . . . 71
4.5 New Call Blocking/Handoff Call Dropping Rate, $R = 90.5$m . . 72
4.6 Performance Impact of MS Quantity, $R = 65$m 73
4.7 Performance Impact of MS Quantity, $R = 90.5$m 74
4.8 Handoff Call Dropping Rate versus Mobility, $R = 65$m 75
4.9 Handoff Call Dropping Rate versus Mobility, $R = 90.5$m 76
4.10 Comparison of MRSS and RRSS, $R = 65$m 77
4.11 Comparison of MRSS and RRSS, $R = 90.5$m 78

List of Tables

2.1 User Priority and Access Category in EDCA 24

3.1 Max/Min Relay Station Selection Example 60

4.1 Default Simulation Parameters 69

List of Abbreviations

AC	Access Category
ACK	Acknowledgement
A-GSM	Ad hoc GSM
AID	Association ID
AIFS	Arbitration Interframe Space
AP	Access Point
ARS	Ad hoc Relay Station
BAAHO	Backward Ad hoc Assisted Handoff
BS	Base Station
BSA	Basic Service Area
BSS	Basic Service Set
CBR	Constant Bit Rate
CFP	Contention Free Period
CP	Contention Period
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send

CW	Contention Window
DB-DCF	Deadline Bursting DCF
DCF	Distributed Coordination Function
DIFS	DCF Interframe Space
DS	Distribution System
EDCA	Enhanced Distributed Channel Access
ES-DCF	Elimination by Sieving DCF
ESS	Extended Service Set
FAAHO	Forward Ad hoc Assisted Handoff
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GW	Gate Way
HAAHO	Hybrid Ad hoc Assisted Handoff
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
H_CHANNEL	Home Channel
HDR	Handoff-call Dropping Rate
IA	Infrastructure Anchoring
IAPP	Inter-Access Point Protocol
IBSS	Independent Basic Service Set
iCAR	Integrated Cellular and Ad hoc Relay
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific, and Medical
LAN	Local Area Network

LOS	Line-Of-Sight
MAC	Medium Access Control
MADF	Mobile Assisted Data Forwarding
MCN	Multihop Cellular Network
MRSS	Max/min Relay Station Selection
MS	Mobile Station
MSDU	MAC Service Data Unit
NAV	Network Allocation Vector
NBR	New-call Blocking Rate
ODMA	Opportunity Driven Multiple Access
OTDoA	Observed Time Difference of Arrival
PC	Point Coordinator
PCF	Point Coordination Function
PHY	Physical Layer
PIFS	PCF Interframe Space
PS	Power Save
PSTN	Public Switched Telephone Network
QoS	Quality of Service
R_CHANNEL	Relay Channel
RP_CHANNEL	Relay Paging Channel
rPCF	Relay-enabled PCF
RRSS	Random Relay Station Selection
RS	Relay Station
RSS	Received Signal Strength

RSSC	Relay Station Selection Criterion
RSSI	Received Signal Strength Indication
RTS	Request to Send
SIFS	Short Interframe Space
TBTT	Target Beacon Transmission Time
TDMA	Time Division Multiple Access
TIM	Traffic Indication Map
TMS	Transparent MAC Spoofing
TSF	Time Synchronization Function
TXOP	Transmission Opportunity
UP	User Priority
WCDMA	Wideband Code Division Multiple Access
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

Chapter 1

Introduction

1.1 Introduction to IEEE 802.11 WLAN

The increasing need to provide a broader class of ubiquitous communications to customers anywhere at anytime leads to a successful development of wireless mobile networks. Cellular systems are widely used for public wireless communications. However, deploying a cellular system takes a long period of RF planning and system design, requires a large investment in equipment and cell sites, as well as in obtaining a license of operation for new ranges of spectrum. Besides these, the limited radio resources of current cellular systems are not adequate to provide quality of service (QoS) for customers in so-called hot spots, such as airports, railway stations, cafés, hotels, conference rooms, campus, and office buildings, where a high density of population and heavy traffic loads exist. There is a need for another cost effective public wireless access solution to fulfill the demand for applications in such situations. Wireless local area network (WLAN) technology becomes a good choice for mobile network operators to meet customers' increasing demand and to generate new revenue streams. Because WLANs operate on the unlicensed frequency bands, the Industrial, Scientific, and Medical (ISM) bands, so that it can offer additional capacity and higher bandwidth for end users at low cost without sacrificing the capacity of cellular users.

Recently, WLANs based on IEEE 802.11 standards have attracted much attention due to their low cost, high capacity, and flexibility in both topology and mobility [15]. The IEEE 802.11 standard [3] supports two operating modes, the ad hoc mode and the infrastructure mode. In ad hoc mode, a group of mobile stations (MSs) communicate directly with each other within a direct communication range, called basic service area (BSA), determined by the propagation characteristics of the wireless medium. The combination of these stations is referred to as an independent basic service set (IBSS) because no fixed infrastructure, typically an 802.11 access point (AP), is needed. Ad hoc networks are highly flexible in topology, but not reliable for providing QoS for real-time services due to their path diversity. In infrastructure mode, on the other hand, communications between mobile stations must be bridged by a fixed infrastructure called access point (AP). MSs must associate with an AP to obtain access to networks. Accordingly, the basic service set (BSS) in this situation is referred to as an infrastructure BSS, and the basic service area corresponding to this infrastructure BSS is determined by the points at which transmissions from the AP can be received. Both independent BSS and infrastructure BSS are illustrated in Figure 1.1.

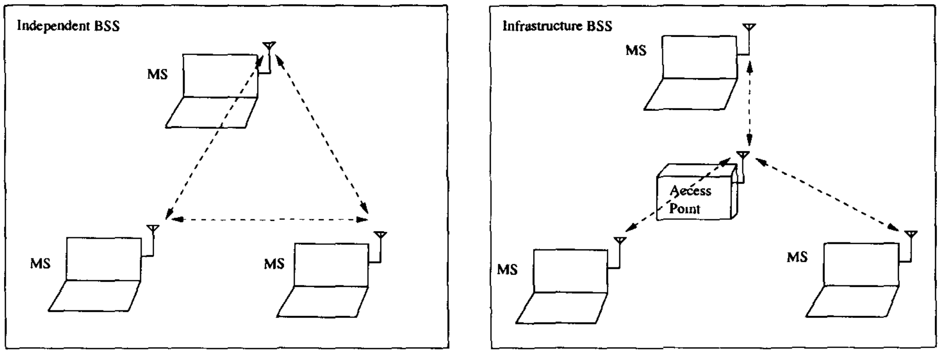

Figure 1.1: Independent BSS and Infrastructure BSS

A BSS can create coverage for MSs which are very close to each other such as small offices and homes, but it cannot provide network level coverage to larger areas due to its fast channel degradation in 2.4 GHz and 5 GHz ISM bands. A typical BSS coverage range of 2.4 GHz IEEE 802.11b is roughly 50 to 100 meters, and a 5 GHz 802.11a BSS can cover roughly 10 to 30 meters. This figure is affected by frequency band, modulation schemes, moving speed, data rates, interference, and desired performance criterion [38] [34] [39]. In office environments, for example, the coverage range varies from the order of several tens of meters to the order of several hundreds of meters [29]. For ad hoc BSS's, coverage extension can be achieved by relaying data frames in multiple hops via intermediate stations between the source and the destination. This multihop path is set by an appropriate routing scheme. For infrastructure BSS's, on the other hand, IEEE 802.11 allows to link multiple APs to a backbone network, called distribution system (DS), to form an extended service set (ESS). The DS provides mobility in an ESS, and also builds a connection to the wired networks such as Internet or Intranet. In practice, overlapping between BSS's is required to offer ubiquitous coverage within the ESS, which is the essence to provide stable transmission links and QoS throughout the coverage areas of interest. However, determining the optimal number of APs and their locations depends on measured signal strength, power level, frequency band, and tradeoff between throughput and coverage area [29]. Such an approach is labor intensive, expensive, and time consuming when deploying a large number of WLAN APs [20]. Due to lack of building licenses, power supply, and/or wired-LAN access, it may be impossible to install APs in some pre-selected optimal locations. In addition, WLAN products are now becoming very inexpensive and easy to be installed by customers themselves. It turns out to be much more difficult to control co-channel interference and proper locations of APs. As a result incomplete and highly variable coverage is typical in many situations where strong shadowing and other fading effects exist.

1.2 Multihop Relaying

There has been much recent activity that considers the combination of ad hoc relaying and infrastructure wireless networks as an alternative coverage extension solution. In this integrated network, a mobile station (MS) within the coverage range of its currently associated AP can access the AP directly, while an MS outside of coverage area of APs may access the AP via relaying through other MSs via multiple hops. MSs which are not carrying any traffic can offer themselves as relay stations (RSs). Some potential advantages of integrating ad hoc relaying and infrastructure WLANs are as follows.

- Ad hoc relaying can provide significant coverage extension to those MSs which are not in the coverage range of the AP.
- Breaking a longer path down into a number of shorter hops can reduce the transmission power. Accordingly, co-channel interference is reduced, and the user's battery life is increased.
- Enabling ad hoc relaying enhances the adaptability to fast channel degradation and provides greater potential for building stable paths and providing real-time QoS.
- Relay stations can help to balance the traffic in some hot spots, where heavy traffic exists, to its adjacent non-congested AP.

Using a mobile station as a relay station will increase the complexity of mobile terminals, and will result in an additional transmission delay due to multihop propagation. Both physical layer (PHY) and medium access control (MAC) layer protocol extensions have to be taken into consideration in system design and implementation.

A variety of systems using ad hoc relaying have been considered, often differing on the basis of whether mobile stations have multiple air interfaces, whether ad hoc infrastructure is present, and whether WLAN and/or cellular is being considered [6] [40] [30] [23] [8] [32] [7].

A dual mode system in [6] uses ad hoc mode to enable direct communications between mobile stations without using the cellular infrastructure whenever mobile stations are within transmission range of each other. When mobile stations are "far" from each other, the communications go through the base stations (BSs). Different radio frequencies and different modulation schemes are used to separate ad hoc mode and cellular mode without overlapping between each other. A similar hybrid wireless network is proposed in [11], but to maintain simplicity, a maximum of two ad hoc hops may be used between the end stations. The discussion is mainly focused on the MAC layer, no PHY layer properties are mentioned in the simulation.

In mobile assisted data forwarding (MADF) [40], an extra ad hoc overlay is added to the cells of a fixed cellular infrastructure where hot spots exist. Special forwarding channels are allocated from resources used by the existing cellular network. These channels are then used for relaying traffic between cells. The objective of MADF is to balance traffic load in the system especially in the case where traffic hotspots are present.

The approach in iCAR [30] is similar to the MADF, but uses special preinstalled ad hoc relay stations (ARSs) to move traffic between cells. Benefits of capacity enhancement, congestion relief, and coverage extension can be achieved through relay station placement scheme called seed-growing approach. Two air interfaces, C air interface for cellular and R air interface for relaying, are implemented in each ARS. Handoff is executed between the relay station and base station, and between the relay station and mobile station. We notice that in both [40] and [30], mobile stations cannot communicate directly even if they are very close. All connections must go through the associated base stations.

The multihop cellular network (MCN) incorporates ad hoc routing into the cellular network using the same air interface as is used by the cellular base stations (BSs) [23] [8]. A key feature of MCN is that mobile stations can communicate directly with each other if they are reachable, which leads to multihop routing. This helps to improve the throughput, reduces the number of base stations, and deals with vulnerable paths caused by base station failure and/or mobile station mobility. A similar concept is proposed by the opportunity driven multiple access (ODMA) system in [32] and the ad hoc GSM (A-GSM) system described in [7].

Unlike the iCAR system in [30], which uses pre-installed relay stations, the other aforementioned systems use mobile stations as relay stations to forward the data frames. When mobility is involved, selecting the proper relay stations and maintaining reliable paths between mobile stations and relay stations and/or between relay stations and base stations becomes a major challenge for designers. In [41] a mechanism named position assisted relaying was proposed for WCDMA cellular networks with dual-mode stations. In this scheme, a nearby station may relay transmissions for another one when that station's cellular link becomes unusable. Geo-location techniques such as global positioning system (GPS) or observed time difference of arrival (OTDoA) are used by the BS to select a candidate relay station (RS). The selection criteria may take into account factors such as direction and speed of a mobile stations' movement [41].

Recently, IEEE 802.11 WLANs have been facing increasing demand to support real-time services such as voice and video [31] [22] [13] [12] [37] [24] [33]. Users not only demand high-speed data rates, but also want to be able to talk with each other. However, WLAN was originally designed as a wireless extension to enterprise LAN networks, and now becomes an attractive technology for home and public environments. Effective access to data networks and the Internet is a primary consideration for both WLAN designers and users. For example, initial 802.11 standard [3] promised up to 2 Mbps data rate on the 2.4 GHz ISM band. Subsequently, the IEEE 802.11 working group standardized both 802.11a [1] and 802.11b [2] in 1999. 802.11b is currently the most widely adopted 802.11 standard in today's WLAN market. 802.11b operates on the 2.4 GHz ISM band, and can support data rates up to 11 Mbps. On the other hand, the 802.11a operates on 5 GHz ISM band, and can provide data rates up to 54 Mbps [15]. In the case of supporting real-time voice services, reliable and seamless communications are required by both fixed and mobile users. Effective and efficient QoS support, such as real-time voice services, is still a challenging issue in contention-based ad hoc relaying networks.

1.3 Overview of Proposed Work

In this thesis, we consider the use of ad hoc relaying in IEEE 802.11-based infrastructure networks that are supporting real-time voice applications. In such a system, active voice calls must be handed off between access points (APs) when the MS moves from coverage area of one AP to another. This handoff is normally performed at Layer 2 by the AP and may utilize mobile stations as relay stations. This thesis proposes and investigates the use of ad hoc assisted handoff (AAHO) in IEEE 802.11-based infrastructure networks. In AAHO, an additional ad hoc hop may be used by a mobile station (MS) to obtain the coverage range extension or channel quality needed to maintain its real-time performance which might otherwise be lost. The limitation of two hops is required to eliminate the effects of multihop routing and the corresponding delay in processing and propagation.

There are three versions of the proposed IEEE 802.11 AAHO. In backward ad hoc assisted handoff (BAAHO), the additional hop uses a relay station (RS) which is already associated with the current AP that the MS is using. In forward ad hoc assisted handoff (FAAHO), the additional hop uses an RS which is already associated with an AP that is different from the one that the MS is currently using. Hybrid ad hoc assisted handoff (HAAHO) is the case where an MS can perform either BAAHO or FAAHO.

The selection of RSs plays an important role in the performance and efficiency of the AAHO. A properly selected RS may reduce the overhead and connection dropping rate, as well as increase the entire system capacity [36]. In the hybrid wireless network presented in [11], relaying stations are selected by maintaining an up-to-date neighboring database. Transmissions can be handed over between mobiles or from mobiles to the base stations depending on the received signal strength and the message type. Different relay station/path selection schemes based on the consideration of different path loss situations in a two-hop relaying cellular network are proposed in [35]. Unlike in a wired network, choosing a relay path using merely the geographic distance as the selection metric is not as efficient as using the path-loss since the radio link quality varies greatly from one hop to the next, depending on the geographic environment between a given pair of transmitter and receiver. Nonetheless, relay path selection based only on the geographic distance can be carried out quite easily and requires minimal overhead, especially with the aid of global positioning system (GPS) technology.

In this thesis, an IEEE 802.11 MAC extension protocol is proposed for quickly identifying potential RSs and a max/min criterion is proposed for making this selection. Link quality maintenance and handoff procedures are described in detail. The effects of different AAHO versions, relay station selection criteria, and mobility and population of mobile stations in the network are investigated and analyzed through simulation coded in C. A novel feature of the proposed system is that the AAHO described in this thesis is backward compatible with legacy 802.11 DCF-based data devices, which means that ad hoc relaying can be performed to support real-time applications while the existing networks are transparently supported. Two implementation options are provided regarding to the compatibility of proposed protocol.

1.4 Thesis Organization

This thesis is organized as follows. Chapter 2 provides a general technology background on IEEE 802.11 infrastructure wireless LANs (WLANs). IEEE 802.11 MAC protocol and its ability to support real-time traffic and handoff are briefly discussed. Chapter 3 describes the proposed ad hoc assisted handoff (AAHO) in IEEE 802.11 infrastructure WLANs to support real-time voice. The discussion includes IEEE 802.11 MAC extension, handoff schemes, link maintenance, and the relay station selection criterion based on the radio channel propagation characteristics. Numerical results and performance discussions are presented in Chapter 4. Here we focus on impacts and implications of handoff schemes, number of mobile stations in the system, mobile station mobility, and relay station selection criteria on the performance. Chapter 5 gives conclusion remarks and suggests some further research topics.

Chapter 2

Background

IEEE 802.11 wireless local area network (WLAN) has become ubiquitous in so-called hot spots to provide broadband Internet access to mobile users. IEEE 802.11 standard describes the functions and services required to operate IEEE 802.11-based ad hoc networks and infrastructure networks. Most WLANs installed today make use of the “infrastructure” mode, where an access point (AP) acts as a bridge between wireless users in APs coverage area and a backbone Internet. There is no direct communication between any two mobile stations. The standard defines MAC procedures and PHY signaling techniques. This chapter begins with a brief description of IEEE 802.11 MAC protocol, which includes an overview of legacy MAC protocol, MAC extension in supporting real-time services, and management operations for an infrastructure IEEE 802.11 WLAN. The discussion of operations deals with scanning, authentication, association, power saving, and synchronization. A normal mobility management procedure is presented, and an introduction of relaying in

IEEE 802.11 infrastructure networks is given at the end of this chapter.

2.1 IEEE 802.11 MAC Protocol

2.1.1 IEEE 802.11 Legacy MAC Protocol

The IEEE 802.11 legacy MAC protocol [3] defines two logical functions called the distributed coordination function (DCF) and the point coordination function (PCF). The DCF is based on a fundamental carrier-sense multiple access with collision avoidance (CSMA/CA) for a distributed, contention-based channel access, whereas the optional PCF is based on poll-and-response mechanism for a centralized, contention-free channel access. Most of today's 802.11 devices operate in the DCF mode only.

1. Distributed Coordination Function (DCF)

   The DCF is based on carrier sense multiple access with collision avoidance (CSMA/CA). It is a technology that is able to sense the medium for accessing, and will try to avoid collision. Basically, the CSMA/CA of the DCF works as listen-before-talk scheme described as follows [3]:

   When an MS has frames to transmit, it will sense the channel to know if other MSs are transmitting. If the channel is busy, the MS waits until the channel becomes idle, then the MS defers for an extra time interval, called the DCF interframe space (DIFS). If the channel stays idle during the DIFS, the MS then starts a backoff process by selecting a random backoff count. When the counter reaches zero, a frame is transmitted.

On the other hand, when a frame arrives and the channel has been idle longer than the DIFS time interval, the frame is transmitted immediately. A basic DCF channel access mechanism is illustrated in Figure 2.1.

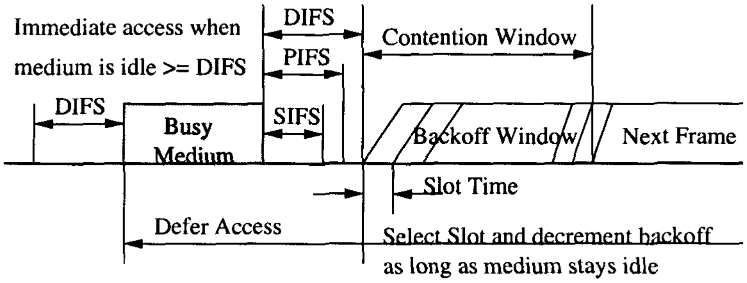

Figure 2.1: IEEE 802.11 DCF Channel Access Mechanism

In carrier sensing based WLAN environments, if an MS is able to receive packets from two different MSs, but these two MSs cannot hear each other directly, in this case, collision might happen at the receiving MS if the two MSs transmit simultaneously since they both cannot sense the transmission from each other. This phenomenon is known as the "hidden station problem". The two stations are called hidden stations. This situation is shown in Figure 2.2, where MS_2 can communicate with both MS_1 and MS_3, but MS_1 and MS_3 are not able to communicate directly due to far apart from each other, or obstacles/interference exist between them. In this case, MS_3 is a so-called hidden station from the perspective of MS_1. If MS_1 and MS_3 transmit simultaneously, the packet frames will collide at MS_2, and no error indication is detected by MS_1 and MS_3.

Since the DCF operates on the carrier-sensing basis, the existence of such hidden stations can degrade the network performance severely. To

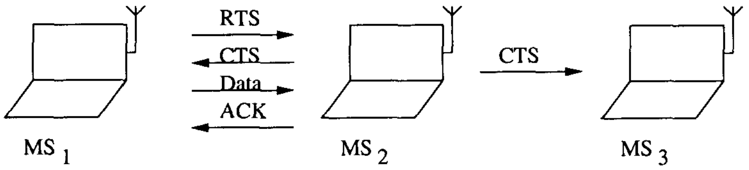

Figure 2.2: Hidden Station and RTS/CTS Procedure Illustration

reduce the hidden station problem, the IEEE 802.11 MAC protocol defines a Request-to-Send/Clear-to-Send (RTS/CTS) mechanism. That is, if the transmitting MS intends to use the RTS/CTS mechanisms, before transmitting a data frame, the MS transmits a RTS frame, and the receiving MS responds with a CTS frame. If the CTS frame is not received within a predefined time interval, the RTS frame is retransmitted by performing a backoff algorithm. The RTS and CTS frames include the information of how long it will take to transmit the subsequent data frame and the corresponding ACK response. Thus, MSs either hear the RTS from the transmitting MS or receive CTS from the receiving MS will not start any transmissions; instead, they set a timer called the Network Allocation Vector (NAV). The NAV indicates the amount of time the medium will be reserved. As long as the NAV value is nonzero, the MS will not contend for the medium because access to the medium is blocked by the NAV. Using NAV ensures that operations between transmitter and receiver are not interrupted. Between two consecutive frames in the sequence of RTS, CTS, data, and ACK frames, a short interframe space (SIFS) is used. The SIFS value is shorter than the DIFS value so that other mobile stations will not collide with ongoing transmission [3] [14].

Figure 2.2 illustrates the procedure of RTS/CTS, and Figure 2.3 indicates the channel access with an RTS/CTS frame exchange [3] [15].

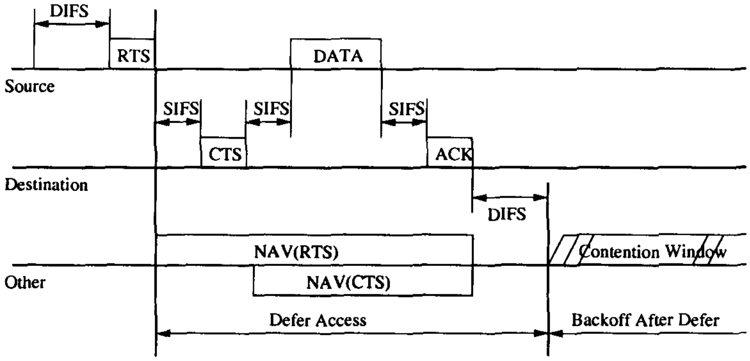

Figure 2.3: DCF Channel Access Mechanism with RTS/CTS Exchange

As can be seen, the CSMA/CA is in fact a random access protocol with delay, which means that all stations have equal probability to contend for accessing to the channel after each DIFS interval. The DCF protocol works well under low traffic load conditions, but suffers from significant throughput degradation and increased channel access delay in high traffic load conditions [19]. Therefore, it can not guarantee acceptable delay for supporting time-bounded services such as voice and video [21].

2. Point Coordination Function (PCF)

In order to support time-bounded services, the IEEE 802.11 standard also optionally defines a Point Coordination Function (PCF) to let MSs have fair contention-free access to the wireless medium. The PCF is only usable on infrastructure network and uses a Point Coordinator (PC), which is a specialized function operated at the AP. The essential operation of PC is polling, with the PC to perform the role of the polling master, and to determine which MS currently has the right to transmit. The PC generates Beacon frames at regular intervals, thus every station knows when the next Beacon frame will arrive. This time is called target Beacon transmission time (TBTT) and is announced in every Beacon frame. The PCF has higher priority than the DCF, because the period during which the PCF is used is protected from the DCF contention via the NAV. Under the PCF, the time axis is divided into repeated periods, called superframes, where each superframe is composed of a Contention Free Period (CFP) and a subsequent Contention Period (CP). During a CFP, the PCF is used by real-time traffic for accessing the medium, while the DCF is used by lower priority packets during a CP. It is mandatory that a superframe includes a CP of a minimum length that allows at least one MSDU (MAC Service Data Unit) delivery under the DCF at the lowest physical layer (PHY) rate [3] [15]. Figure 2.4 shows the PCF superframe with CFP and CP co-existence.

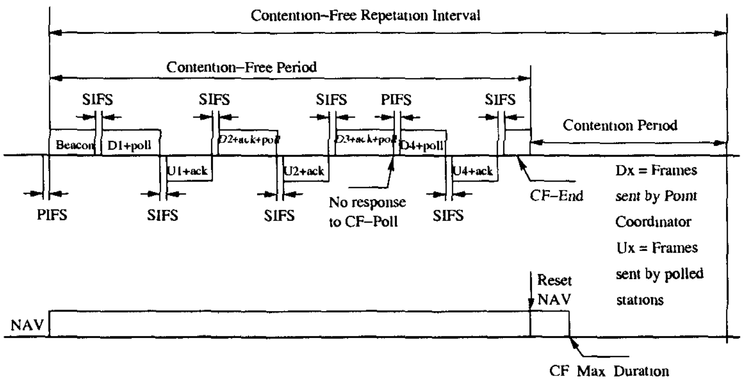

Figure 2.4: IEEE 802.11 PCF Channel Access Mechanism

As shown in Figure 2.4, a superframe starts with a Beacon frame, which is a management frame that maintains the synchronization of the local timers in MSs and delivers protocol related parameters. During a CFP, there is no contention among MSs; instead, PC polls MSs as the role of the polling master. See Figure 2.4 for the typical frame exchange sequences during a CFP. The PC polls an MS asking for a pending frame. If the PC itself has pending data for this MS, it uses a combined data and poll frame by piggybacking the CF-Poll frame on the data frame. A CF-POLL is used to poll an MS for the transmission of a data frame. Upon being polled, the MS acknowledges the successful reception of both the CF-Poll and data. If the PC receives no response from a polled MS after waiting for a PCF interframe space (PIFS) interval, it polls the next MS, or ends the CFP by sending a CF-End frame when the CFP period ends or if all MSs on the polling list have been polled and no more data has to be transmitted by the PC during the CFP. Upon receiving the CF-END, all MSs reset their NAV.

There are several problems with the PCF that led to the development of enhancements to the PCF protocol. The problems with the PCF protocol are as follows [5]:

- The transmission of the Beacon by the point coordinator depends on whether the medium is idle at the time of TBTT. After the medium is idle, the PC will get priority due to shorter PIFS. But the time at which the medium becomes idle is unpredictable. Thus the Beacon frame can get delayed affecting the time allocated to time-bounded traffic. This is referred to as the deferred Beacon problem of PCF.

- Furthermore, the duration of the transmission that happens after the polling is not under the control of the point coordinator.

- All the CF-pollable MSs have the same level of priority since they are simply polled one by one. The PC has to poll all MSs on its polling list, even if there is no frame to be sent. Since the CFP repetition rate is not dynamically variable, there is a trade-off between low latency applications requiring a fast repetition rate and an efficient use of the medium requiring slower repetition rate. Most of the time, such a trade-off would be difficult.

2.1.2 IEEE 802.11 MAC Extension

There have been many efforts to evaluate, extend, and revise the legacy IEEE 802.11 protocols in order to support a wider range of applications especially real-time services. Real-time traffic is going to have a bigger portion of the total load of any existing packet radio network, therefore, providing services to meet corresponding requirements becomes a critical task to researchers and engineers.

A relay-enabled PCF (rPCF) protocol was proposed in [42], where the AP collects channel information, and notifies mobile stations which data rate to use and whether to use a relay station. The basic idea behind rPCF is to exploit physical layer multi-rate capability, and in responding to different channel conditions. Data packets may be delivered through a much faster relaying link if the direct link can provide only low data rates. System throughput and transmission delay are improved significantly with small signaling overhead. However, both the AP and stations have to maintain a table in which channel conditions are collected and updated. Also all stations must be within the AP's coverage area, there is no coverage extension benefit achieved by multihop relaying. Mobility and handoff are not the consideration of this protocol either.

Two priority-based MAC layer protocols called ES-DCF and DB-DCF for real-time traffic in ad hoc wireless networks were proposed in [27]. The ES-DCF (elimination by sieving DCF) uses graded channel-free-wait-times to determine the packet's priority. Packets with smaller grades obtain higher priority class in accessing the medium. On the other hand, in the DB-DCF (deadline bursting DCF), each real-time station that wishes to access the channel transmits a black-burst of length inversely proportional to the urgency of its real-time data packet. The longer the black-burst is, the more emergent the real-time packet will be. Experiments confirmed that these two protocols perform well for real-time traffic in terms of throughput and latency. However, all stations in the experiment have to be able to hear one another at all times, no mobility, coverage extension, and handoff issues are taken into consideration. In addition, ES-DCF and DB-DCF are not backward compatible with the legacy 802.11 DCF protocol, and could not be laid on top of existing 802.11 WLANs [27].

The IEEE 802.11 task group is working towards a new MAC scheme called 802.11e [5] which defines a few enhancements to the PCF and introduces a new coordination function, called Hybrid Coordination Function (HCF), for the purpose of supporting real-time services in WLANs. The 802.11e MAC is backward compatible with the legacy 802.11 MAC, and hence it is a superset of the legacy MAC. Please note that one important new feature of the 802.11e HCF is the concept of transmission opportunity (TXOP), which is a time interval to allow a mobile station to transmit packets. The TXOP can be obtained either by Enhanced Distributed Channel Access (EDCA) contention (EDCA-TXOP), or by receiving a CF-poll frame from the AP (polled-TXOP). The value of TXOP is determined by the AP, and is broadcasted to all mobile stations via the Beacons or CF-poll frames. The purpose of using TXOP is to limit the time period a mobile station used to transmit frames. The following discussion is based mainly on [25].

The HCF composes two channel access mechanisms:

1. Enhanced Distributed Channel Access (EDCA)

   The EDCA is a contention-based channel access and operates only in contention period (CP). EDCA uses prioritized access categories (AC) to support QoS. There are four ACs labeled according to their dedicated applications, and associated with eight different user priorities (UPs) as shown in Table 2.1. They are AC_VO (Voice), AC_VI (Video), AC_BE (Best Effort), and AC_BK (Background) respectively. Accordingly, four channel access entities are required in one mobile station to accommodate each AC as depicted in Figure 2.5.

   Basically, EDCA uses AIFS [AC] to determine the priority of channel access. The AIFS [AC] is calculated by the priority level. A higher priority level has a smaller AIFS [AC] value which leads to a higher

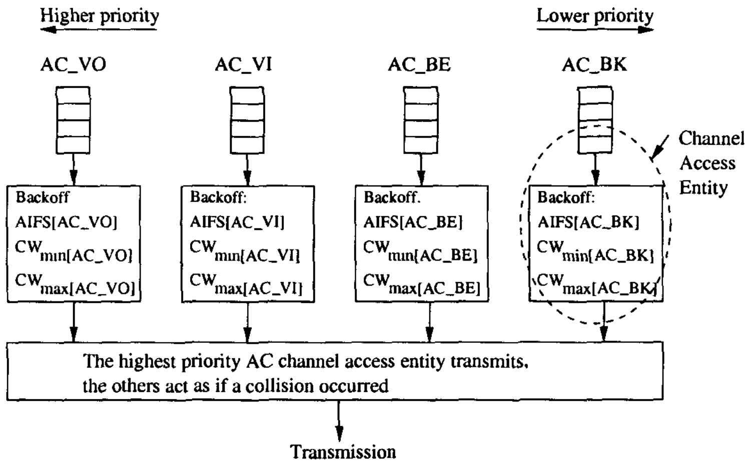

Figure 2.5: Channel Access Entities for EDCA

priority in accessing the channel. This also results in more bandwidth share and shorter channel access delay for a specific traffic condition.

2. HCF Controlled Channel Access (HCCA)

   The HCCA extends the channel access to both contention period (CP) and contention-free period (CFP). During CP, each 802.11e station begins its TXOP either when the medium is measured to be available under the EDCA rules, or when a channel access entity receives a polling frame from the hybrid coordinator (HC), which is co-located with the AP. During CFP, the HC specifies the starting time and the maximum duration of each TXOP using the CF-poll frames. In this case, the 802.11e channel access entities will not attempt to access the medium until it is explicitly polled by the HC. Hence, only the HC can allocate TXOPs by transmitting CF-Poll frames, or by immediately transmitting downlink data. During a polled TXOP, a polled station can transmit multiple frames that

Table 2.1: User Priority and Access Category in EDCA

Priority	User Priority(UP)	Access Category(AC)	Applications
Lowest	1	AC_BK	Background
.	2	AC_BK	Background
.	0	AC_BE	Best Effort
.	3	AC_VI	Video
.	4	AC_VI	Video
.	5	AC_VI	Video
.	6	AC_VO	Voice
Highest	7	AC_VO	Voice

the station selects to transmit according to its scheduling algorithm. However, developing a good scheduling algorithm is a challenging issue since the wireless medium involves the time-varying and location-dependent channel conditions.

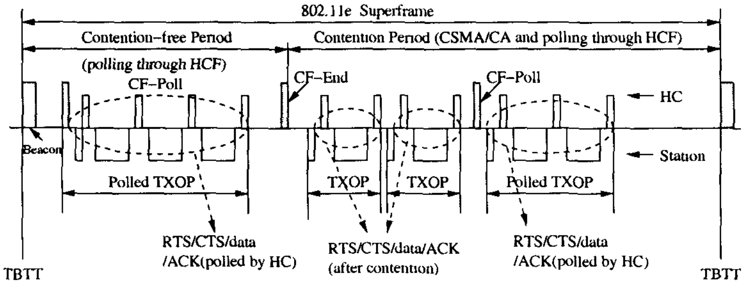

Figure 2.6: Example of IEEE 802.11e HCCA Channel Access

Figure 2.6 illustrates a superframe that includes a CFP and a CP. During the CP, the HC can also poll a station, but it is different from the PCF poll of the legacy 802.11.

2.2 Management Operations in Infrastructure IEEE 802.11 WLAN

The IEEE 802.11 management features were designed to reduce the effect of an unreliable medium, unauthorized users, and power consumption for battery-powered devices. Basically there are five different MAC management functions: (1) scanning, (2) authentication, (3) association, (4) power management, and (5) synchronization [3].

2.2.1 Scanning

In wireless environment, an MS must identify a compatible network before joining it. The process of identifying existing networks in the area is called scanning. In 802.11 infrastructure networks, the scanning can either be done passively by listening for Beacon messages from APs or actively by sending a Probe Request message on each channel, and listening on that channel for Probe Responses from APs.

An example of the passive scanning is shown in Figure 2.7. The MS sweeps from channel used by $AP1$ to channel used by $AP3$ to record Beacon frames. Beacons include information that allows an MS to find out everything it needs to match parameters with the AP and begin communications. If the MS receives Beacons from all three APs, it reports that it finds three APs. Passive

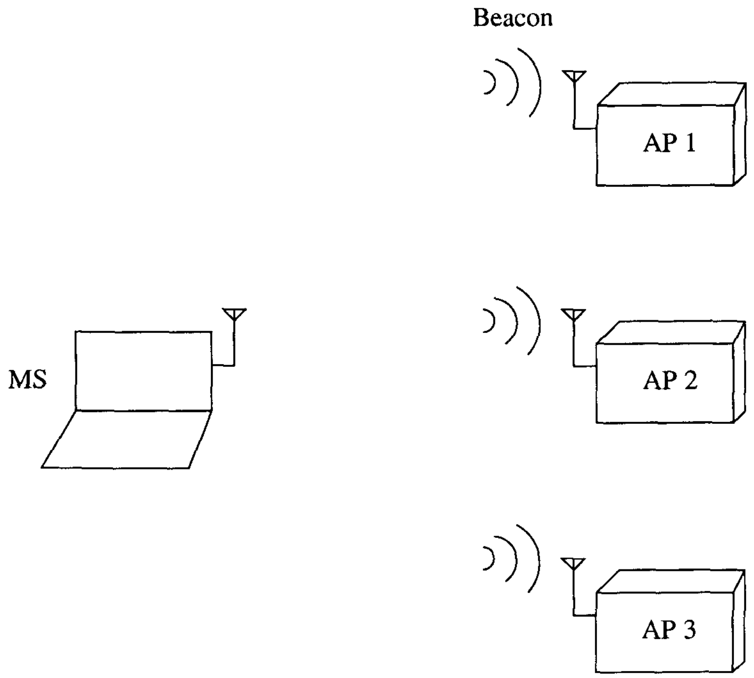

Figure 2.7: Passive Scanning Procedure

scanning saves battery power because it does not transmit.

In the active scanning, however, an MS broadcasts Probe Request frames on each channel to solicit responses from all APs in the area. Probe Response frames are generated by APs when they receive Probe Request frames. The Probe Responses are unicast management frames and are therefore subject to the positive acknowledgement requirement of the MAC.

It is common for multiple Probe Responses to be transmitted as a result of a single Probe Request. The purpose of the active scanning is to find every AP that the MS can join, so a broadcast Probe Request results in a response from every AP within the range.

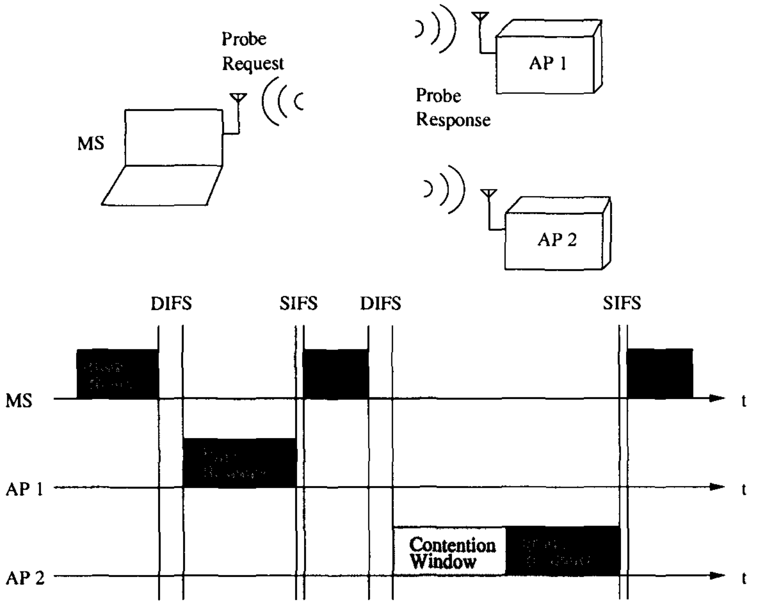

Figure 2.8: Active Scanning Procedure and Medium Access

Figure 2.8 shows the procedure of active scanning and the relationship between frames and various timing intervals during the scan. An MS sends a Probe Request after gaining access to the medium. Both access points respond with a Probe Response. Note that Probe Response from AP2 is subject to the rules of DCF and must wait for the contention window to expire before transmitting. The MS has to wait until the maximum response time has expired before processing the results. In areas with large number of APs, it may be necessary to adjust the maximum channel time so that the responses from all APs in the area can be processed.

After compiling the scanning results, an MS can decide to join one of the APs. Before this can happen, both authentication and association are required.

2.2.2 Authentication

Stations must authenticate with an access point before associating with it. Authentication is most useful in infrastructure networks. Network administrators may wish to authenticate mobile stations to ensure that only authorized users can access the 802.11 networks.

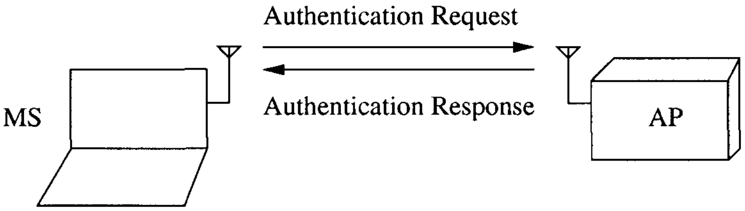

Figure 2.9: Frame Exchange during Authentication

Figure 2.9 shows a process of authentication frames exchanging between MS and AP. An MS sends an Authentication Request frame to notify its identity to the AP. In 802.11 networks, the identity of an MS is its MAC address, which must be unique throughout the network. The AP then processes the authentication request and returns its response by sending an Authentication Response frame.

2.2.3 Association

Once authentication has completed, stations can associate with an access point to gain full access to the network. Association provides the MS to AP mapping to the DS so that the DS can use this information to track the location of each mobile stations, and to accomplish its message distribution service [15]. Association is restricted to infrastructure networks. Once the association procedure is completed, a mobile station can use the distribution system to reach out to the world, and the world can respond through the distribution system. An MS can only associate with one AP at any given instant.

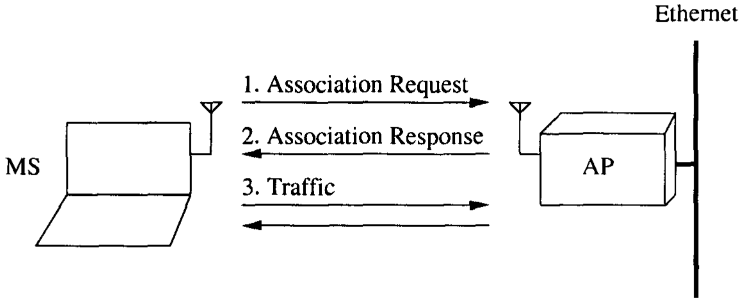

Figure 2.10: Association Procedure

A basic association procedure is shown in Figure 2.10. Once an MS has authenticated to an AP, it can issue an Association Request frame. The AP then processes the Association Request, and may grant the association by sending an Association Response with an Association ID (AID). The AID is a numerical identifier used to logically identify the MS to which buffered frames need to be delivered.

Once the MS has associated with an AP, the AP begins processing frames for the MS. In commonly used IEEE 802.11 products, the distribution system medium is Ethernet. When an AP receives a frame destined for an associated MS, that frame can be bridged from the Ethernet to the wireless medium or buffered if the MS is in a power-saving state. In shared Ethernets, the frame will be sent to all APs and will be bridged by the correct one. In switched Ethernets, the mobile station's MAC address will be associated with a particular switch port. That switch port is then connected to the AP currently providing service for the station.

2.2.4 Power Management

Many IEEE 802.11 devices are battery-powered. The battery power is a scarce resource which can only run a certain time before it needs to be recharged. However, many wireless applications require long battery life without sacrificing network connectivity. Therefore, IEEE 802.11 standard supports a power conservation mode, which is achieved by minimizing the time spent in the active mode and maximizing the time spent in the power-saving mode. If an MS is in the active mode, it is fully powered. A station on the polling list of a PC has to be in the active mode for the duration of the CFP. Whereas when an MS in the power-saving (PS) mode, it is able neither to receive nor transmit, and consumes very low power.

Power management can achieve the greatest savings in infrastructure networks. Because all traffic for MSs must go through APs and APs remain active all the time, so APs are ideal to buffer traffic for those MSs who are in the PS mode. An MS can inform its power management state to its associated AP via frame exchange. The AP buffers frames for MSs in PS mode, and announces periodically which stations have frames waiting for them in a Traffic Indication Map (TIM) included in all Beacons generated by the AP. Mobile stations must wake up and enter the active mode to listen for Beacon frames to receive TIM. An MS then examines the TIM to determine if the AP has buffered frames on its behalf, and may poll the AP for the delivery of buffered frames during the Contention Period using a PS-Poll frame. After transmitting the PS-Poll, an

MS must remain awake until either the polling transaction has concluded or all the buffered frames for the MS are delivered or discarded. The buffering and delivery process is illustrated in Figure 2.11, which shows the medium as it appears to an AP and two associated power-saving MSs.

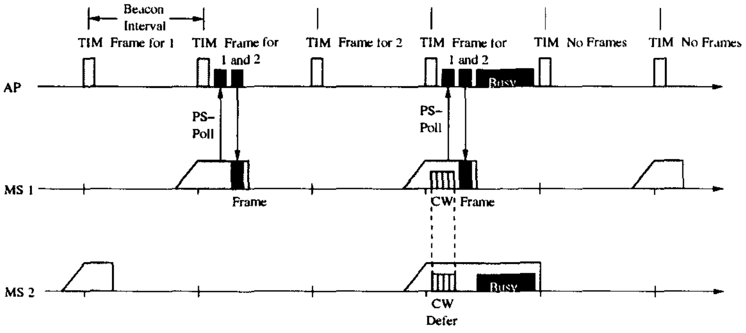

Figure 2.11: PS-Poll and Buffered Frames Retrieval Process

In this simplified figure, the AP transmits a Beacon frame with a TIM element in every Beacon interval. MS 1 is assigned a listen interval of 2, so it must wake up to receive TIM every 2 Beacon intervals, while MS 2 has a listen interval of 3, and it wakes up every 3 Beacon intervals. The lines above the MS base lines indicate the ramp-up process of the receiver to listen for the TIM. At the first Beacon interval, MS1 is in sleep and MS 2 wakes up, the TIM indicates that there are no frames buffered for MS2, so it returns to sleep immediately. At the second Beacon interval, the TIM indicates that there are buffered frames for both MS1 and MS2, but only MS1 wakes up, so MS1 issues a PS-Poll and receives the frame in response, then it returns to sleep. Both MS1 and MS2 are asleep during the third Beacon interval, and wake up at the fourth Beacon to listen to the TIM, which indicates that there are frames buffered for both of them. MS1 and MS2 prepare to issue PS-Poll frames after the expiration of a contention window (CW) countdown. In this example, MS1 has shorter random delay, so it issues a PS-Poll and receives its buffered frames in response. MS2 differs during the MS1 transmission, and fails to seize the medium after MS1 has completed, because the third party gains the access to the medium, which is shown as busy in the figure. In this case, MS2 must stay awake until it receives the next TIM. If the AP has run out of its buffer space and has discarded the buffered frames for MS2, which is indicated in the TIM at the fifth Beacon frame, MS2 can then return to sleep mode again.

MSs may switch from a PS mode to an active mode at any time. The information of power management is included in the frame control field of each data frame sent to an AP. When an MS switches to the active mode, frames can be transmitted without waiting for a PS-Poll frame.

2.2.5 Synchronization

As a wireless network, IEEE 802.11 depends a great deal on maintaining and updating timing information to all MSs. Each MS in a basic service area maintains a copy of the timing synchronization function (TSF) in addition to its local station timing. The TSF is a local timer synchronized with the TSF of every other station in the same BSA. Beacon frames are used to periodically announce the value of the TSF to other stations in the network.

Timing in infrastructure networks is quite similar to the power management since they both based on the use of access points as central coordinators. APs are responsible for maintaining the TSF time, and any MS associated with an

AP must simply accept the AP's TSF as valid.

When an AP prepares to transmit a Beacon frame, it makes a copy of its timer into the Beacon's timestamp field. MSs received the Beacon frame accept the timing value, but may add a small offset to the received timing value to account for local processing. MSs have to maintain local TSF timers. In case of missing Beacon frames occasionally, local TSF timers enable MSs remain roughly synchronized with the global TSF.

Timing values are also distributed in Probe Response frames. When an MS scans a network, it saves the timestamp from the Beacon or Probe Response, and adds the value of local offset to match the local timer to the network timer.

2.3 Mobility Management

Mobility is the most important feature of a wireless mobile network since users expect to be able to communicate anywhere at anytime. The network should support continuous connections when an active mobile station roams from one coverage area to the other. This is commonly referred to as a handoff. With the rapid growth and deployment of IEEE 802.11-based wireless networks in recent years, handoff has become a critical issue to the 802.11 MAC operation since mobile stations tend to move around freely in the whole network, which leads to the transference of data connections from one associated AP to another.

The IEEE 802.11 WLAN supports three types of station mobility: (1) static or intra-BSS movement, (2) inter-BSS movement, and (3) inter-ESS movement [28]. The inter-ESS transitions are only supported when it is easy to obtain association with an access point in the new extended service area. IEEE 802.11 does not support seamless inter-ESS transitions since the active network connections are likely to be dropped when the mobile station leaves its original ESS [15]. Higher-layer cooperation is also required to support the inter-ESS transition. In this thesis, we investigate only handoffs that relate to inter-BSS movement, which is defined as the movement of an MS from one BSS to another one within the same ESS. The inter-BSS movement is supported by the reassociation service defined in the IEEE 802.11 MAC protocol [3]. Typically, a handoff process starts when an MS is moving away from the AP with which it is currently associated and is experiencing signal quality degradation. The MS continuously monitors the signal strength and quality from all access points in the ESS coverage area, then scans all the possible channels and tries to locate another AP with the best link quality. If such an AP exists, the MS proceeds with authentication and reassociation procedures to join the BSS of the new AP. This process is depicted in Figure 2.12. APs with overlapping coverage areas are commonly configured to operate on different frequency channels to avoid interference between the adjacent cells.

Most traditional handoff schemes rely on the measured received signal strength (RSS). Figure 2.13 shows an MS which is moving from one AP ($AP1$) to another AP ($AP2$). The mean signal strength of $AP1$ decreases as the MS moves away from it. In the mean time, the mean signal strength of $AP2$ increases as the MS approaches it. The mean signal strength is the average signal strength over a time period so that rapid fluctuations due to multipath fading can be eliminated. Figure 2.13 illustrates various handoff algorithms based on

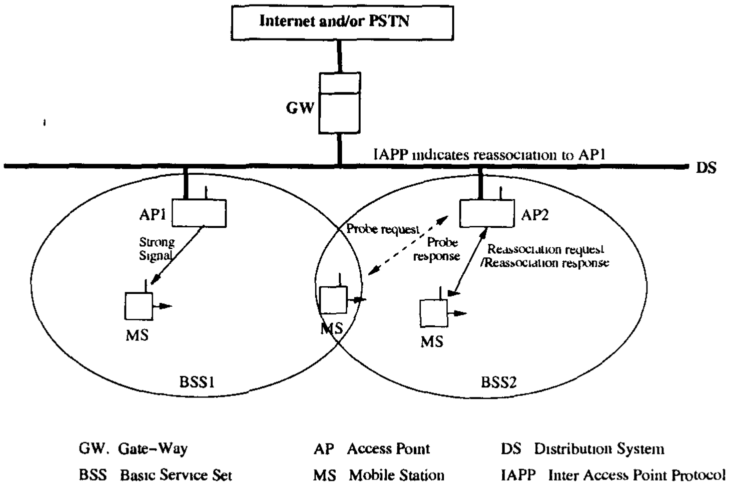

Figure 2.12: Handoff in IEEE 802.11 Infrastructure WLAN

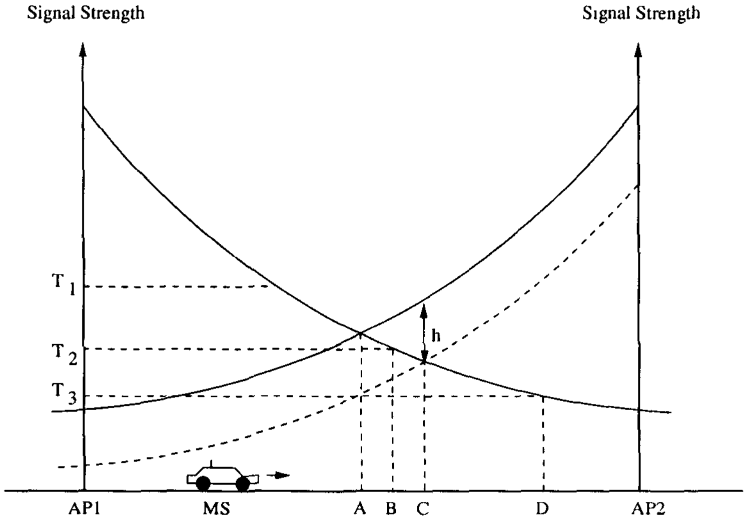

Figure 2.13: Illuatration of Handoff Algorithms

RSS [26].

1. Received Signal Strength (RSS)

The handoff decision is based on the RSS at the MS on the downlink from access points. Handoff is initiated when the RSS from the approaching AP is greater than the RSS from the serving AP, i.e. RSS $(AP2) >$ RSS $(AP1)$. In Figure 2.13, the handoff would occur at point A. This method may initiate frequent unnecessary handoffs when the signal strength from the serving AP is still adequate to give quality of service (QoS), i.e. RSS $(AP1) > T$ where T is the threshold required for QoS. This is called ping-pong effect.

2. Received Signal Strength (RSS) with Threshold

In this approach, a handoff is initiated when the RSS from the serving AP falls below a certain threshold value T and the signal strength from the approaching AP is greater than the RSS from the serving AP, i.e. RSS$(AP1) < T$ & RSS$(AP2) >$ RSS$(AP1)$. In this method, proper choice of the threshold is important. Ideally, the point where identical signal strengths from two APs are met is the middle point between these two APs. If the chosen threshold is higher than this value, for instance, T_1 in Figure 2.13, the effect is similar to the RSS scheme, and the handoff occurs at point A. If the chosen threshold is less than this value, say T_2 in Figure 2.13, the handoff will not happen until signal strength of the serving AP crosses this threshold value at point B. If the chosen threshold T_3 is much less than the above T_1 and T_2, the handoff delay may be high and the MS moves far into the new cell. This may degrade the quality of the communication link and result in call dropping. It also causes interference to co-channel users.

3. Received Signal Strength (RSS) with Hysteresis

   In this approach, a handoff is initiated only if the RSS of the new AP is sufficiently stronger by a hysteresis margin (h) than the RSS of the serving AP, i.e. RSS($AP2$) > RSS($AP1$) + h. In this case, the handoff would occur at point C as shown in Figure 2.13. This scheme prevents the ping-pong effect. But this scheme involves in unnecessary handoffs when the RSS of the serving AP is sufficiently strong.

4. Received Signal Strength (RSS) with Hysteresis and Threshold

   In this approach, a handoff is initiated only if the RSS of serving AP drops below a threshold and signal strength of the new AP is stronger by a hysteresis margin, i.e. RSS ($AP1$) $< T$ & RSS ($AP2$) > RSS ($AP1$) + h. In Figure 2.13, the handoff would occur either at point C if the threshold is T_2 or at point D if the threshold is T_3. This scheme can be used to reduce the unnecessary handoffs further when the signal strength of the serving AP is still strong enough to maintain the link.

When a mobile station (MS) experiences degraded signal quality between itself and the AP it is currently associated with (e.g., by measuring the quality of the received Beacons), it will start a handoff procedure. If locations of APs are selected carefully, and the handoff threshold value is configured so that a handoff is triggered before losing the connectivity with the current AP, then the time to detect movement will not affect the total handoff latency. To find a candidate AP to reassociate with, the MS will start to scan the different radio channels. Scanning can either be done passively by listening for Beacon messages from APs or actively by sending a Probe Request message on each channel, and listening on that channel for Probe Responses from APs. Messages $A - D$ in Figure 2.14 illustrate an active scanning procedure. The MS sends at least one Probe Request and receives zero or more Probe Responses per channel depending on the number of APs on that channel serving the ESS specified in the Probe Request. This phase of the handoff is referred to as the discovery phase.

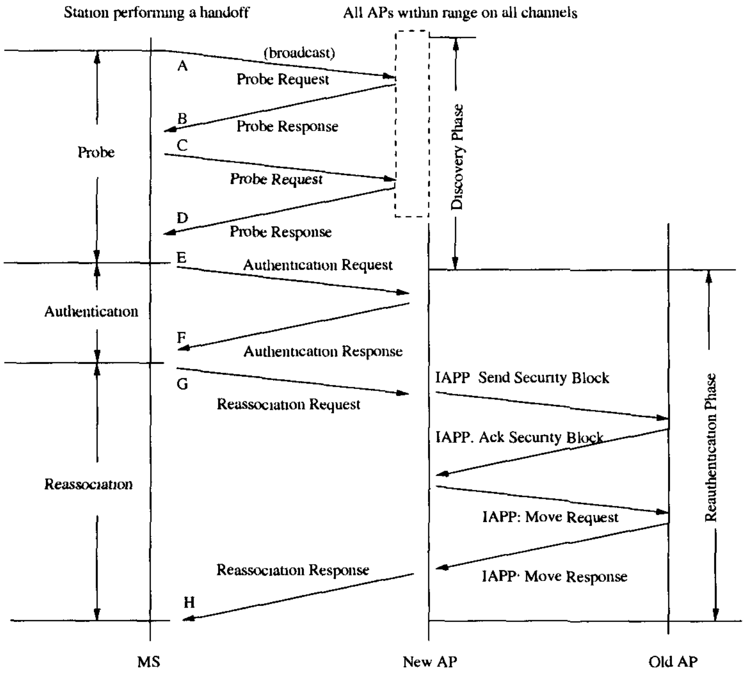

Figure 2.14: Handoff Procedures in IEEE 802.11 Infrastructure WLAN

When an MS has finished scanning for candidate APs, it will initiate the reassociation procedure with the AP which is the best of all candidate APs. The factors used to make this decision are product dependent. A reassociation can be divided into two sub-procedures, the authentication message exchange (messages E and F in Figure 2.14) and the reassociation message exchange (message G to H in Figure 2.14). This handoff procedure is referred to as the reauthentication phase. During this period, information has to be exchanged between the old AP and new AP, that is, the new AP needs to inform the old AP that the mobile station is now associated with it, and all frames destined to this mobile station will go through this new AP. This communication between APs is supported by the distribution system (DS) through so-called inter access point protocol (IAPP) [4], and is illustrated in Figure 2.14.

2.4 Relaying in IEEE 802.11 Infrastructure Networks

Because of the short transmission range of IEEE 802.11 radios [18] [17], 802.11 access points are mostly deployed in either hot spots where a high density of low-mobility users exist, or for a group of subscribers gathering in an office building/convention center. However, there are incremental demands for 802.11 WLANs with large coverage area, invulnerable radio link, and more flexible mobility in practice. Such environments include highways, university campuses, battlefields, and rescue environments. Relaying through mobile stations turns out to be a robust solution for these problems as we discussed in Section 1.1.

In contrast with many other mobile multihop network architectures, we focus on a relay scheme that uses one additional hop to forward packets. The two-hop relaying architecture can provide an uncomplicated architecture to enhance the system performance while avoiding the possible drawbacks of multihop systems in packet delay, signaling overhead, and system complexity [35].

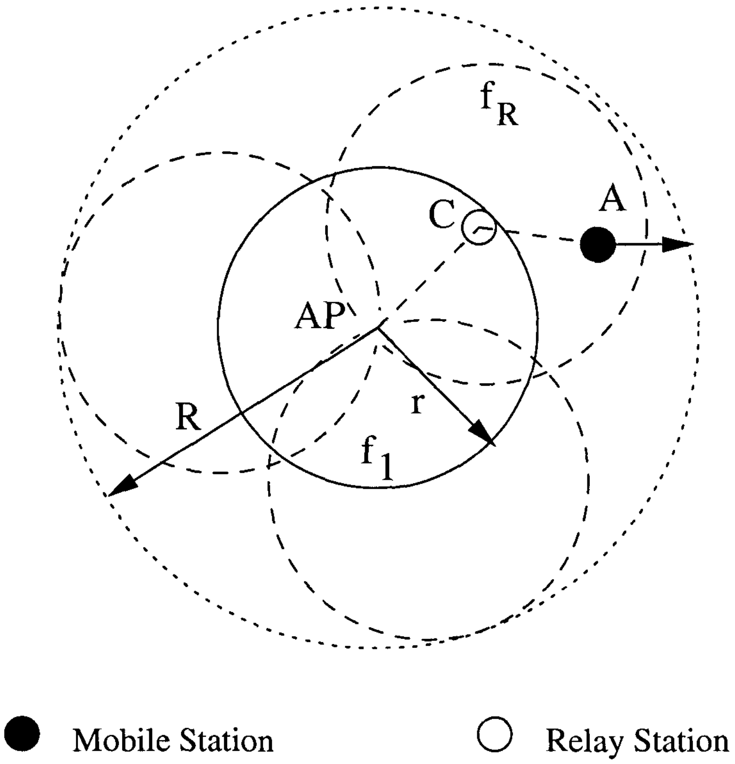

Figure 2.15: Example of WLAN coverage area

Figure 2.15 shows an IEEE 802.11 infrastructure WLAN coverage area with and without applying two-hop relaying. The solid circle is the original coverage area of the AP, whereas the dashed circle depicts the extended coverage area provided via relay stations. The coverage extension depends upon the ratio of R to r, where R is the radius of the potentially extended coverage area of the AP which is determined by the location and transmission range of mobile station. r is the original coverage radius of the AP which is determined by the transmission range of the AP. In this figure and the rest of this thesis, to simplify the analysis, we assume that the mobile stations and the APs have the same circular transmission range, ideally, R is twice as large as r. An example of coverage extension is also shown in Figure 2.15. In this figure, MS A is outside of the original coverage area of the AP, and builds a relaying connection with AP via relay station C. The depicted relaying system has obviously extended the coverage area and is able to support much more freedom of customer mobility.

In this thesis, we assume that whenever relaying is performed, a relay channel, which is different from the one the MS is using, will be employed for the relaying link between the relay station and the mobile station. This channel can be used by relay stations to perform multi-hop relaying while accommodating conventional IEEE 802.11 end users without any modification to existing devices.

Relaying in an IEEE 802.11 infrastructure network, using other terminals, differs from an ad hoc network in that there is a central controller - access point (AP) in the infrastructure network. Based on this, following advantages and disadvantages, comparing an IEEE 802.11 infrastructure network with an ad hoc network, are observed:

Advantages:

- AP can buffer and forward frames for stations operating in the power saving mode.
- Improved line-of-sight (LOS) reduces peak power consumption by both the access point and the mobile station, which may result in reduced interference and increased system capacity.

- Multihop relaying via other mobile stations provides flexible path diversity.

- Dead spots can be reduced and load balancing can be improved by using multihop relaying.

Disadvantages:

- Requires a strategic relay station/path selection scheme.

- Requires additional channel for relaying purposes (although, this also applies in ad-hoc networks).

- Requires an efficient link maintenance strategy.

- Requires a strategic handoff algorithm.

- Requires cooperation among mobile stations as well as cooperation among APs, relay stations, and mobile stations.

- May require a high subscriber density to perform relaying effectively.

In this thesis, we will address aforementioned disadvantages and investigate solutions in our proposed AAHO protocol.

Chapter 3

Ad Hoc Assisted Handoff (AAHO) in IEEE 802.11 Infrastructure WLANs

In this chapter, we propose and investigate the use of ad hoc assisted handoff (AAHO) for real-time voice in IEEE 802.11 infrastructure WLANs. The discussion starts from an example of system architecture. Then, three versions of AAHO are proposed. Followed by a detailed description of IEEE 802.11 MAC protocol extension in supporting the multihop operation of AAHO. Procedures of link maintenance and handoff are given, and a relay station selection criterion is presented with an example. Finally, we give two compatible implementation options for performing AAHO in IEEE 802.11 infrastructure WLANs.

3.1 System Architecture

An example of IEEE 802.11 infrastructure network where there are two APs, AP_1 and AP_2, each having its own geographic coverage area is shown in Figure 3.1. Both AP_1 and AP_2 are connected via a wired LAN to the Internet and/or PSTN. Each AP can provide voice and data services to a population of mobile stations (MSs). Two different frequencies f_1 and f_2 are used by AP_1 and AP_2 respectively to reduce the impact of interference. MSs are able to move around freely within the entire system. The network has poor single hop coverage, mostly experienced by mobile stations located at the coverage gap of the cells or under deep shadowing dead spots. For example, in Figure 3.1, MS A is out of AP_1's coverage range, but has not entered into AP_2's coverage range. So it is not able to build a direct connection with either AP_1 or AP_2.

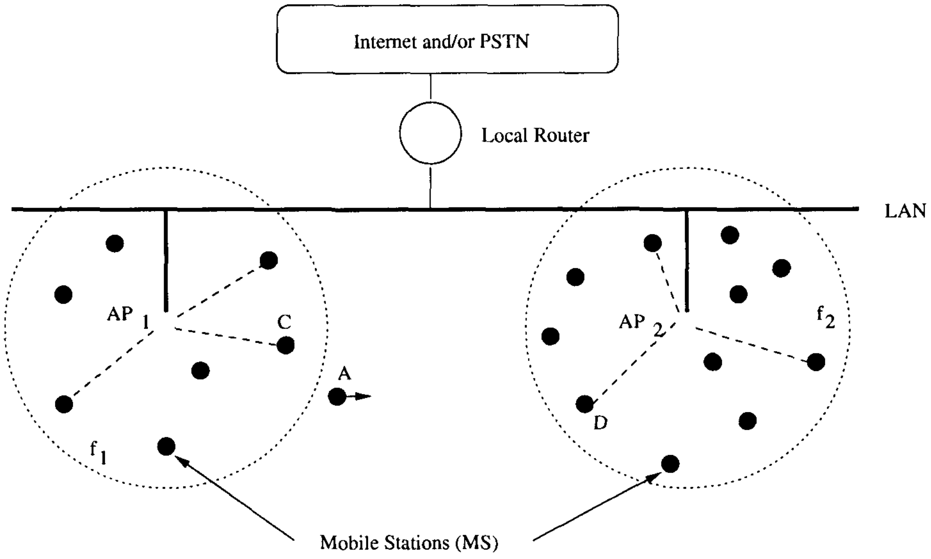

Figure 3.1: IEEE 802.11 Infrastructure Network

Three main network entities are considered in this thesis. They are access point (AP), relay station (RS), and mobile station (MS). A normal mobile station can offer itself as a relay station for other peer mobile stations if required. There are no special relay entities in the network, hence no additional infrastructure is needed. This leads to an easy implementation.

In this thesis, we assume that APs operate in different frequencies in such a way that there is negligible interference between different APs. This is possible because the IEEE 802.11 standard defines multiple physical channels in the PHY layer, for example, 3 non-overlapping channels in IEEE 802.11b and 8 in IEEE 802.11a [1] [2] in North America. Whenever a relaying is performed, a different frequency, which is not used by any of the nearby APs, is used by relay stations in the second hop. This channel is referred to as relay channel (R_CHANNEL), whereas the channel used by the AP is referred to as home channel (H_CHANNEL). The reason for using a separate frequency for relaying is that transmitting and receiving at the same channel as H_CHANNEL will yield excessive interference and subsequently reduce network capacity.

When an MS with an active connection associates with an AP and then moves from the coverage area of this AP to another, it will search for an alternative AP to hand over the connection by performing conventional IEEE 802.11 reassociation discussed in Section 2.3. The APs involved in this handoff will employ the IAPP protocol [4] to facilitate changes in networking required to enable the handoff. If there is a coverage gap between these two adjacent APs as depicted in Figure 3.1, the normal IEEE 802.11 handoff will not succeed, and the connection will be terminated. An example of this case is shown in

Figure 3.1. For this case, MS A moves out of the AP_1's coverage area, and can not be covered by AP_2, and thus its connection with AP_1 will be dropped.

3.2 Ad Hoc Assisted Handoff (AAHO)

To deal with problems mentioned above, a mobile station not carrying any traffic is employed to forward the traffic of MS A to a proper AP in two hops. This is called ad hoc assisted handoff (AAHO) [16]. In AAHO, an additional ad hoc hop may sometimes be used by an MS to obtain the required coverage range extension or channel quality needed to maintain real-time performance. The maximum number of hops is limited to two, this constraint balances the tradeoff between routing complexity, radio link reliability, and corresponding delay in processing and propagation.

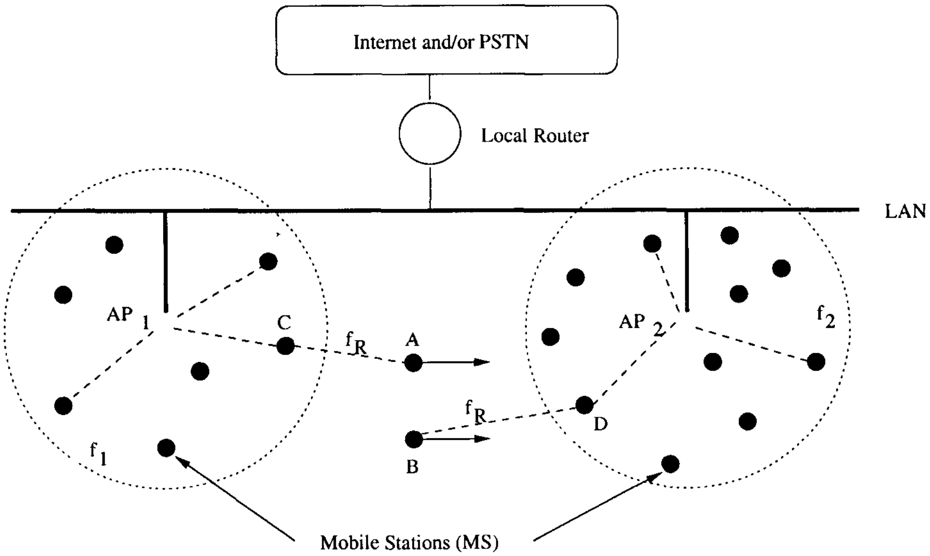

Figure 3.2: Forward and Backward Ad Hoc Assisted Handoff

An example of AAHO is shown in Figure 3.2. In each cell, dashed lines illustrate connections between MSs and their currently associated AP. MSs are able to support real-time voice services and are able to act as relay stations if required. An MS, which is associated with an AP first, can initiate a real-time voice connection with the AP, and may move in a specific mobility pattern. If the MS moves to an area out of the coverage of both APs, one of the idle MSs between the AP and the MS, for example MS C for MS A and MS D for MS B in Figure 3.2, will volunteer itself as a relay station to create a two-hop path for the MS. A separate frequency f_R is used to eliminate interference between relay link and the original link.

There are three types of AAHO proposed in this thesis:

- Backward Ad Hoc Assisted Handoff (BAAHO)

  In BAAHO, when an MS's MS/AP link quality drops below a predefined threshold, it will create a 2-hop path via an idle MS backwards to the same AP to which it is currently associated. An example of BAAHO is shown in Figure 3.3, where MS C is acting as a relay station (RS) for MS A's real-time connection to the same access point AP_1. If we assume the MS and the AP have the same transmission range, ideally the BAAHO can double the AP's coverage radius. In Figure 3.3, the AP's original coverage area is shown in solid lines and the extended coverage area is shown in dashed lines.

- Forward Ad Hoc Assisted Handoff (FAAHO)

  In FAAHO, when an MS's current MS/AP link quality drops below a

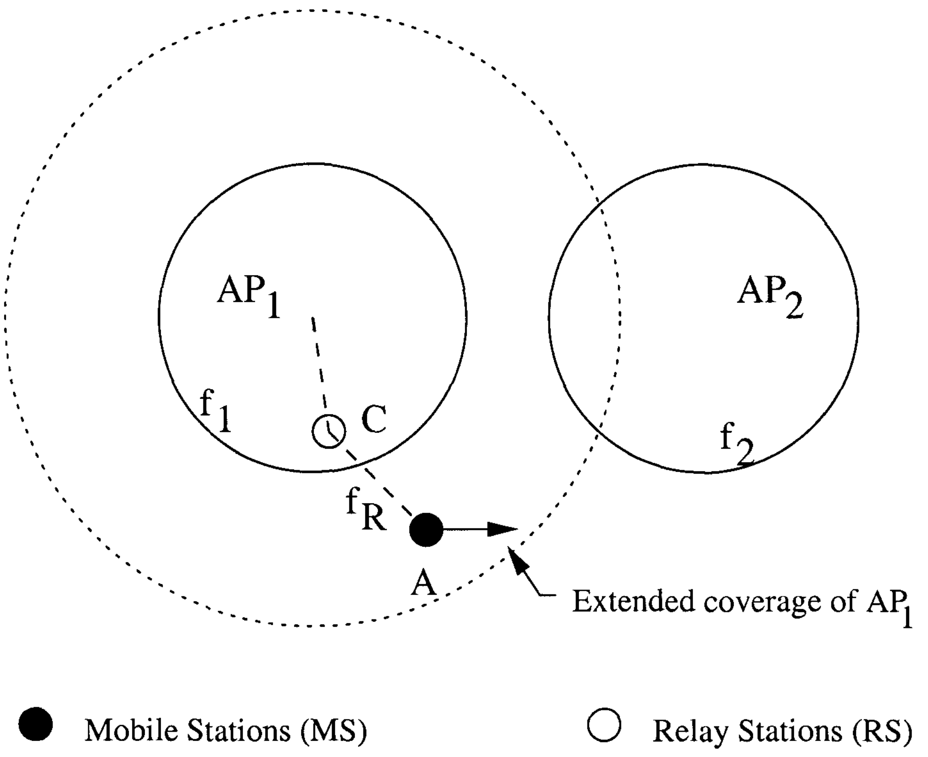

Figure 3.3: Example of BAAHO

predefined threshold, the MS will create a 2-hop path via an idle MS to an AP which is different from its original associated AP. In this case, the relay station (RS) is an MS that is associated with a different AP and has both good RS/AP and RS/MS link quality. An example of FAAHO is shown in Figure 3.4 where MS A's packets are forwarded to AP_2 through the relaying of MS D. It is obvious that using FAAHO alone does not make any realistical sense since the MS may move out of its current associated AP's coverage, but may not reach the extended coverage area of a new AP. In this case, the MS has to stay with its current serving AP by BAAHO to keep the connection.

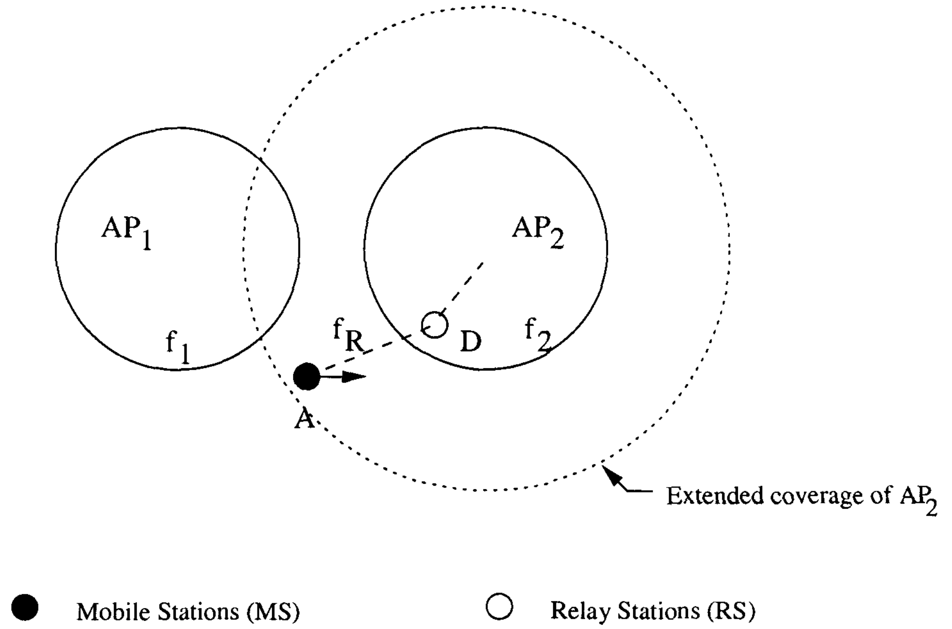

Figure 3.4: Example of FAAHO

- Hybrid Ad Hoc Assisted Handoff (HAAHO)

  HAAHO is shown in Figure 3.5 where an MS can perform either BAAHO through RS C or FAAHO through RS D, depending on which RS has the best link quality according to the link selection criterion which we will discuss in the following section. When an MS which is performing BAAHO moves out of the extended coverage area of its currently associated AP, or it is still in the extended coverage area of the AP but there is no RS available to perform BAAHO, the MS is handed over to a new AP by performing FAAHO.

Conceptually, performing AAHO is not much more complex than a conven-

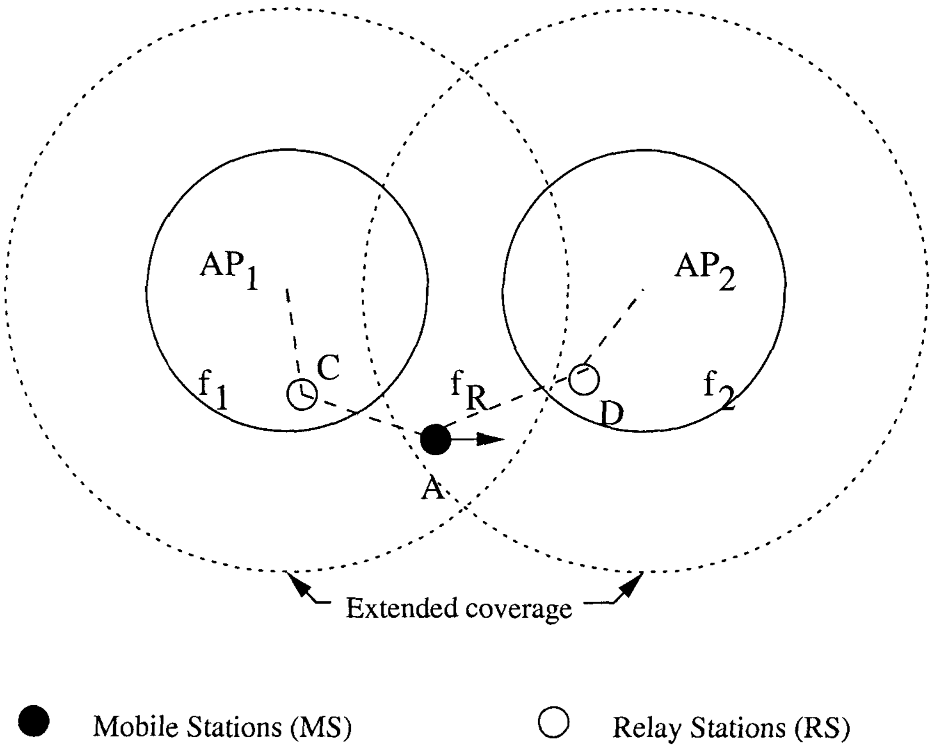

Figure 3.5: Example of HAAHO

tional IEEE 802.11 handoff. This is due to the fact that an AAHO handoff just replaces a single poor quality link between the MS and the AP with a single high quality link between the MS and an RS since the RS already has a good RS/AP link. Also, both BAAHO and FAAHO use 2-hop paths in operation but there are obvious differences between these two schemes. In theory, a BAAHO can be set up with much lower latency since BAAHO does not change its serving AP, thus it involves less infrastructure coordination. By comparison, an FAAHO requires infrastructure interaction since it involves in selecting and switching to a new serving AP. Note that in both BAAHO and FAAHO, the

2-hop path will be replaced immediately with a single MS/AP link whenever the MS moves into the original coverage area of an AP. By doing this, the RS is released and the MS reassociates with the AP directly. Obviously, depending upon mobility patterns, this may not be possible in some cases. In BAAHO, the final handoff to a single MS/AP link will require infrastructure cooperation if the AP is a different one, whereas the final handoff for FAAHO will ideally not require as much infrastructure coordination when the MS moves into the AP's original coverage area.

3.3 IEEE 802.11 MAC Protocol Extensions

Since the conventional IEEE 802.11 infrastructure MAC protocol [3] does not support multihop operation, MAC protocol extensions are required to facilitate the operation of AAHO and relay station functionality. In this section, we will describe how an IEEE 802.11 mobile station functions as a potential RS for AAHO.

An MS in the original coverage area of an AP first associates with this AP using normal infrastructure mode procedures [3]. The channel used by the AP is referred to as the MS's home channel or H_CHANNEL. Any MS which is currently not carrying active traffic may offer itself as a potential RS. In this case, it indicates to the AP that it is operating in IEEE 802.11 DCF power saving (PS) mode. Operating in PS mode ensures that inbound packets arriving for the station will be buffered at the AP, to await download by the MS using PS-Poll procedures as discussed in Section 2.2.4. The MS must wake up and switch to active mode at each Beacon corresponding to its listen period and listen to Beacon frames to receive the traffic indication map (TIM). The TIM contains information to indicate which stations have buffered packets waiting to be picked up. By checking the TIM, the MS can determine if there is buffered traffic in the AP on its behalf. Then the MS can retrieve the buffered packets using PS-Poll control frames. When multiple mobile stations have buffered frames, all stations with buffered packets must use the random backoff algorithm before transmitting the PS-Poll. While operating in this mode, the MS can now make itself available as a potential RS. In the time periods between home channel awakenings, the MS moves its radio to the relay paging (RP_CHANNEL) channel and listens for RS probe packets (RS_PROBE). While performing this operation, it periodically returns to its H_CHANNEL as described above. This process is illustrated in Figure 3.6, where the activity of RS on the H_CHANNEL is shown above the time line, whereas the RS activity on the RP_CHANNEL is shown below the RS time line. Similarly, the activity of MS on the RP_CHANNEL is also shown above the MS time line.

Now consider the actions of an active voice MS. We will assume that when the station initiates a voice connection it is associated with an AP following a normal association procedure. When the link to the AP drops below an AP's search threshold, the MS begins probing for a new AP. If a suitable AP is found, the connection can be handed off in the usual manner of IEEE 802.11 reassociation. In the case of no such an AP exists for normal handoff, the MS also has the option to search for an RS in between the MS and the relevant AP

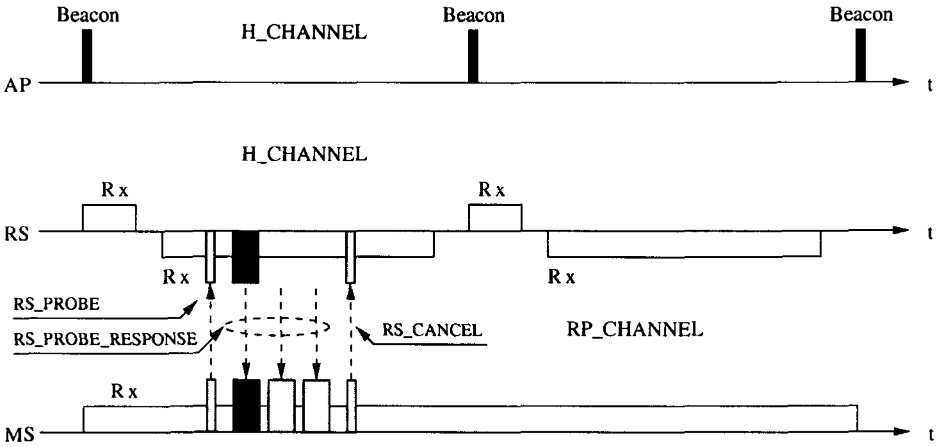

Figure 3.6: Relay Station Probing Procecss

as follows. To look for an RS, the MS sends a multicast RS_PROBE packet on the RP_CHANNEL. The RS_PROBE includes information identifying the home AP and the quality of the current link. All potential RSs that receive the RS_PROBE will measure the quality of the link between the probing MS and itself, and that between itself and the AP. Based on all information obtained, one or more potential RSs may reply to the RS_PROBE, by sending a unicast RS_PROBE_RESPONSE packet on the RP_CHANNEL to the probing MS. Since more than one potential RS may respond to the RS_PROBE. In order to control unnecessary transmissions, the responses are prioritized according to the relay station selection criteria (RSSC) being used. There are a number of ways in which this can be accomplished and one simple method is to map the range of possible selection priorities to a time deferral range, with higher priority giving smaller deferral values. Using this scheme, when a potential RS receives an RS_PROBE, it will not reply with an RS_PROBE_RESPONSE until its deferral value has expired. Once the probing MS has received one or more RS_ PROBE_RESPONSEs, it can cancel the probe by sending an RS_CANCEL packet. RS_CANCEL is a multicast packet containing an identifier that associates it with the original RS_PROBE. Stations who receive the RS_CANCEL packet will cancel their pending RS_PROBE_RESPONSE transmissions for that probe. This process is also illustrated in Figure 3.6. Once the soliciting MS has selected an RS, the two stations can relay packets between them on a relay channel, i.e., the R_CHANNEL. In most cases the R_CHANNEL will be the same as the RP_CHANNEL, but it could be a different available channel. In the former case MAC level prioritization is used to ensure that voice and probe related transmissions are given higher access priority to the channel.

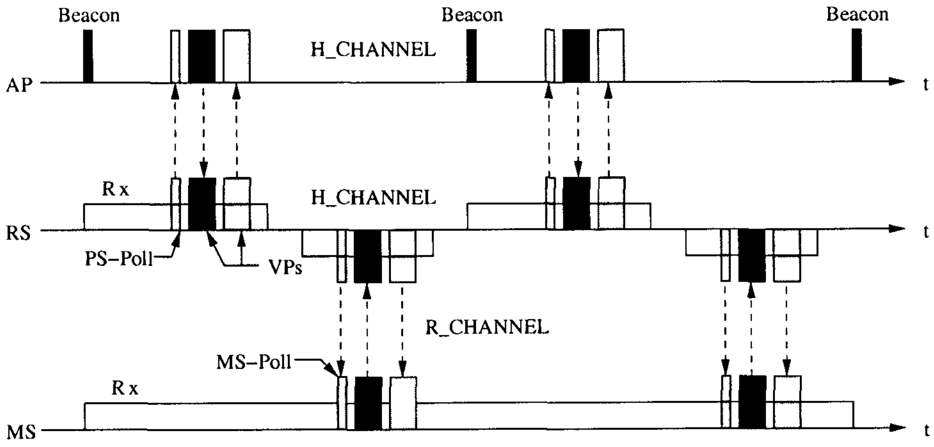

Figure 3.7: Relay Station Operation During AAHO

When voice relaying is in progress, the RS is responsible for bridging voice packets between the R_CHANNEL and H_CHANNEL. To best mitigate time synchronization requirements, the RS operates as a master in this case, polling for voice packets on both channels. An example of this is given in Figure 3.7. Three time lines are shown illustrating the activities of the AP, RS and MS during an AAHO. To simplify things, the time line is condensed and only shows packets relevant to this discussion. The AP resides on the H_ CHANNEL and the MS on the R_CHANNEL as shown in the figure. The RS however bridges between the two channels. Activities of the RS on the H_CHANNEL are drawn above the RS time line, and those on the R_CHANNEL are shown below the RS time line. On the R_CHANNEL, the RS periodically transmits downstream voice packets and polls the MS for upstream packets. The voice packets are marked VPs in the figure, and the poll is shown as MS-Poll. On the H_CHANNEL the RS periodically transmits uplink voice packets and polls for downlink voice packets using the IEEE 802.11 PS-Poll mechanism. In the figure, we have assumed that the beacon rate is the same as the voice packet generation rate, but this need not be the case. By setting the RS as a polling master, the dual-frequency operation is easily accomplished without the packet loss. Using the same procedures described above, an MS can easily perform successive FAAHO and/or BAAHO. It should be noted that the MS/RS relaying described above does not necessarily imply a formal IEEE 802.11 association between the two stations. The ability to perform this is currently available in certain IEEE 802.11 chipset designs, but may require firmware alterations in others.

3.4 Link Maintenance and Handoff

When mobility is taken into consideration, and mobile stations are used as relay stations, it is not easy to build and maintain a stable connection as mobile stations move randomly. Frequent path reconfiguration is required. If there were no relay stations available to forward the packets to the AP, forced termination would occur. Handoff is thereby a challenging issue to be dealt with. When a mobile station moves from one AP's coverage area to another, a proper handoff procedure should be able to keep the connection continuous, which is especially important for real-time voice.

When an active MS is associating with an AP in direct connection, it normally monitors the quality of the link using RSSI (received signal strength indication) measurements obtained from Beacons and other packets transmitted by the AP. When the RSSI drops below a preset threshold, HO_Threshold, the MS initiates a search for an alternate AP using IEEE 802.11 active scanning [3]. If a new AP exists, the MS is reassociated with this new AP through the basic IEEE 802.11 handoff procedures. On the other hand, if there is no AP available in the direct connection range of the MS, the MS uses the procedures discussed in Section 3.3 to search for a potential relay station (RS). If a suitable RS is found, then either BAAHO or HAAHO is performed. When an MS is operating as an RS for an active connection, an arriving voice connection to the RS will generate a forced handoff for the existing voice connection. This simplifies the operation of the RS since a station will never have to handle more than a single active voice connection. If a forced handoff is not possible then the incoming call is blocked.

Once an AAHO has occurred, procedures are required to monitor both links involved in the voice connection. The RS employs usual procedures to monitor the link quality between itself and the AP, i.e., the RS/AP link. This information is relayed from the RS to the MS when voice packets relaying occurs between them. At the same time, the MS takes RSSI measurements to monitor the quality of the RS/MS link. A new handoff will be performed if the worst of the two links is below the HO_Threshold.

Three types of handoff might happen in the process of AAHO:

- AP-to-RS handoff When the direct connection of an MS with the AP is poor and an RS is available, the MS is handed off from a directly connected AP to the RS. The RS is used to forward frames to the AP.
- RS-to-AP handoff When a mobile station which is using an RS as relaying station moves into an AP's original coverage area and the AP has radio resource to facilitate this MS, the MS is then handed off from the RS to the AP with one hop direct connection.
- RS-to-RS handoff If the current relaying link is below the threshold, the MS is handed off to a new RS which is either associated with the same AP as the old RS or associated with a different AP.

3.5 Relay Station Selection Criterion

When an AAHO occurs, there may be more than one potential RS. In this thesis, we use a max/min criterion for making the RS selection. As discussed in Section 3.3, when a potential RS responds to an RS_PROBE, it will include information indicating the channel quality of its current AP. In this thesis, the channel quality is referred to as received signal strength, and is measured in dBm. Similarly channel quality will be measured for the link between the MS and each potential RS when the RS responds to the RS_PROBE. We will refer to these channel quality values for a particular potential $RS(i)$, as $L_{RS-AP}(i)$ and $L_{MS-RS}(i)$, i.e., the quality of the potential RS/AP and MS/RS links. For this discussion we assume that the L values correspond to measured path loss and that n potential RSs have been identified and indexed, i.e., $i \in \{1, ..., n\}$. To obtain the Max/Min RS station selection (MRSS) we define

$$\widehat{L}_i = \max(L_{RS-AP}(i), L_{MS-RS}(i)) \tag{3.1}$$

i.e., $\widehat{L}_i$ is the poorest link quality associated with the use of $RS(i)$. Under the MRSS criterion, the potential RS, $RS(j)$, is selected in such a way that

$$\widehat{L}_j \leq \widehat{L}_i \qquad \text{for all} \quad i \in (1, ..., n) \tag{3.2}$$

This type of relay station selection criterion was used in [36].

An example of MRSS is shown in Figure 3.8. There are five mobile stations available as relay stations named as RS_1 to RS_5. For each potential RS, the values corresponding to the path loss L_{RS-AP}(i) or L_{MS-RS}(i) are marked beside each link. The maximum value of each path can then be determined. Once these are identified, then the smallest of these values is found, and the associated RS is the one that is corresponding to the smallest value. In Figure 3.8, it corresponds to RS_3. The process is also shown in Table 3.1, where

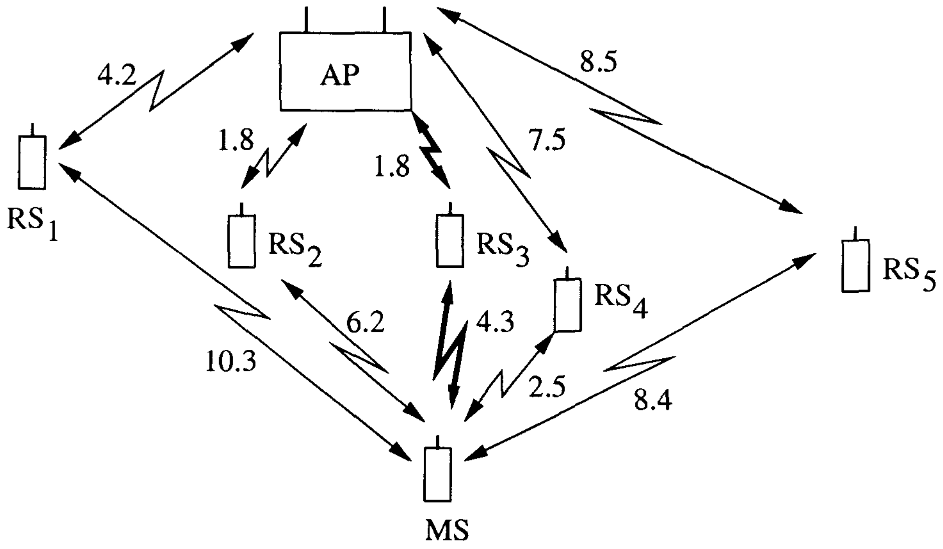

Figure 3.8: Example of Relay Station Selection in MRSS

the maximum value of each path appears in bold letter in the table. By definition, in BAAHO, the selected RS will be associated with the AP that the MS is currently using. In this thesis we assume that in HAAHO the MRSS algorithm makes the final decision as to whether the handoff will be a FAAHO or a BAAHO. Other options are also possible such as setting a preference for BAAHO versus FAAHO.

3.6 Compatible Implementation Options

From an implementation standpoint, AAHO for real-time voice can be accomplished using at least two different approaches. It is important to note that both schemes can permit AAHO in existing IEEE 802.11 installations without making any changes to existing legacy APs. We will briefly discuss how

Table 3.1: Max/Min Relay Station Selection Example

Relay Station	L_{RS-AP}	L_{MS-RS}
1	4.2	**10.3**
2	1.8	**6.2**
3	1.8	**4.3**
4	**7.5**	2.5
5	**8.5**	8.4

each option works. They are referred to as Infrastructure Anchoring (IA) and Transparent MAC Spoofing (TMS).

In Infrastructure Anchoring (IA), AAHO requires a handoff anchor station operating on the wired infrastructure. This is shown in Figure 3.9 as the station marked IA. Essentially the IA acts as an anchor for all voice connections, i.e., all voice connections pass through IA in both inbound and outbound directions. In typical situations, it is expected that the IA would be able to support a large number of APs since wired infrastructure data rates are usually much higher than wireless data rates. Considering the BAAHO case shown in Figure 3.9 , prior to the handoff, MS A receives and routes packets via IA. At the time of the BAAHO, MS A sends a signal to IA, and the IA creates an IP tunnel to MS C. This is shown as Tunnel C in Figure 3.9. An alternative is to create a tunnel from the IA to each potential RS at the time when the station indicates its willingness to become an RS. This avoids the tunnel setup time required just prior to handoff, but may lead to a large number of unused tunnels. Note that the path from A to IA does not need tunneling but requires that MS A adds a station specific route for IA through C to its routing table. When uplink packets arrive at C, they are routed to IA in the usual manner. FAAHO operates in a similar manner, and Tunnel D is shown in the figure being used to support the FAAHO for station D. After the handoff has occurred, voice packets in the downlink direction are tunneled to the RS, e.g., to MS A through MS C and to MS B through MS D. Tunnels have been used in a similar way in some micromobility schemes to insulate routers from the effects of mobility [10].

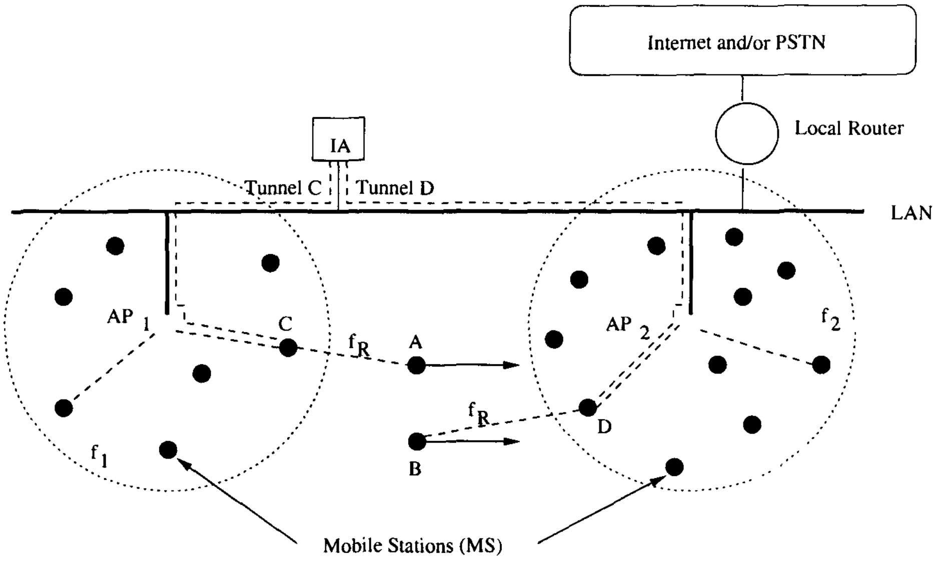

Figure 3.9: Infrastructure Anchor for Ad Hoc Assisted Handoff

The second option uses Transparent MAC Spoofing (TMS). BAAHO and FAAHO both occur by having the RS spoof the identity of the target MS. First consider the BAAHO case shown in Figure 3.9. Once MS A has identified MS C using the mechanism discussed in Section 3.3, MS C then interacts with

AP_1 using MS A's MAC address on frequency f_1. Frames which are forwarded in the downlink direction from AP_1 and transmitted to MS A are intercepted and acknowledged by MS C, using MS A's MAC identity. These packets are then relayed to MS A using MS C's MAC identity on frequency f_R. Similarly, packets which originate at MS A are forwarded to MS C over f_R and are then relayed by MS C using MS A's MAC identity. Note that it is possible to perform these functions in a manner that is transparent to the encryption that is typically used on IEEE 802.11 links (e.g., WEP). However a complex custom chip design is required to implement the functionality needed to do the MAC spoofing.

Chapter 4

Simulation Results and Performance Analysis

This chapter discusses the simulation results and performance analysis of proposed AAHO. First, a simulation model of the AAHO in an IEEE 802.11 infrastructure WLAN is introduced. Then the mobility model, which is used to represent the movement pattern of mobile stations and relay stations, is presented. Following that, simulation environment and parameters used are discussed, and numerical results and discussions are presented at the end.

4.1 Simulation Model

A simulated system is shown in Figure 4.1. M APs are arranged in a rectangular grid coverage area. There are N mobile stations (MSs) randomly distributed in this square area of $X \times Y$ m^2. We assume that both APs and MSs have circular coverage area with the same transmission range. APs are located at the center of each cell and can interact with each other through the wired LAN. MSs are uniformly distributed in the whole network area at the beginning, and move according to a certain mobility pattern discussed in Section 4.2. Operating frequencies assigned to APs are assumed non-overlapping among neighbors. In the simulation, we focus on the coverage extension performance of the system and assume that the MAC layer voice traffic prioritization is provided by the IEEE 802.11e EDCA [5].

The distance between neighboring APs is D meters. Each AP or MS has a circular coverage area of radius R. Please note that the system shown in Figure 4.1 is meant to model a two dimensional layout of the APs, and by manipulating the ratio R/D, we can model various levels of coverage throughout the area in which MSs move around.

4.2 Mobility Model

A mobility model is a useful tool to mimic movements of mobile stations in a wireless communications network. Changes in speed and direction must be taken into consideration in a reasonable manner so that the model can accurately represent the mobility pattern in a given system. In this thesis, we implement one of the most popular mobility models, the random waypoint mobility model [9], in our simulation. Discussion of other mobility models for research of ad hoc networks is referred to [9].

In a random waypoint mobility model, MSs are initially distributed uni-

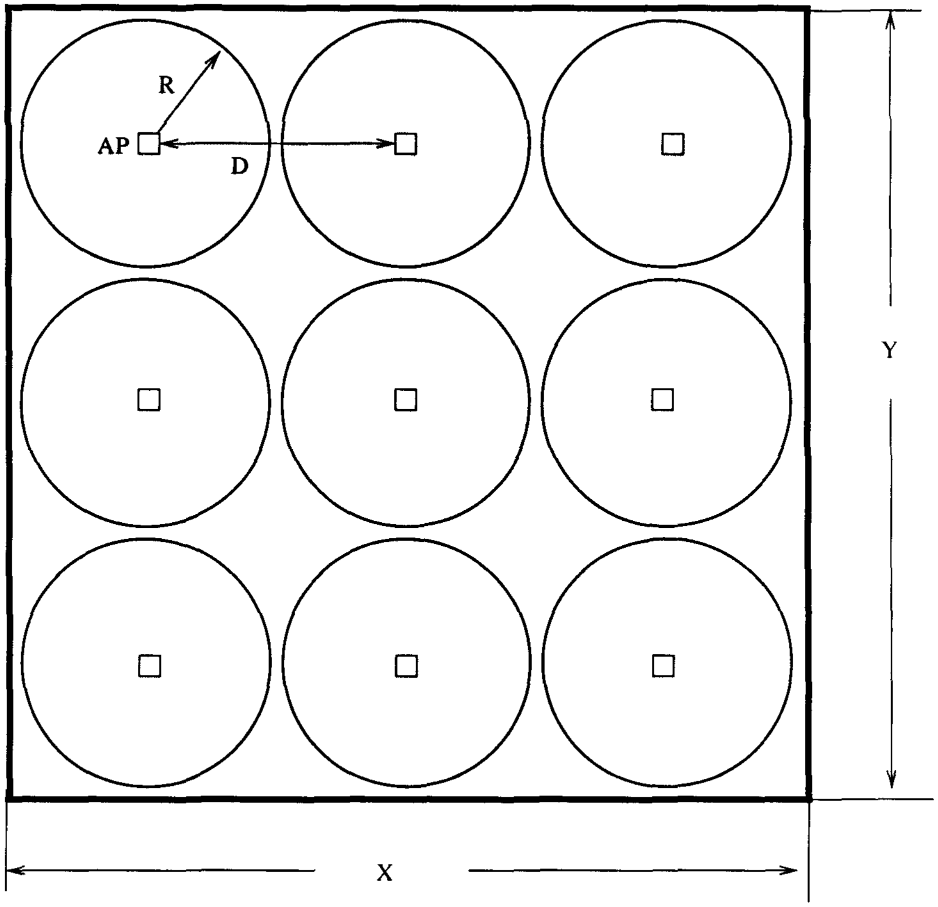

Figure 4.1: Simulation System Configuration

formly in the simulation area. An MS begins by staying in one location for a certain period of time, which is called pause time. Once this pause time expires, the MS chooses a random destination in the simulation area and moves towards the destination at a randomly chosen speed. This speed is uniformly distributed between the preset minimum and preset maximum speeds. When the MS reaches its destination, it remains there for a new randomly chosen pause time, and then moves to a newly selected destination at a new random speed.

The selection of moving speed in the random waypoint mobility model determines the user mobility pattern. For example, slow moving MSs produce a more stable network than fast moving MSs.

4.3 Simulation Environment and Parameters Settings

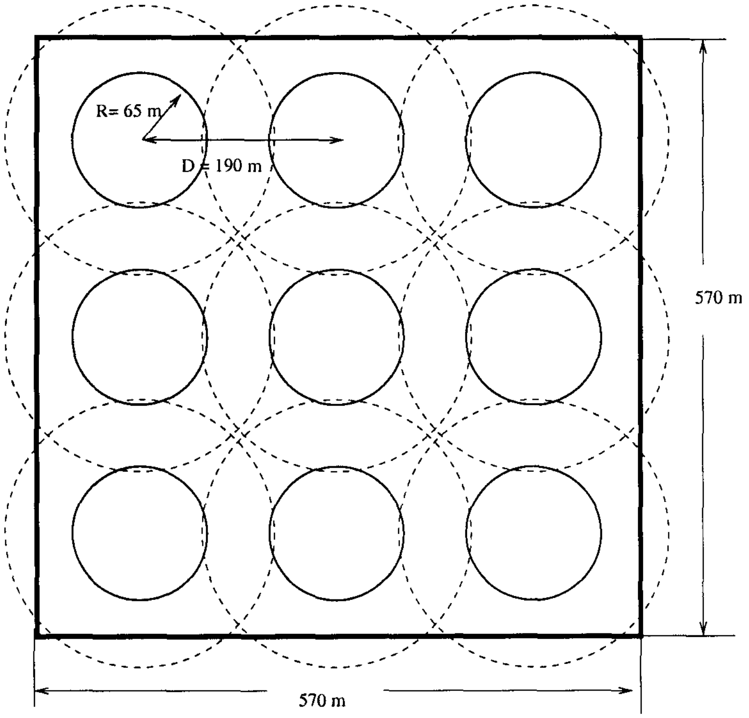

Figure 4.2: Illustration of Extension Coverage Area, $R = 65$ m

Based on the aforementioned simulation model, we executed our simulation

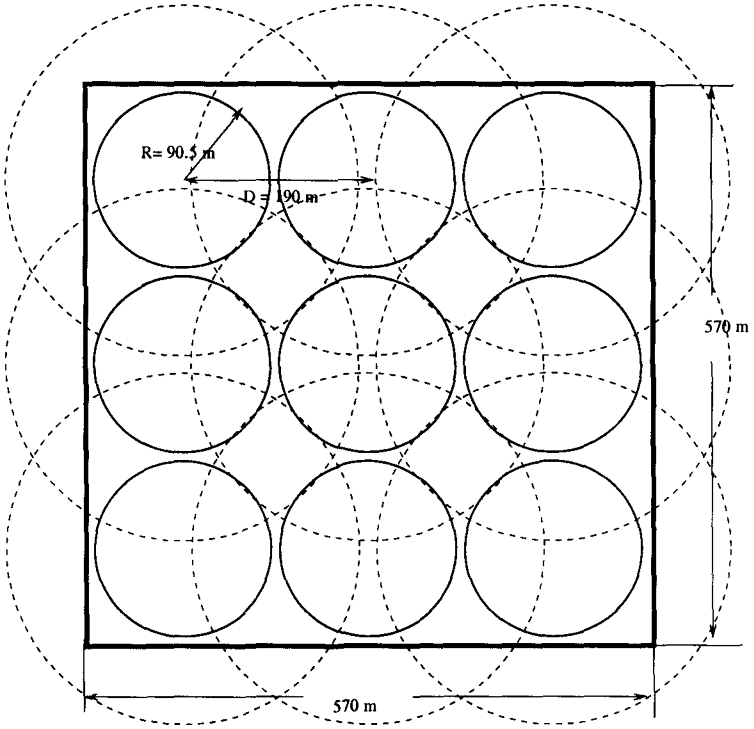

Figure 4.3: Illustration of Extension Coverage Area, R = 90.5 m

in a 570 m × 570 m rectangular area with 9 APs. The distance D between two adjacent APs is 190 m. The transmission radius R of AP and MS is either 65 m or 90.5 m. The overlapping and extended coverage areas for both 65 m and 90.5 m cases are shown in Figure 4.2 and Figure 4.3 respectively, where the AP's original coverage area is marked as solid circles and the extended coverage area is marked as dashed circles. These two situations represent small and large overlapping extended coverage areas respectively. There are a total of 300 MSs distributed in the system. We consider constant bit rate (CBR) as the real-time voice traffic. Each real-time CBR connection is assigned a constant service rate in the simulation, which is similar to the circuit switched mode. Each AP can admit up to 15 voice connections, which is determined by the superframe length that is set equal to the time interval between any two successive voice packets, so that each voice connection can be polled once in every superframe successfully. The MSs move at a speed uniformly distributed between the maximum speed of 2 m/second and the minimum speed of 0 m/second. An exponential path loss propagation model is used throughout the simulation, i.e., $L = d^n$, where L is the average path loss between transmitter and receiver, d is the distance between transmitter and receiver. n is 2 for a distance of less than 500 meters, and 4 for a distance of greater than 500 meters. The threshold to initiate handoff process is set to be 10 dB. Unless otherwise stated, some default simulation parameters used are given in Table 4.1.

In addition to the above assumptions, we ignore the effect of error propagation to simplify the simulation, and thus concentrate our simulation on the performance of interest.

In the simulation, each MS generates a voice call after an exponentially distributed sleep time. Voice call durations are exponentially distributed with an average call holding time of $1/\mu$ seconds. An MS that is carrying a call associates with the AP with the best signal strength based on local RSSI measurements. If the targeted AP has no capacity to serve the call, the call is blocked. The new call blocking rate (NBR) is the ratio of the number of blocked calls to the number of total originated calls for MSs that are within the APs' coverage.

When an MS which is carrying a voice call moves across the boundary of the currently associated AP, it may require a handoff using the proposed AAHO.

Table 4.1: Default Simulation Parameters

Parameter	Description	Value
X, Y	Simulation area	X = 570m, Y = 570 m
D	Distance between two adjacent APs	190 m
R	Coverage radius of APs and MSs	65 m or 90.5 m
M	Number of APs	9
N	Number of MSs	300
C	Max. call admission capacity per AP	15
λ	Average call generation rate	Varies from 0.1 to 5
$1/\mu$	Average call duration	60 seconds
V_{max}	Max. MS moving speed	2 m/second
V_{min}	Min. MS moving speed	0 m/second
T_p	Average pause time	1.5 second
n	Path loss propagation exponent	2 if d $\leq$ 500 m, 4 if d $>$ 500 m
γ	SNR threshold for handoff	10 dB

The handoff may happen from the current serving AP to a new AP in one-hop direct connection, or to the same AP via an RS using BAAHO. During the period of the call, handoff may occur many times either from one RS to another RS, or from the current serving AP to a new AP with better RSSI. Handoff also might happen from two-hop to one-hop when the MS moves back to an AP's original coverage area. In this case, RSs are released so that they are able to start a new call or act as an RS for other calls. A handoff call may be dropped if there is no RS available or the maximum voice capacity at the target AP has been reached. The handoff call dropping rate (HDR) is the ratio of the number of dropped calls to the number of accepted calls. Simulations were run to compare the BAAHO and HAAHO cases. Our purpose is to examine the performance of different AAHO schemes under different system conditions such as call arrival rate, MS velocity, and MS density. Experiments are also conducted to compare the MRSS criterion discussed in Section 3.5 with the scheme called random RS selection (RRSS) which selects an RS randomly among all available RSs. For comparison purpose, we also included the one-hop case without using AAHO in the simulation. The performance metrics of interest in this thesis are handoff call dropping rate and new call blocking rate.

4.4 Numerical Results and Performance of AAHO

In this section, the simulation results based on the system model discussed in the previous sections are presented. The performance of using AAHO and traditional single-hop network in an IEEE 802.11 infrastructure WLAN is discussed.

The discussion of AAHO performance is divided into four sections based on the network performance measurements. Section 4.4.1 contains the results and discussion of performance for different AAHO schemes. Section 4.4.2 discusses the impact of number of MSs on the performance measure of interest. Section 4.4.3 contains results and discussion of performance with variable moving speed in the random waypoint mobility model. Finally, Section 4.4.4 compares the performance of the MRSS and RRSS criteria.

4.4.1 Comparison of AAHO Schemes

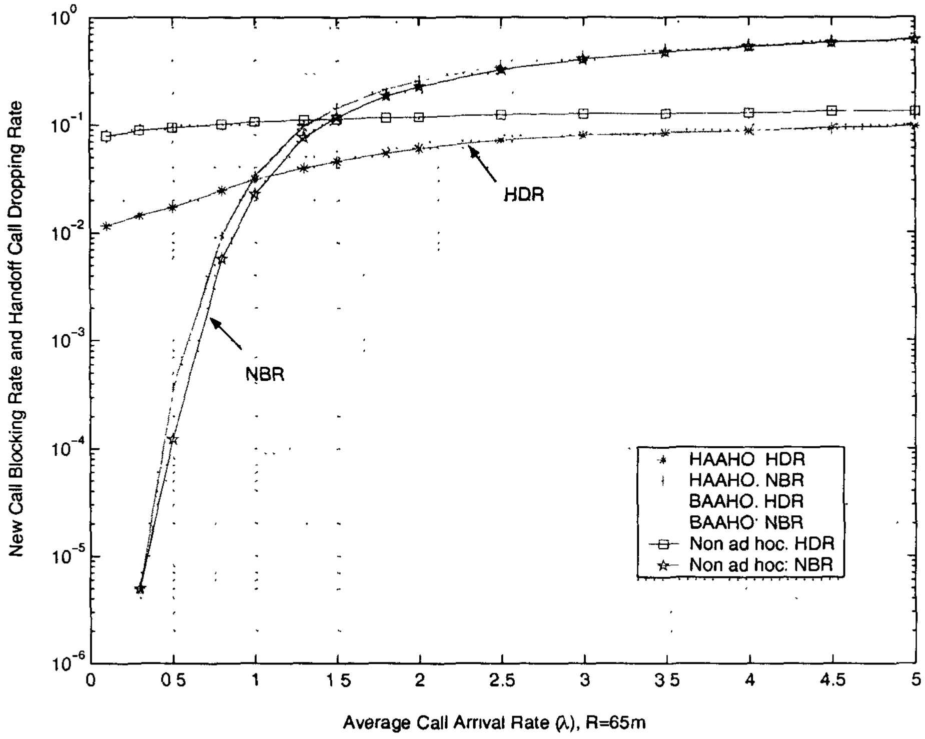

Figure 4.4: New Call Blocking/Handoff Call Dropping Rate, R = 65m

Figure 4.4 and Figure 4.5 show the simulation results of different AAHO schemes for the cases when the coverage radius for AP/MS are 65 meters and 90.5 meters, respectively. As can be seen in Figures 4.4 and 4.5, both BAAHO and HAAHO can reduce the handoff call dropping rate significantly compared with the case without AAHO. The reason that the BAAHO can reduce the handoff call dropping rate is because it extends the AP's coverage radius from

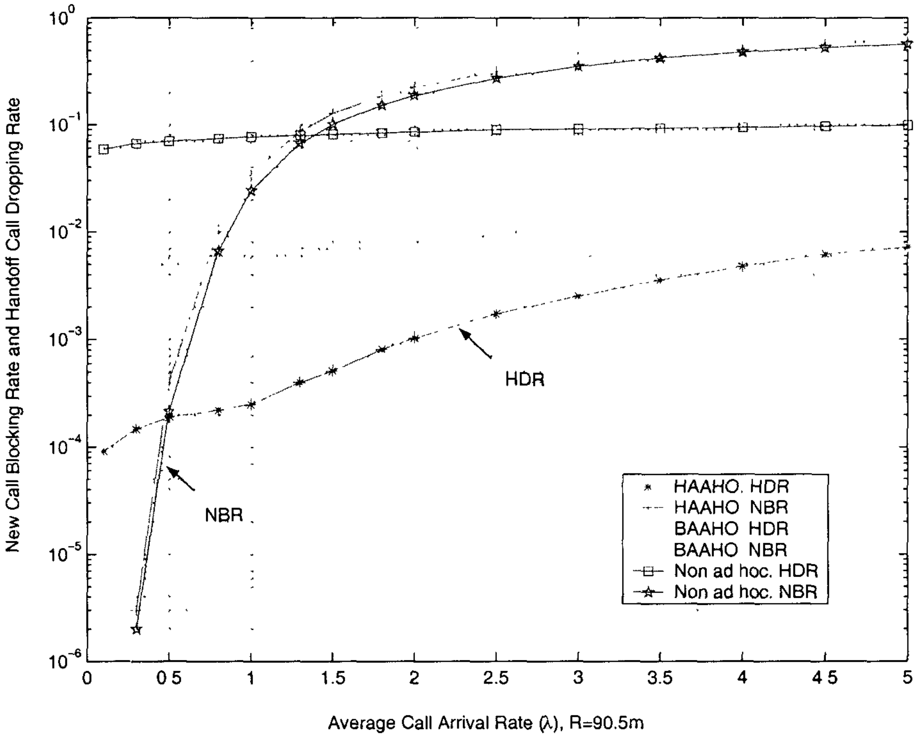

Figure 4.5: New Call Blocking/Handoff Call Dropping Rate, R = 90.5m

R up to $2R$ as long as RSs are available. HAAHO can further reduce the handoff call dropping rate since it offers multiple choices, BAAHO or FAAHO, for an MS to connect to its current serving AP or neighboring APs. The difference between these two figures is that in the 90.5 meters case, the AP has larger original and extended coverage area, and can create a large coverage overlap between two adjacent APs, this overlapping area is where MSs can potentially perform FAAHO. As can be seen in Figures 4.2 and 4.3, the overlapping area for performing FAAHO in the 65 m case is much smaller than the overlapping area in the 90.5 m case. Therefore, the advantage of using HAAHO over BAAHO in the 65 m case is not very much significant. Figures 4.4 and 4.5 also show that the new call blocking rate is almost not affected by the AAHO schemes used in the simulation, because in the experiments discussed above, there is no capacity reserved at APs for handoff use only.

4.4.2 Impact of the Number of Mobile Stations

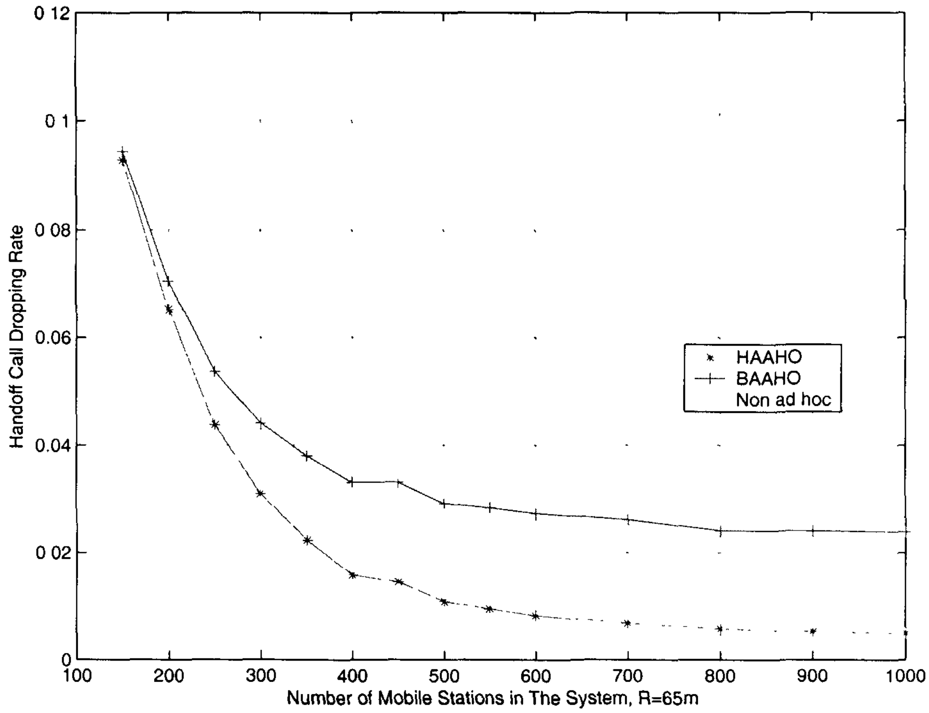

Figure 4.6: Performance Impact of MS Quantity, R = 65m

Figure 4.6 and Figure 4.7 illustrate the performance of handoff call dropping rate versus number of MSs in the system. Figure 4.6 represents the results of the case where R = 65 m, and Figure 4.7 is for the case where R = 90.5 m.

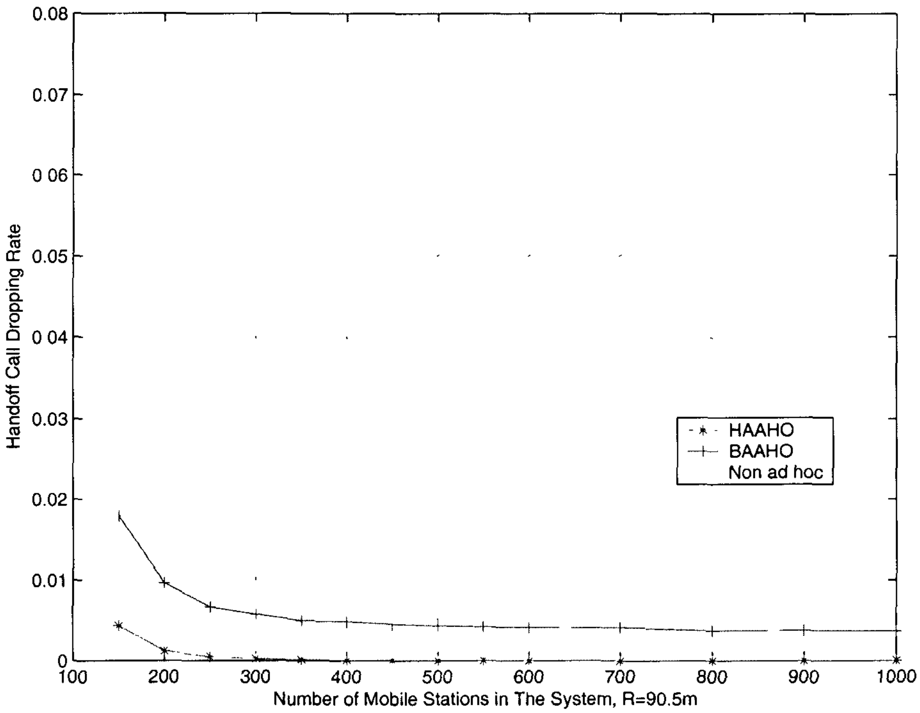

Figure 4.7: Performance Impact of MS Quantity, R = 90.5m

For the same reason mentioned in the previous section, in both cases, HAAHO performs better than BAAHO in this experiment. As can be seen, handoff call dropping rates decrease with the increased MS quantity. This is due to the fact that a great density of MS's provides more opportunities for an active MS to find an RS to forward packets for it. This is more sensitive when the MS density is relatively low. However, when the number of MSs approaches a certain higher level, MS quantity will only contribute a small amount to the overall performance improvement. Comparing Figure 4.6 and Figure 4.7, we can also see that the R = 90.5 m case results in a lower handoff call dropping rate than that of the R = 65 m case. This is due to the fact that when an AP has a larger coverage range, it will include more MSs in its coverage area, and thus provide more opportunity to find MSs which can act as RSs.

4.4.3 Impact of Mobile Station Moving Speed

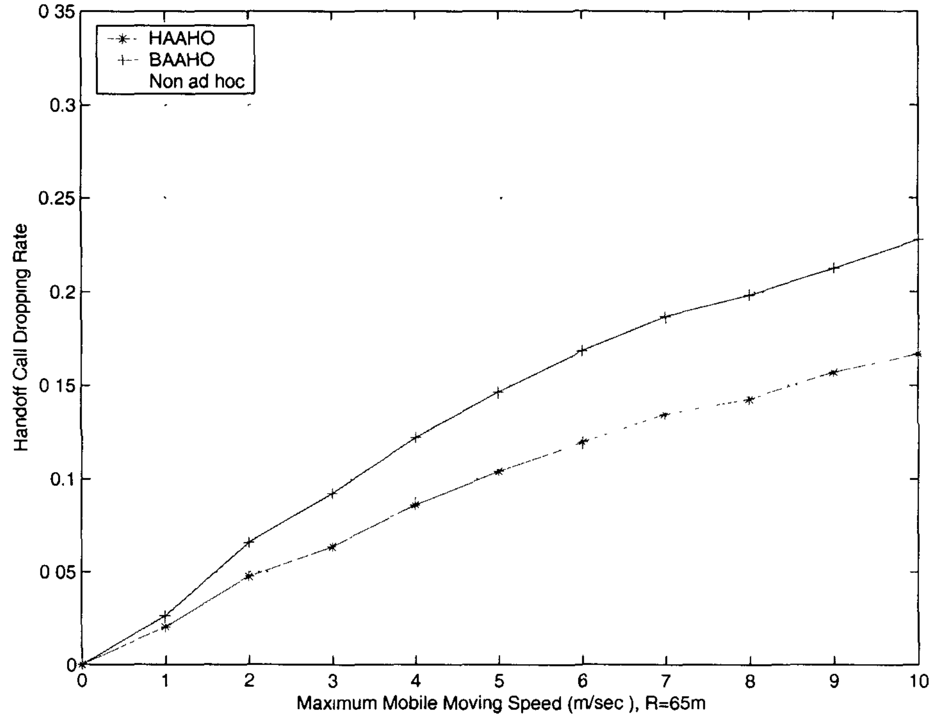

Figure 4.8: Handoff Call Dropping Rate versus Mobility, R = 65m

Figures 4.8 and 4.9 show that the handoff call dropping rate increases when an MS's velocity increases. Using AAHO can improve handoff call dropping rate significantly compared with the no AAHO situation because the extension of coverage area provides more flexibility to MS movement. When the mobility is low, however, HAAHO provides less advantage over BAAHO since calls tend

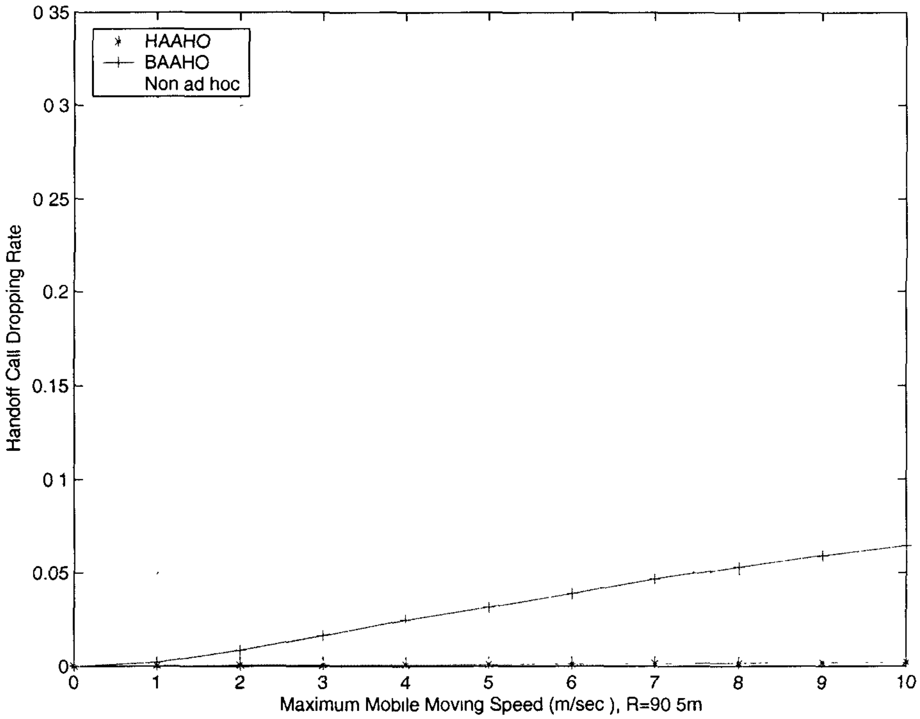

Figure 4.9: Handoff Call Dropping Rate versus Mobility, R = 90.5m

to terminate before stations move out of their AP/RS coverage area. When comparing the performance impact of mobility in the 65 m and 90.5 m cases, it can be seen that the effect of performing AAHO on improving handoff call dropping rate in the 65 m case is less significant than that of in the 90.5 m case. This is due to the smaller overlapping area available for performing FAAHO in the 65 m case. In the 90.5 m case, however, performing HAAHO makes the system much less sensitive to MS velocity because of the larger original and extended coverage area.

4.4.4 Impact of Relay Station Selection Criteria

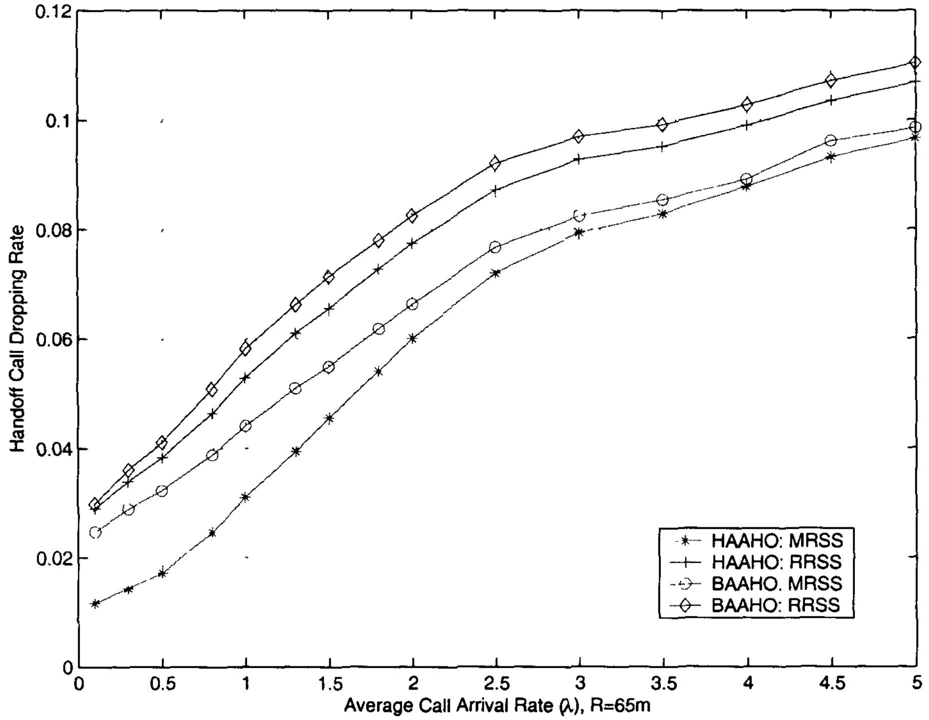

Figure 4.10: Comparison of MRSS and RRSS, R = 65m

In this section, we compare system performance in conducting two relay station selection criteria, max/min relay station selection (MRSS) criterion and random relay station selection (RRSS) criterion. Figures 4.10 and 4.11 clearly indicate that the proposed MRSS link selection criterion performs better than the RRSS criterion in both BAAHO and HAAHO cases. This is because in a system where all MSs move randomly, using the MRSS link selection criterion can establish a more stable link with higher probability.

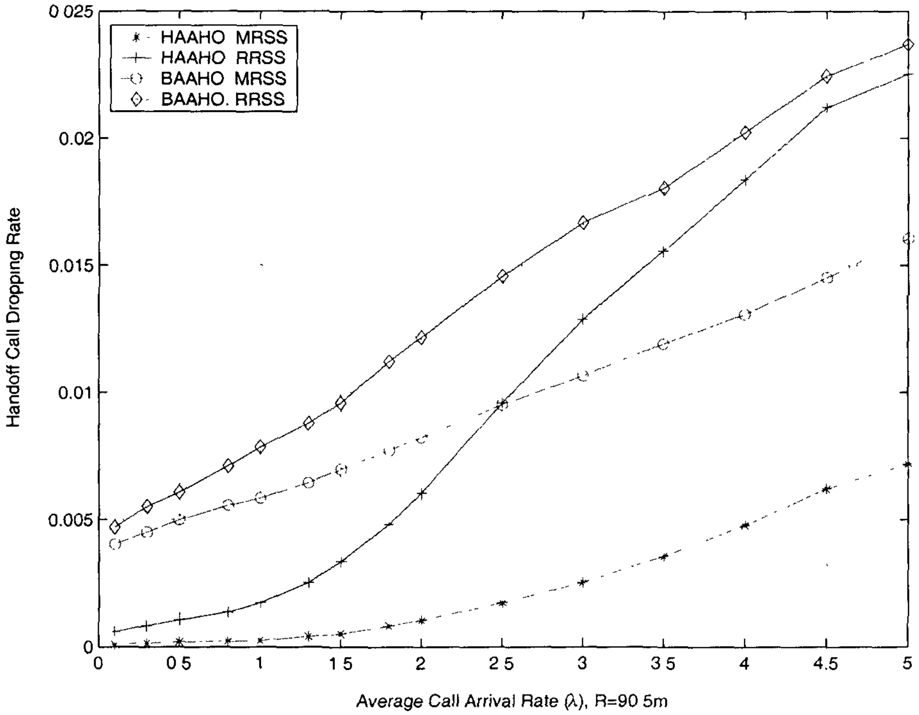

Figure 4.11: Comparison of MRSS and RRSS, R = 90.5m

Chapter 5

Conclusions and Future Work

In this thesis, we propose and investigate the use of Ad Hoc Assisted Handoff (AAHO) in an infrastructure IEEE 802.11 WLAN, where an additional ad hoc hop may be used by an MS to extend the coverage range or to improve channel quality required to maintain its desired real-time performance. The purpose of using AAHO is to overcome quality of service degradation due to incomplete AP coverage and station mobility, and to maintain cost effective and reliable propagation paths.

Three different AAHO schemes are presented and discussed in detail. The BAAHO is the case that an MS is relayed to the same AP the MS is currently associated with. BAAHO involves less infrastructure cooperation because it does not change the AP during the handoff. On the other hand, FAAHO requires more infrastructure cooperation since the MS is relayed to a different AP from the one that the MS is currently associated with. HAAHO can perform either BAAHO or FAAHO depending on which scheme are available and can provide better link quality. In order to facilitate operations of the proposed multihop relaying, 802.11 MAC protocol is extended in finding the relay stations. MSs which are not carrying traffic offer themselves as relay stations. A relay station acts as a polling master to poll for packets from both MS and AP. Link maintenance and handoff procedures are discussed. Relay station selection criterion is provided with an example. The constraint behind the proposed AAHO is that it is backward compatible with conventional 802.11 standards, and can be transparently implemented on existing 802.11 networks. Two compatible implementation options for performing AAHO in IEEE 802.11 infrastructure WLANs are presented. Simulation results show that the AAHO can greatly improve the performance of real-time applications in many realistic situations compared with the situation without using AAHO. The effect of the performance improvement depends on factors such as coverage, MS density, MS mobility, and relay station selection criteria. From performance perspective, the HAAHO always performs the best among three AAHO schemes because it takes advantages of both BAAHO and FAAHO.

In this thesis, we focus our discussions on the performance of handoff call dropping rates. However, some other measures are also important to evaluate the system performance in supporting real-time voice traffic. For example, real-time applications are sensitive to transmission delay and delay jitter. Delay performance of AAHO in supporting different types of real-time applications such as voice, video, and multimedia has to be investigated in detail. In the future, evaluating impacts of AAHO on the performance of throughput and power consumption are also our research directions.

Bibliography

[1] *IEEE Standards Department, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHZ Band, IEEE Std. 802.11a-1999.* IEEE Press, 1999.

[2] *IEEE Standards Department, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-speed Physical Layer Extension in the 2.4 GHz Band, IEEE Std. 802.11b-1999.* IEEE Press, 1999.

[3] *IEEE Standards Department, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE Std 802.11, 1999 Edition.* IEEE Press, 1999.

[4] *IEEE Standards Department, Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution System Supporting IEEE 802.11 Operation, IEEE 802.11f/D5.0,* . IEEE Press, January 2003.

[5] *IEEE Standards Department, Draft Supplement to Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications:*

Medium Access Control (MAC) Enhancements for Quality of Service (QoS), IEEE 802 .11e/D5.0. IEEE Press, July 2003.

[6] T. Adachi and M. Nakagawa, "Capacity analysis for a hybrid indoor mobile communication system using cellular and ad-hoc modes," in *Proc. of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications,PIMRC 2000*, September 2000.

[7] G. N. Aggelou and R. Tafazolli, "On the relaying capability of next-generation GSM cellular networks," *IEEE Trans. on Personal Communications*, vol. 8, no. 1, pp. 40–47, February 2001.

[8] R. Ananthapadmanabha, B. Manoj, and C. Murthy, "Multi-hop cellular networks: the architecture and routing protocols," in *Proc. of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications,PIMRC 2001*, October 2001.

[9] T. Camp, J. Boleng, and V. Davies, "Survey of Mobility Models for Ad Hoc Network Research," in *Wireless Communication and Mobile Computing (WCMC 2002): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, vol. 2, pp. 483–502, May 2002.

[10] A. Campbell, J. Gomez, S. Kim, C.-Y. Wan, Z. Turanyi, and A. Valko, "Comparison of IP micromobility protocols," *IEEE Trans. on Wireless Communications*, vol. 9, no. 1, pp. 72–82, February 2002.

[11] R.-S. Chang, W.-Y. Chen, and Y.-F. Wen, "Hybrid wireless network protocols," *IEEE Trans. on Vehicular Technology*, vol. 52, no. 4, pp. 1099–1109, July 2003.

[12] B. P. Crow, J. G. Kim, and P. T. Sakai, "IEEE 802.11 Wireless Local Area Networks," *IEEE Communications Magazine*, vol. 35, no. 9, pp. 116–126, September 1997.

[13] F. Eshghi and A. K. Elhakeem, "Performance Analysis of Ad Hoc Wireless LANs for Real-time Traffic," *IEEE Journals on Selected Areas in Communications*, vol. 21, no. 2, pp. 204–215, February 2003.

[14] F. H. P. Fitzek, D. Angelini, G. Mazzini, and M. Zorzi, "Design and Performance of an Enhanced IEEE 802.11 MAC Protocol for Multihop Coverage Extension ," *IEEE Wireless Communications*, vol. 10, no. 6, pp. 30–39, December 2003.

[15] M. S. Gast, *802.11 Wireless Networks: The Definitive Guide.* O'Reilly, 2002.

[16] M. He, T. D. Todd, D. Zhao, and V. Kezys, "Ad Hoc Assisted Handoff for Real-time Voice in IEEE 802.11 Infrastructure WLANs," in *IEEE Wireless Communications and Networking Conference ,WCNC 2004*, vol. 1, pp. 201–206, March 2004.

[17] M. F. Ho, M. S. Rawles, M. Vrijkorte, and L. Fei, "RF Challenges for 2.4 and 5 GHz WLAN Deployment and Design," in *IEEE Wireless Communications and Networking Conference, WCNC 2002*, vol. 2, pp. 783–788, March 2002.

[18] M.-J. Ho, M. S. Rawles, M. Vrijkorte, and L. Fei, "RF Challenges for 2.4 and 5 GHz WLAN Deployment and Design," in *Wireless Communications and Networking Conference, 2002. WCNC2002*, March 2002.

[19] A. Kösel and A. Wolisz, "Voice Transmission in an IEEE 802.11 WLAN based access network," in *Proceedings of the 4th ACM international workshop on Wireless mobile multimedia, Rome, Italy, 2001*, pp. 23–32, 2001.

[20] Y. Lee, K. Kim, and Y. Choi, "Optimizing of AP Placement and Channel Assignment in Wireless LANs," in *Proceedings of IEEE Conference on Local Computer Networks, LCN 2002*, November 2002.

[21] C. Li, J. Li, and X. Cai, "Performance analysis of IEEE 802.11 WLAN to Support Voice Services," in *IEEE 18th International Conference on Advanced Information Networking and Applications, 2004. AINA 2004*, vol. 2, pp. 343–346, March 2004.

[22] Q. Li and M. van der Schaar, "Providing Adaptive QoS to Layered Video Over Local Area Networks Through Real-time Retry Limit Adaptation," *IEEE Trans. on Multimedia*, vol. 6, no. 2, pp. 278–290, April 2004.

[23] Y.-D. Lin and Y.-C. Hsu, "Multihop cellular: a new architecture for wireless communications," in *Proc. of IEEE Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. INFOCOM 2000*, March 2000.

[24] H. H. Liu and J. C. Wu, "Packet Telephony Support for the IEEE 802.11 Wireless LAN," *IEEE Journals on Selected Areas in Communications*, vol. 22, no. 4, pp. 643–652, May 2004.

[25] S. Mangold, S. Choi, G. R. Hiertz, O. Klein, and B. Walke, "Analysis of IEEE 802.11e for QoS Support in Wireless LANs," *IEEE Wireless Communications*, vol. 10, no. 6, pp. 40–50, December 2003.

[26] P. Marichamy, S. Chakrabarti, and S. Maskara, "Overview of handoff schemes in cellular mobile networks and their comparative performance evaluation," in *IEEE VTS 50th Vehicular Technology Conference, 1999. VTC 1999 - Fall.*, vol. 3, pp. 1486–1490, September 1999.

[27] A. Pal, A. Dogan, and F. Ozguner, "MAC Layer Protocols for Real-time Traffic in Ad-hoc Wireless Networks," in *IEEE Proceedings of the International Conference on Parallel Processing, ICPP'02*, August 2002.

[28] M. Portoles, Z. Zhong, S. Choi, and C.-T. Chou, "IEEE 802.11 link-layer forwarding for smooth handoff," in *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003*, vol. 2, pp. 1420–1424, September 2003.

[29] N. R. Prasad, "IEEE 802.11 System Design," in *IEEE International Conference on Personal Wireless Communications*, December 2000.

[30] C. Qiao and H. Wu, "iCAR: an integrated cellular and ad-hoc relay system," in *Proc. of IEEE Ninth International Conference on Computer Communications and Networks, 2000*, October 2000.

[31] R. Ramanathan and J. Redi, "A Brief Overview of Ad Hoc Networks: Challenges and Directions," *IEEE Communications Magazine*, vol. 40, no. 5, pp. 20–22, May 2002.

[32] T. Rouse, I. Band, and S. McLaughlin, "Capacity and power investigation of opportunity driven multiple access (ODMA) networks in TDD-CDMA based systems," in *Proc. of IEEE International Conference on Communications, ICC 2002*, May 2002.

[33] S. Sharma, N. Zhu, and T. Chiuch, "Low-Latency Mobile IP Handoff for Infrastructure-Mode Wireless LANs," *IEEE Communications Letters*, vol. 4, no. 9, pp. 286–288, September 2000.

[34] M. Siebert, E. Bolinth, O. Stauffer, and R. Kern, "Coverage Investigations for Adaptive Modulation in 5GHz WLANs," in *The 57th IEEE Semiannual Vehicular Technology Conference, 2003. VTC-2003-Spring.*, vol. 2, pp. 925–929, April 2003.

[35] V. Sreng, H. Yanikomeroglu, and D. Falconer, "Coverage enhancement through two-hop relaying in cellular radio systems," in *2002 IEEE Wireless Communications and Networking Conference, 2002. WCNC2002*, vol. 2, pp. 881–885, March 2002.

[36] V. Sreng, H. Yanikomeroglu, and D. Falconer, "Relayer Selection Strategies in Cellular Networks with Peer-to-peer Relaying," in *IEEE Vehicular Technology Conference, VTC 2003*, October 2003.

[37] M. Veeraraghavan, N. Cocker, and T. Moors, "Support of Voice Services in IEEE 802.11 Wireless LANs," in *IEEE Proceedings of IFCOM 2001*, April 2001.

[38] J. D. Vriendt, P. Laine, C. Lerouge, and X. Xu, "Mobile Network Evolution: A Revolution on the Move," *IEEE Communications Magazine*, vol. 40, no. 4, pp. 104–111, April 2002.

[39] K. K. Wong and T. O'Farrell, "Coverage of 802.11g WLANs in the Presence of Bluetooth Interference," in *14th IEEE Proceedings on Personal*

Indoor and Mobile Radio Communications, 2003. PIMRC 2003, vol. 3, pp. 2027–2031, September 2003.

[40] X. Wu, S.-H. Chan, and B. Mukherjee, "MADF: a novel approach to add an ad-hoc overlay on a fixed cellular infrastructure," in *Proc. of IEEE Wireless Communications and Networking Conference, WCNC. 2000*, September 2000.

[41] J. H. Yap, X. Yang, S. Ghaheri-Niri, and R. Tafazolli, "Position assisted relaying and handover in hybrid ad hoc WCDMA cellular system," in *Proc. of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications,PIMRC 2002*, September 2002.

[42] H. Zhu and G. Cao, "On Improving the Performance of IEEE 802.11 with Multi-hop Concepts," in *IEEE Proceedings of International Conference on Computer Communications and Networks, ICCCN 2003*, October 2003.