A Study on Multi-Radio Wireless LAN Systems for Mobility and Positioning

By

Thavisak Manodham

The University of Electro-Communications

Tokyo, Japan.

December 2007

A Study on Multi-Radio Wireless LAN Systems for Mobility and Positioning

Approved by Supervisory Committee

Chairperson:	Prof. Tetsuya MIKI
Member:	Prof. Yoshio KARASAWA
Member:	Prof. Yasushi YAMAO
Member:	Prof. Nobuo NAKAJIMA
Member:	Associate Prof. Naoto KISHI
Member:	Associate Professor Takeo FUJII

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.
I understand that my thesis may be made electronically available to the public.

移動通信と位置検出のための複数無線機ワイヤレスLANシステムに関する研究

タビサック　マノタム

論文の和文概要

この論文は、学位申請者が新たに提案した複数無線機をアクセスポイントに備えるワイヤレスLANに関する研究成果をまとめたものである。

近年、IEEE 802.11 標準に基づいたワイヤレス LAN（WLAN）が広く普及し、インターネットをベースにした様々なサービスを提供出来る WLAN システムの需要が急増している。このような状況から、高い伝送速度のみならず、移動しながらのリアルタイムアプリケーションの利用を可能とするシステムの実現が望まれている。しかし、リアルタイム通信を行うには、隣接するアクセスポイント間でのシームレスなハンドオーバとトラヒック負荷分散が重要になってくる。この論文では、まずハンドオーバ切替時間とトラヒック負荷に関する検討を行った。次に、WLAN によるリアルタイム通信を利用しながら同時に高い精度での位置検知を実現できるシステムを検討した。

第１章は前書きであり、WLAN によるアルタイム通信の背景と動機を述べている。

第２章では、現行の WLAN システムの問題点を示し、WLAN の関連技術を概説している。また、リアルタイム通信を行うために必要なハンドオーバのアーキテクチャーとそれらの性能に関する現行の WLAN 技術の問題点を示す。さらに、屋内・屋外での位置検知システムとそれらの精度と、既存の位置検知システムを紹介している。

第３章では、まず現行の WLAN の移動端末に対する資源割当管理に関する詳細な解析を行い、ハンドオーバ時のレイヤ 2 ならびにレイヤ 3 での瞬断が生じること、アクセスポイントの状況を無視した制御しか出来ないこと、などの問題点を指摘している。その上で本研究の基本となるアクセスポイントに複数無線機を配置しアクセスポイントで受信した近隣エリアの端末状況を把握し、それを相互に活用する WLAN 方式を提案している。この方式によれば、通信中とは別の制御系が構成できるため、合理的リアルタイム通信のシームレス接続が実現できる。

複数無線機 WLAN による提案するハンドオーバは、アクセスポイントでの受信電界強度とトラヒック負荷条件を考慮している。ファジー演算に基づいた受信電界強度とトラヒック負荷に関する重み付けしたメトリックがハンドオーバプロセスを開始する実用的な判断基準となることを示している。この提案の効果をシミュレーションにより従来の WLAN による方式と比較して、その効果を示している。

第４章では、リアルタイムサービス中にも行える位置検知システムのための手法を検討している。近年、移動端末の位置を検出可能な位置情報サービスが急速に普及しており、緊急救助をはじめ様々なアプリケーションとして広く利用されている。これらのシステムにおいて、インターネットを切断することなく位置検出を行えるようなシステムは、WLAN によるサービスの有効性を高める。これらを踏まえ、複数無線機 WLAN 方式がこれに有効に対応できるシス

テムであることを示している。複数無線機 WLAN により、リアルタイム通信を行いつつ正確な位置トラッキングが可能な位置検出システムを実現する構成案について検討し、位置検知には端末からアクセスポイントへの到着時間の差分を利用する手法を用い、これらの到着時間の差分をデータベース化し、アクセスポイント間の相対的な相関情報を利用する方式が適していることを導いている。さらに、この方式をシミュレーションによって従来方式と比較し、提案方式の有効性を明らかにしている。

第５章は、本論文の結論であり、得られた成果をまとめると共に WLAN の将来性について述べている

ABSTRACT

Recently, wireless LANs based on the IEEE 802.11 standard have become popular and widely used. New technologies improve WLAN system to provide various kinds of service, including Internet services, Voice-over-IP (VoIP), e-learning, video conference, and even location-based services (LBS). New technologies can provide high data rates and high stabilization for wireless LAN support of different types of real-time applications. However, seamless handoff and traffic load balancing among neighbor APs are other important issues to be addressed, so that people can receive real-time services across wireless LANs without any interruption. The positioning system based on the wireless LAN infrastructure has led to growing interest in finding location in-building (indoor) areas. However, these current technologies interrupt the Internet connection every time that they are activated.

This dissertation addresses the issues of handoff latency and traffic load, and focuses on how to improve the performance of the wireless LANs handoff scheme in terms of reducing the latency time to support seamless handoff and balancing the traffic load among neighbor APs. Moreover, it aims to improve wireless LANs to support wireless positioning systems with higher accuracy and uninterrupted Internet connection for real-time services.

First, a novel wireless network architecture is introduced to improve network efficiency in terms of supporting seamless handoff and balancing the traffic load in wireless networks. In the proposed scheme, the multi-radio access point (AP) with two transceivers is used to scan and find neighboring mobile stations (STAs) in the transmission range and then send the results to its associate AP, which compares and analyzes whether the STA should perform a handoff. The initial results from the simulations show that the proposed scheme is more effective than the conventional and related works in terms of providing a handoff process with low latency and support for traffic load sharing with neighbor APs.

Second, a novel wireless positioning system (WPS) based on the wireless LAN infrastructure is presented to improve the performance of WPS in terms of accuracy of the location estimation and to avoid service connectivity interruption. Based on the proposal the AP finds information from neighboring STAs in the transmission range and then sends information in advance to associated APs, which estimate the location of the STA based on an internal database. A time difference of arrival (TDOA) technique is used to estimate the location of the STA when there is not enough information in the database (in this case, the STA moves to a new area where the system has not run the calibration phase). Using TDOA, the database can be generated and updated automatically. The initial results from the simulations show that the proposed system provides high location accuracy and does not interrupt the Internet connection for end users, in contrast with other proposed schemes.

PREFACE AND ACKNOWLEDGEMENTS

My work concerning wireless network architectures and protocols for such networks initiated in my master thesis work for the Graduate School of Information Systems, the University of Electro-Communications, which was completed in March 2004 and supervised by Professor Tetsuya Miki. Recently, I registered as a doctoral candidate at the Department of Electronic Engineering (EE), the University of Electro-Communications, and began work toward a Ph.D. thesis. The entire study was conducted at the University of Electro-Communications with support in various ways from all members of the MIKI laboratory.

First, I would like to express my gratitude to my wonderful wife, Viengvilay, and to my lovely family—my parents, my brother, and my sisters—for their endless patience and support. I would also like to express my gratitude and very special thanks to my supervisor, Professor Tetsuya Miki, for giving me the opportunity to continue on to the doctoral course and especially for encouraging my work.

I would like to thank professors Yoshio Karasawa, Yasushi Yamao, Nobuo Nakajima, Naoto Kishi, and Takeo Fujii for being part of my judging committee. Special thanks go to Professor Yoshio Karasawa and Yasushi Yamao, whom I received many good technical advices and encouragement from during

these years. Likewise, I would like to express my thankfulness to Associate Professor Minoru Terada and Assistant Professor Motoharu Matsuura for technical guidance at crucial moments of my research.

I would like to express my special thanks to Dr. Luis Loyola, Mitsuo Hayasaka, and Gustavo Atoche for supports, comments, and discussions.

Last, I want to encourage those curious people who are thinking about pursuing a Ph.D. It is a lot of works, but the experiences are well worth it.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

Introduction

This dissertation reflects a paradigm shift toward new generations of wireless local area networks (WLANs), where seamless mobility across wireless LAN and uninterrupted wireless positioning system are possible. These new generations are referred to as the next generation network (NGN). Seamless mobility among wireless access networks and uninterrupted wireless positioning systems need further research and development beyond the current generation wireless networks.

Generally, customers do not need to know what wireless technology, base station, access point, or router they are using at any given moment—they only need to experience seamless and effective service based on their location. Telecommunication engineers and researchers can be thought of as secret agents: they design the systems and only reveal technical details on a need-to-know basis. Transfers from one technology to another should be easy and transparent.

This dissertation contributes to the evolution of wireless networking technology by providing an understanding of mobility and wireless positioning

systems as technical problems and by helping to make these systems transparent for the average user. This paper presents the main contributions of the author's research studies during the past 3 years, along with an overview of the field.

This first chapter discusses the research questions and provides the problem statement and motivation. The scope and the methodology are described, and an overview of the contributions is given. Finally, the outline of the dissertation is introduced.

1.1 Background and Motivation

The wireless local area network (WLAN) deserves research attention from many perspectives. This dissertation focuses on finding a solution to the service performance problem. First, it seeks to improve the current WLAN for seamless mobility support of real-time services and traffic load balancing among neighboring access points (AP) in order to provide quality of service (QoS) to every end user. Second, it determines what kind of added value and changes to the WLAN-based positioning system architecture bring benefits when considered from the viewpoint of uninterrupted Internet connectivity and high location accuracy.

Currently WLANs can provide high-speed Internet connectivity up to 11Mbps (IEEE 802.11b) or 54Mbps (IEEE 802.11a/g), which can support real-time services. However, recent works [1] address the problem of a mobile station (STA) that moves from one WLAN access point to another while remaining connected to the Internet. In this case, the delay time involved in the handoff process when a STA switches from its current AP to an adjacent AP becomes an important issue for supporting seamless connectivity to a mobile station in IEEE 802.11-compliant wireless networks, especially for real-time

applications such as voice-over-IP (VoIP), e-conference, and e-learning services. In order to support real-time applications with continuous mobility, there must be a small total latency period provided at layer 2 and layer 3 during a handoff. Elaboration of this problem requires analyzing the system architecture and related communication procedures to develop a framework for handoff analysis that considers both moving-in and moving-out scenarios. The objective is to find a method that will give better performance than a traditional handoff algorithm, which is based on the received signal strength threshold. This type of holistic approach requires experimenting and prototyping with both advanced handoff algorithms and mobility management solutions.

The motivation for addressing the given problem areas is to develop a novel wireless network architecture for handoff and mobility management in wireless networks. The handoff scheme in the proposed system takes into consideration the received signal strength (RSS) and the traffic load condition of the APs. A weighted combination of received signal strength and traffic load based on generic fuzzy logic is used to compare the capabilities of current and neighbor APs. This technique gives us a practical way to compare two APs and decide whether to start handoff process. The entire problem involves designing systems that can effectively manage the system capacity for various applications and mobility scenarios for a growing user population.

A relatively recent branch of mobile networking, location-based services (LBS) have expanded rapidly since mobile networks were enabled to determine the locations of mobile devices. LBS provide navigation, service information, targeted advertising, notification, and other services for which the awareness of user location is critical [2] [3]. Some critical applications and services based on indoor localization—such as emergency rescue, fire brigade, or incident

management—require an easily deployable location system that provides high positioning accuracy (i.e., about 1m of error [4]) in medium and deep indoor environments. Since outdoor location systems, for example, global positioning systems (GPS) and location systems based on cellular phone networks, remain inefficient indoors, wireless position systems based on the WLAN infrastructure are focused. However, obtaining the location of a user without interrupting his or her Internet connection is another key issue in this system related to the level of user satisfaction. Thus, it would be desirable, for example, if a user could have a VoIP conversation with a friend while running an LBS application that guides him or her to a gathering place.

The research challenge is the design and implementation of an indoor location system capable of providing accurate tracking and continuous Internet connection using the existing WLAN infrastructure (i.e., taking advantage of the wide deployment of IEEE 802.11b networks). The main motivation for this approach is twofold: to improve the accuracy of location estimation and to avoid Internet connectivity interruption for end users. Two location estimation techniques, fingerprinting and time difference of arrival (TDOA), are integrated to introduce a novel wireless positioning system. This system using a multi-radio access point module to scan neighboring STAs in the coverage area, then report information in advance to its associated AP, which analyzes and searches a database to estimate the location of the STA. TDOA technique is used to estimate the location of the STA when there is not enough information in the database, as is the case when the STA moves into a new area where the system has not yet run the calibration phase. After the position of the STA has been estimated using the TDOA technique, all correlations between coordinate values of this position will be recorded in the database.

In this dissertation, the proposed system is simulated and compared to the traditional work and relative works. The numerous simulations have been performed to show how parameters such as the number of access points, the number of mobile stations, or even the moving direction can affect the results of wireless LAN mobility and positioning.

1.2 Scope and Methodology

This research discusses performance issues in WLANs and presents a seamless handoff scheme with access point load balance. It identifies the theoretical aspects of this concept and builds a framework for analysis and future works. The characteristics of delay and throughput in handoff process between two APs are analyzed with simulations. Transition analysis provides information about the key parameters affecting algorithm performance, measured as the mean throughput perceived by a single user. Mobility management with a fuzzy logic algorithm is evaluated and compared with a hysteresis based algorithm.

Moreover, it discusses performance issues in the current wireless positioning system, present the concepts of a new wireless positioning system that does not interrupt the Internet connection of the WLAN and that includes an automatically generated and updated database. The characteristics of location accuracy and performance of the wireless positioning system are analyzed with simulations. Sensitivity to location accuracy is compared between the traditional work, relative works, and the proposed scheme.

An analytical model for this dissertation is also developed to include more than two overlapping wireless networks. The validity of the results are evaluated in terms of the simulation model. A simulation model is always an approximation of a real system, expressing only a portion of the whole truth of

the studied phenomenon; the performance estimates of the simulation results have at least a theoretical value. While simulation studies can be easily extended for areas that are difficult to measure in a real-life testbed environment, experimental studies complement the analytical holistic approach. It must be noted that the results presented in this thesis were achieved from several research projects and separate tasks, thus resulting in some fragmentation in the overall scope. On the other hand, the methodology provides an overall analysis.

1.3 Contribution of the Thesis

This dissertation contributes to the given research problem area by utilizing architectural design, developing a theoretical and simulation framework, and providing proof-of-concept implementation and experimental results. First, a novel wireless network architecture is proposed to improve network efficiency by reducing the latency time at layer 2 and layer 3 during the handoff process and supporting AP traffic load balancing. The multi-radio AP with two transceivers is used to scan and find neighboring STAs in the transmission range and then sends the result to associated APs. This information is useful for current AP to control its associated STAs in order to initiate a handoff process whenever a neighbor AP can provide higher quality of service and/or better traffic load sharing with other APs. As a tradeoff for the advantages provided by the latency time reduction and the traffic balance among APs, customers might need to update the firmware in their wireless LAN cards in order to support the proposed handoff scheme. Simulations and results are used to compare the performance of the proposed system with the traditional work and relative works both in terms of handoff delay and traffic load balancing among

neighbor APs. The results demonstrate the importance of controlling the handoff delay and traffic load among APs.

Second, a novel wireless positioning system based on the WLAN infrastructure is proposed. This system integrates two location technologies: fingerprinting and TDOA. The multi-radio access point introduced in the first step is used to correct the information of neighbor STAs in the coverage area. The information regarding the STA is sent to its associated AP, which analyzes and searches the database to estimate the location of the STA by using a fingerprinting technique. The TDOA technique is used to estimate the location of the STA when there is not enough information in the database, such is the case when the STA moves to a new area where the system has not yet run the calibration phase. The simulations and results of this proposed system are analyzed and compared with a traditional algorithm and another related work [5] [6] in terms of location accuracy and disruption of the Internet connection for end users.

1.4 Outline of the Thesis

In this dissertation, a novel wireless network architecture and efficient wireless positioning system are proposed to improve the performance of future wireless LANs. The remainder of the dissertation is outlined as follows. Chapter 2 provides an overview of wireless LAN technologies along with the background and types of wireless LAN technologies. Then, the detail the WLAN handoff architecture and performance issues are explained. Moreover, this chapter provides an overview of the positioning system, including outdoor and indoor geolocations, the accuracy of the positioning method, and different types of wireless LAN positioning systems. Chapter 3 details the problem issues related to mobility engineering and resource allocation management.

Mobility management is elaborated through mobility scenarios, the handoff procedure, and resource allocation aspects, with an emphasis on transition analysis. The summary of contributions is given, and conclusions are offered at the end of the chapter. Chapter 4 describes the theoretical modeling of the WPS and discusses the details of each model. This chapter also introduces various parameters that might affect the accuracy of the positioning system, provides the details of each measurement scenario, and discusses the relationship between the scenario and specific parameters. The summary and discussion of results is presented through the simulations. Finally, chapter 5 concludes this dissertation and provides the directions for future research in this area.

Chapter 2

Technical Background

2.1 Introduction

This chapter presents an overview of wireless local area network (WLAN) technologies and standards. The details of IEEE 802.11 WLANs related to the handoff algorithm are discussed such as the handoff process and the handoff type. Moreover, the fundamentals of wireless positioning systems are reviewed, including outdoor and indoor positioning systems, the wireless position method, and performance issues.

2.2 Wireless Local Area Networks

Traditional local area networks (LANs) link computers, file servers, printers, and other network equipment using cables. These networks enable users to communicate with each other by exchanging electronic mail and accessing multi-user application programs and shared databases. Using cables, all computers that connect to this network are fixed at a location. People are no

longer confined to their desks; they can change locations and continue working. Thus, there is a need for a mobile, flexible network to access databases and the Internet. Wireless local area networks (WLANs) were introduced at the end of the 20th century; the emergence of WLANs brought the benefits of user mobility and flexible network deployment in local area computing. With mobility, a network client can migrate between different physical locations within the LAN environment without losing connectivity. A more compelling advantage of WLANs is the flexibility to reconfigure or to add more nodes to the network without much planning effort or cost of recabling, thereby making future upgrades inexpensive and easy.

WLANs deliver data rates in excess of 1 megabit per second (Mbps) and up to 11Mbps (IEEE 802.11b) or 54Mbps (IEEE 802.11a/g). They are normally used for computer data transfer within a building. WLANs allow easy implementation of broadcast and multicast services, although these services must be protected from unauthorized access. In a typical wireless LAN configuration (see Figure 2-1), a transmitter/receiver (transceiver) device called an access point (AP) connects to the wired network from a fixed location. The access point receives, buffers, and transmits data packets between the wireless LAN and the wired network infrastructure. A single access point can support a small group of mobile nodes and can function within a range of a few hundred meters.

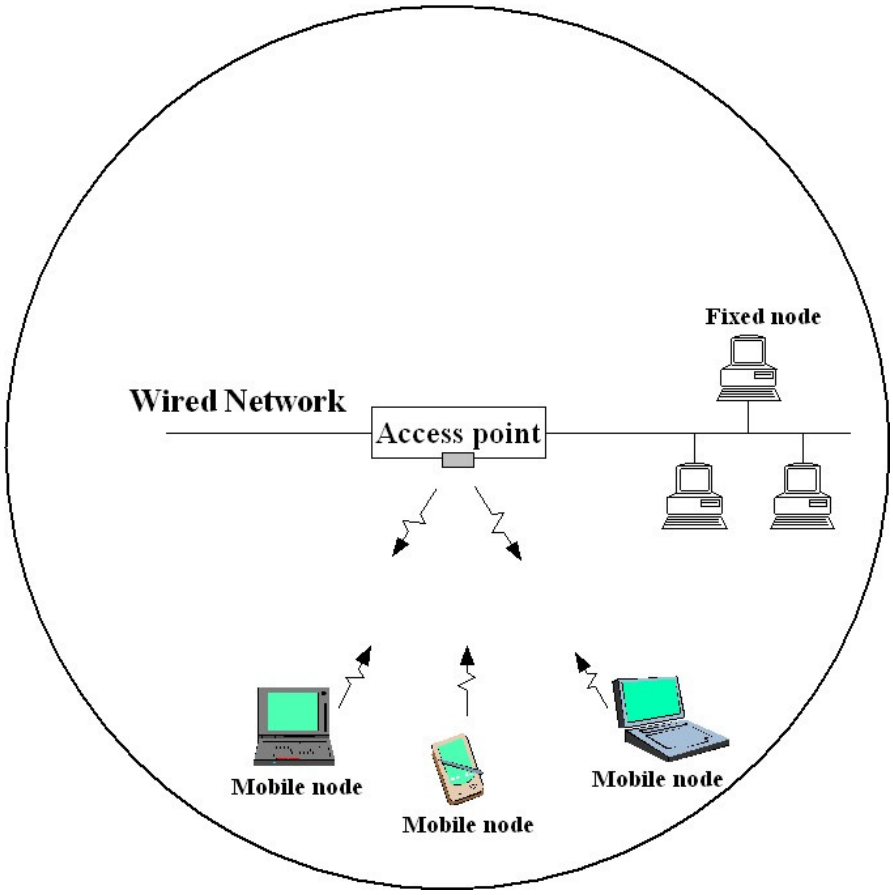

Figure 2-1. A Typical Wireless LAN Configuration.

2.2.1 Wireless LAN Standards

In 1990, the Institute of Electrical and Electronics Engineers (IEEE) formed a committee to develop a standard for wireless LANs operating at 1 and 2Mbps. Later, various committees were formed to develop standards for difference uses. The outline of these standards is explained in the following sections.

The IEEE 802.11 Wireless LAN standard

In 1997, the IEEE adopted the 802.11 standard [7], the first wireless LAN standard. This standard defines media access control (MAC) layers and physical (PHY) layers for a local area network with wireless connectivity. There are several specifications in the 802.11 family:

The 802.11 standard applies to wireless LANs and provides 1 or 2Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

The 802.11a standard is an extension of 802.11 that applies to wireless LANs and provides up to 54Mbps in the 5GHz band using an Orthogonal Frequency Division Multiplexing (OFDM) encoding scheme rather than FHSS or DSSS.

The 802.11b standard (also referred to as 802.11 High Rate or Wi-Fi) is an extension of 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2, and 1Mbps) in the 2.4 GHz band using only DSSS.

The 802.11g standard applies to wireless LANs and provides up to 54 Mbps in the 2.4 GHz band; it specifies complementary code keying (CCK) as the mandatory modulation schemes, with 24Mbps as the maximum mandatory data rate, but it also provides for optional higher data rates of 36, 48, and 54Mbps using OFDM encoding scheme.

HiperLAN

Developed by the European Telecommunications Standards Institute (ETSI), the high performance radio local area network (HiperLAN) is a set of wireless LAN communication standards used chiefly in European countries. This standard is similar to the IEEE 802.11 wireless LAN standards used in the United States.

The HiperLAN Type I standard is a wireless LAN standard that is ISO 8802 compatible (equivalent to IEEE 802). Like the 802.11 standard, HiperLAN Type 1 caters to both independent and infrastructure networks. However, it has only one physical layer specification that is not based on spread spectrum

transmission. HiperLAN Type 1 operates in the 5GHz band with a peak power level of 1W. It supports low-mobility users (1.4m/s) that carry asynchronous or isochronous traffic at a range of up to 50 m and a maximum wireless data rate of about 23.5Mbps [8].

The HiperLAN Type II standard is a flexible radio LAN standard designed to provide high speed access (up to 54Mbps at the PHY layer) to a variety of networks including 3G mobile core networks, asynchronous transfer model (ATM) networks, and IP-based networks. Unlike its predecessor, HiperLAN Type 2 has been specifically developed for a wired infrastructure, providing short range wireless access to IP, ATM, and universal mobile telecommunications system (UMTS) networks. HiperLAN Type 2 operates in the 5GHz frequency band with 100MHz spectrum.

Other Wireless LAN standards

In addition to the two wireless standards mentioned above, other wireless standard groups were formed to establish sets of wireless standards for different purposes, for example, WLIF OpenAir, HomeRF SWAP, Bluetooth, etc. This dissertation mainly focuses on the popular and widely used IEEE 802.11 Wireless LAN standard that is explained in the following section.

2.2.2 IEEE 802.11 Wireless LANs

The wireless LAN IEEE 802.11 standard specifies wireless connectivity for fixed, portable, and moving nodes in a geographically limited area. Specifically, it defines an interface between a wireless client and an access point as well as among wireless clients. As in any IEEE 802.x standard, such as the 802.3 carrier sense multiple access with collision detection (CSMA/CD) and the 802.5 (token ring), the 802.11 standard defines both the PHY and MAC layers. However, the

802.11 MAC layer also performs functions that are usually associated with higher layer protocols (e.g., fragmentation, error recovery, mobility management, and power conservation). These additional functions allow the 802.11 MAC layer to conceal the unique characteristics of the wireless PHY layer from higher layers.

IEEE 802.11 Physical Layer

The physical layer specification allows three transmission options that enable 802.11 wireless LANs to be deployed in different coverage areas, ranging from a single room to an entire campus. These options are direct sequence spread spectrum (DSSS), frequency hopping spread spectrum (FHSS), and diffuse infrared (DFIR) [8] [9].

Direct Sequence Spread Spectrum (DSSS)

The DSSS 802.11 packet format is shown in Figure 2-2. Some of the terms in the various fields of the PLCP header have been expanded to clarify their use in IEEE 802.11 standard [9]. Besides allowing a receiving node to detect the auto-correction peaks of the pseudo noise code and lock on to the timing of an incoming packet, the synchronization bits also enable selection of the appropriate antenna (if antenna diversity is employed). The signal field indicates whether the MAC protocol data unit (MPDU) is modulated using differential binary phase shift keying (DBPSK) at 1Mbps and differential quadrature phase shift keying (DQPSK) at 2Mbps and can be used to identify higher data rate extensions. The start frame delimiter indicates the start of the data packet; the length field defines the length of the MPDU; and the header error check protects the three fields in the physical layer convergence protocol (PLCP) header.

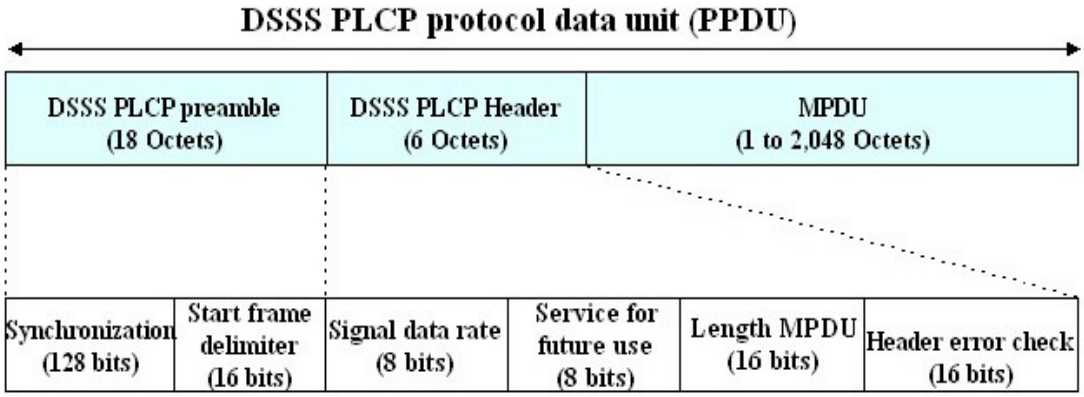

Figure 2-2. DSSS PLCP Packet Format

The 1Mbps basic rate is encoded using DBPSK, where each data bit is mapped into one of two phases. The 2Mbps enhanced rate uses DQPSK. In this case, two data bits are mapped into one of four phases of the spreading code. The DSSS 802.11 specification requires both data rates to be implemented. The receiver input signal level is specified as -80dBm for a packet error rate of 8×10^{-2}.

Frequency Hopping Spread Spectrum (FHSS)

The FHSS also uses the 2.4GHz ISM frequency band. The FHSS 802.11 packet format is shown in Figure 2-3. By comparing the DSSS and FHSS PLCP packet formats, it can be observed that FHSS requires fewer bits for synchronization. However, the maximum length of the MPDU for FHSS is longer compared to DSSS.

In Japan, a maximum of 23 channels are specified in the hopping set. The channel separation corresponds to 1Mbps of instantaneous bandwidth. Three different hopping sequence sets are established with four hopping sequences per set. Different hopping sequences enable multiple basic service sets (BSSs) to coexist in the same geographical area, which may become important to alleviate congestion and maximize the total throughput in a single BSS.

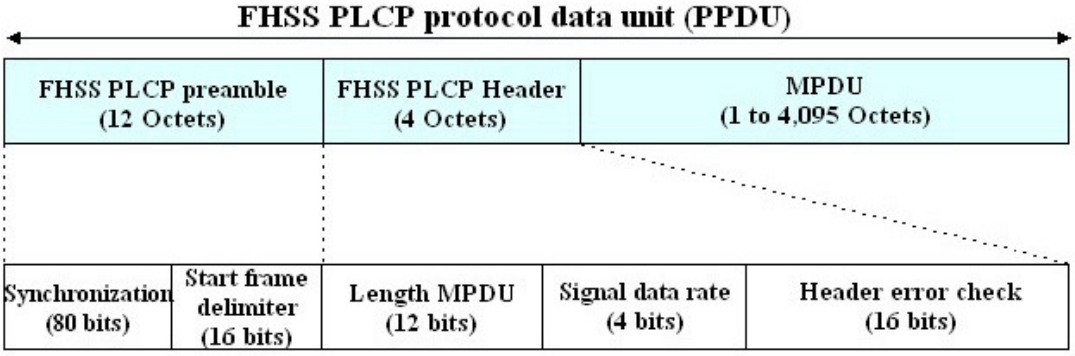

Figure 2-3. FHSS PLCP packet format.

Diffuse Infrared (DFIR)

The DFIR physical layer operates in the 850 to 950nm wavelength using pulse position modulation (PPM) with a peak power of 2W. The DFIR 802.11 PLCP packet format is shown in Figure 2-4. The first three fields are transmitted using on-off keying intensity modulation. The direct current level adjustment (DCLA) is used to allow the receiver to stabilize the average signal level after the transmission of the first three fields. The start frame delimiter (SFD) pattern requires careful selection, because it directly affects the packet error rate. The probability that the SFD is correctly detected depends on the probability of imitation and the probability of error of the SFD.

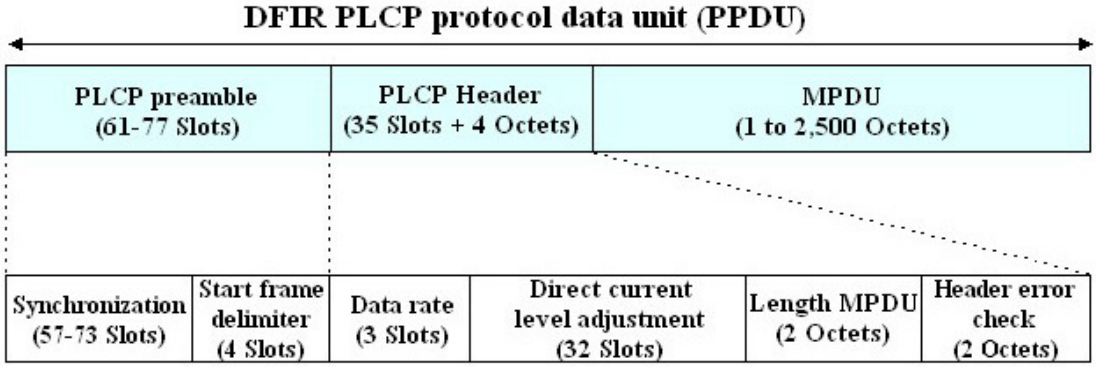

Figure 2-4. Infrared LAN PLCP Packet Format.

The DFIR band is designed for indoor use only and operates with non-directed transmissions. The DFIR specification was designed to enable stations to receive line-of-site and reflected transmissions.

IEEE 802.11 Medium Access Control (MAC) Layer

The 802.11 MAC layer is primarily concerned with the rules for accessing the shared wireless medium. Two different access methods, distributed coordination function (DCF) and point coordination function (PCF), have been defined. The function of the MAC protocol is common to all three PHY layer options (DSSS, FHSS, and DFIR) and is independent of the data rates [8] [9] [10].

Figure 2-5 shows the general 802.11 MAC protocol data unit (MPDU) format. IEEE 802.11 supports three different types of packets: management, control, and data. The management packets are used for mobile station association and disassociation with the AP, timing and synchronization, and authentication and deauthentication. Control packets are used for handshaking during the contention period (CP), for positive acknowledgments during the CP, and to end the contention-free period (CFP). Data packets are used for the transmission of data during the CP and CFP and can be combined with polling and acknowledgments during the CFP. The IEEE standard 48 bits addressing MAC is used to identify a station. The two duration octets indicate the time in microseconds that the channel will be allocated for successful transmission of a MAC protocol data unit. The type of bits identifies the frame as either control, management, or data. The subtype bits further identify the type of frame (e.g., clear to send control frame). A 32-bit cyclic redundancy check (CRC) is used for error detection.

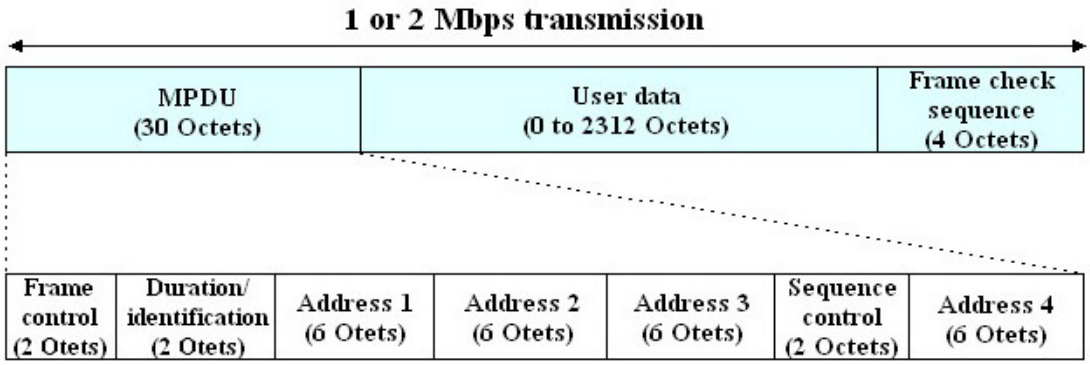

Figure 2-5. General MAC Protocol Data Unit (MPDU) Format.

Distributed Coordination Function (DCF)

The distributed coordination function (DCF) is the fundamental access method used to support asynchronous data transfer on a best effort basis. As identified in the specification, all stations must support the DCF. The DCF operates solely in the ad-hoc network and either solely or coexists with the PCF in an infrastructure network. The DCF is based on carrier sense multiple access with collision avoidance (CSMA/CA). In IEEE 802.11, carrier sensing is performed at both the air interface, referred to as physical carrier sensing, and at the MAC sublayer, referred to as virtual carrier sensing. Physical carrier sensing detects the presence of other IEEE 802.11 WLAN users by analyzing all detected packets and by detecting activity in the channel via related signal strength from other sources [8] [9].

A source station performs virtual carrier sensing by sending MPDU duration information in the header of request to send (RTS), clear to send (CTS), and data frames. An MPDU is a complete data unit that is passed from the MAC sublayer to the physical layer. The MPDU contains header information, payload, and a 32-bit CRC. The duration field indicates the amount of time in microseconds after the end of the present frame that the channel will be utilized to complete the successful transmission of the data or management frame.

Stations in the BSS use the information in the duration field to adjust their network allocation vector (NAV), which indicates the amount of time that must elapse before the current transmission session is complete and the channel can be sampled again for idle status. The channel is marked busy if either the physical or virtual carrier sensing mechanisms indicate that the channel is busy.

Priority access to the wireless medium is controlled through the use of interframe space (IFS) time intervals between the transmission of frames. The IFS intervals are mandatory periods of idle time on the transmission medium. Three IFS intervals are specified in the standard: short IFS (SIFS), point coordination function IFS (PIFS), and DCF-IFS (DIFS). The SIFS interval is the smallest IFS, followed by PIFS and DIFS, respectively. Stations only required to wait for a SIFS have priority access over those stations required to wait for a PIFS or a DIFS before transmitting; therefore, SIFS has the highest-priority access to the communications medium.

For the basic access method, when a station senses that the channel is idle, the station waits for a DIFS period and samples the channel again. If the channel is still idle, the station transmits an MPDU. The receiving station calculates the checksum and determines whether the packet was received correctly. Upon receipt of a correct packet, the receiving station waits for a SIFS interval and then transmits a positive acknowledgment frame (ACK) back to the source station, indicating that the transmission was successful. Figure 2-6 presents a timing diagram illustrating the successful transmission of a data frame. When the data frame is transmitted, the duration field of the frame is used to let all stations in the BSS know how long the medium will be busy. All stations receiving the data frame adjust their NAV based on the duration field value, which includes the SIFS interval and the ACK following the data frame.

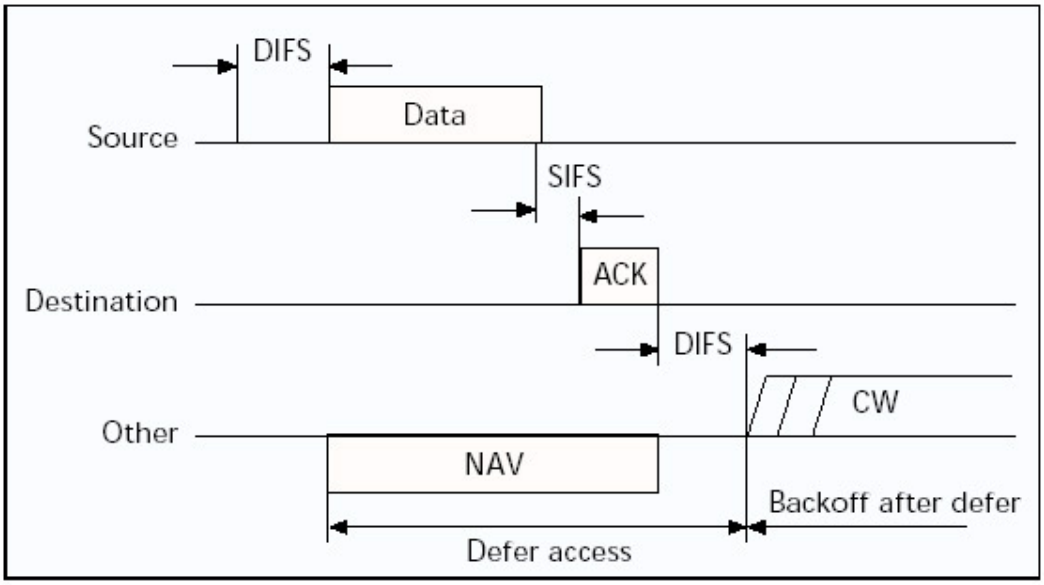

Figure 2-6. Transmission of an MPDU.

Since a source station in a BSS cannot receive its own transmissions, when a collision occurs, the source continues transmitting the complete MPDU. If the MPDU is large (e.g., 2300 octets), then a lot of channel bandwidth is wasted due to a corrupt MPDU. RTS and CTS control frames can be used by a station to reserve channel bandwidth prior to the transmission of an MPDU and to minimize the amount of bandwidth wasted when collisions occur. RTS and CTS control frames are relatively small (RTS is 20 octets and CTS is 14 octets) compared to the maximum data frame size (2346 octets). After successfully contending for the channel, the RTS control frame is first transmitted by the source station, with a data or management frame queued for transmission to a specified destination station. All stations in the BSS receive the RTS packet; the destination station responds to the RTS packet with a CTS packet after an SIFS idle period has elapsed. Stations receiving the CTS packet look at the duration field and update their NAV again. Upon successful reception of the CTS, the source station is virtually assured that the medium is stable and reserved for successful transmission of the MPDU. Note that stations are capable of

updating their NAVs based on the RTS from the source station and CTS from the destination station, which helps to combat the hidden station problem. The hidden station problem occurs when a station is visible from an AP but not from other stations communicating with said AP.

The collision avoidance portion of CSMA/CA is performed through a random backoff procedure. If a station with a frame to transmit initially senses that the channel is busy, then the station waits until the channel becomes idle for a DIFS period to compute a random backoff time. For IEEE 802.11, time periods are divided into slot times. Unlike slotted aloha, where the slot time is equal to the transmission time of one packet, the slot time used in IEEE 802.11 is much smaller than an MPDU; it is used to define the IFS intervals and determine the backoff time for stations in the contention period.

The time slot is different for each physical layer implementation. The random backoff time is an integer value that corresponds to the number of time slots. Initially, the station computes a backoff time in the range from 0 to 7 time slot. After the medium becomes idle after a DIFS period, stations decrement their backoff timer until the medium becomes busy again or until the timer reaches zero. If the timer has not reached zero and the medium becomes busy, then the station freezes its timer. When the timer is finally decremented to zero, the station transmits its frame. If two or more stations decrement to zero at the same time, a collision will occur, and each station will have to generate a new backoff time in the range 0 to 15 time slot. For each retransmission attempt, the backoff time grows as $[22 + i \times ranf()] \times SlotTime$, where i is the number of consecutive times that a station attempts to send an MPDU and *ranf()* is a uniform random variants in (0, 1). The idle period after a DIFS period is referred to as the contention window (CW). The advantage of this channel

access method is that it promotes fairness among stations. Fairness is maintained because each station must recontend for the channel after every transmission of an MSDU. All stations have an equal probability of gaining access to the channel after each DIFS interval [11].

Point Coordination Function (PCF)

Real-time traffic requires bounded end-to-end delays beyond which the information loses its value and may be discarded. There is an optional point coordination function (PCF) that may be used to support time-bounded services. PCF employs a centralized, contention-free multiple access scheme where nodes are allowed to transmit only when polled by the access point. Note that collisions may be introduced when access points transmit polling messages to mobile nodes stationed in overlapped wireless coverage areas.

To allow other nodes with asynchronous data to access the medium, the MAC protocol alternates between DCF and PCF, with PCF having higher priority access. This is achieved using a superframe concept where the PCF is active in the contention-free period, while the DCF is active in the contention period (see Figure 2-7). The contention-free period can vary in length within each superframe without incurring any additional overhead. At the beginning of the superframe, if the medium is free, PCF gains control over the medium. If the medium is busy, then PCF defers until the end of the packet has been transmitted/received or until an acknowledgment has been received. Since the PIFS is of shorter duration than the DIFS, PCF can gain control of the medium immediately after the completion of a busy period. Since the contention period may be of variable length, this causes the contention-free period to start at different times (see Figure 2-7). Similarly, a packet may start near the end of the

contention period, thereby stretching the superframe and causing the contention-free period to start at different times.

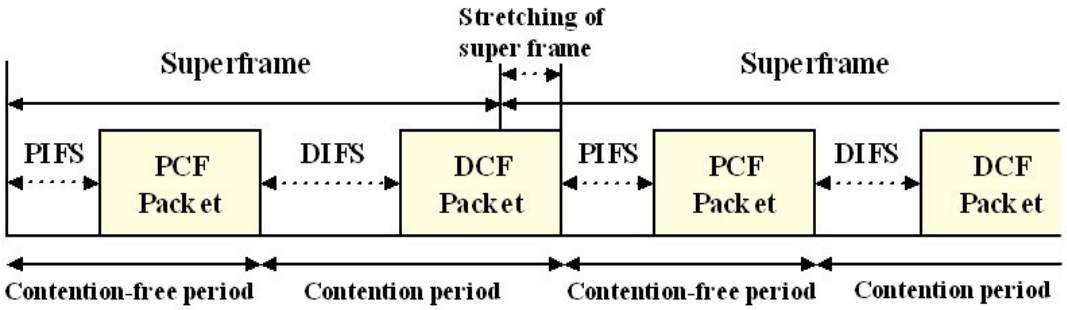

Figure 2-7. Coexistence of PCF and DCF in a Superframe.

Association and Reassociation

Association enables the establishment of wireless links between mobile nodes and access points in infrastructure networks. A node joins a network and is capable of transmitting and receiving data packets only after the association process is completed. To initiate a new connection with an access point, the node transmits a probe signal. After receiving a probe response from the access points, the node selects the access point with the best signal strength and then sends an association request to the access point, which will issue an association response.

Association is necessary but not sufficient to support mobility. In order to support mobility and roaming, an additional function, called reassociation, must be used in conjunction with the association function. Reassociation enables an established association to be transferred from one access point to another. Reassociation is always initiated by the mobile node. Association and reassociation are dynamic processes, since mobile nodes may power on, power off, move within range, or move out of range.

2.3 Handoff Schemes in Wireless LAN

Data loss, blocked data, and delayed data are unacceptable for wireless users, especially when using real-time services. Users expect to be able to connect to the network at any time and to receive high signal power and high speed connections. These user demands are addressed through the management of radio resources. Handoff is an important aspect of radio resource management. Handoff makes continuous connection possible by transferring a mobile station from one access point to another. Handoff also determines how many mobile stations can be served in a given area and the quality perceived by users. Thus, efficient handoff algorithms are essential for preserving the capacity and quality of service (QoS) of wireless communication systems.

2.3.1 Different Types of Handoff Schemes

This research distinguish two types of handoff: hard and soft. Hard handoff breaks that connection to the old base station (BS) before a connection to the candidate BS is made. Soft handoff does not break the connection to the old BS until a connection to the new BS is made [12] [13].

Hard Handoff

Hard handoff algorithms are employed in current cellular networking standards such as GSM, GPRS, and wireless LAN. In a hard handoff algorithm, the assignment set contains only one base station at a time. When a handoff occurs, the mobile station leaves the cell associated with the base station and enters the cell associated with another base station. Figure 2-8 illustrates the hard handoff scheme.

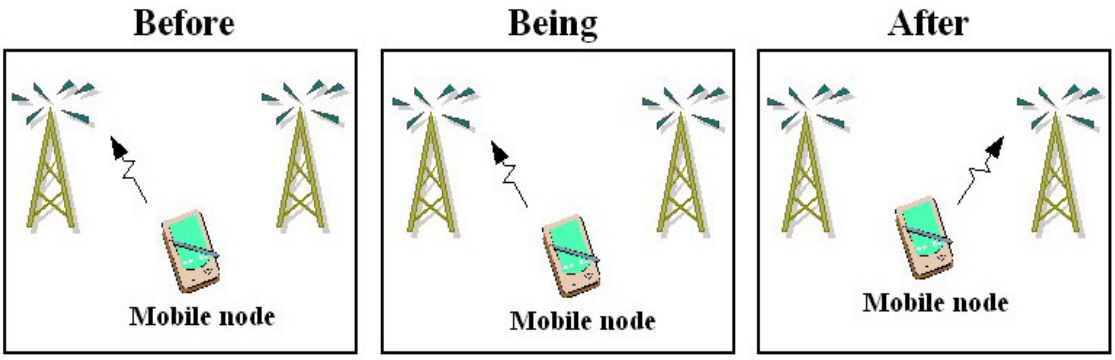

Figure 2-8. Hard Handoff Scheme.

Hard handoff is based on a simple approach that trades some packet loss in exchange for minimizing handoff signaling rather than trying to guarantee zero packet loss. Hard handoff causes packet losses proportional to the round-trip time and to the downlink packet rate. To perform a handoff, a mobile host tunes its radio to a new base station and sends a route-update packet. The route-update packet creates routing cache mappings enroot to the gateway, configuring the downlink route cache to point toward the new base station.

Soft Handoff

In soft handoff algorithms, the assignment set may contain more than one base station. Soft handoff employs diversity in order to make handoff transitions smoother. Soft handoff is employed in networks based on code division multiple access (CDMA), e.g., the IS-95, WCDMA, and CDMA2000. Figure 2-9 presents the soft handoff scheme.

To initiate soft handoff, the moving mobile host transmits a route-update packet to the new base station and continues to listen to the old one. Soft route-update packets create new mappings in the route and paging cache similar to regular route-update packets. When the soft route-update packet reaches the crossover router, where the old and new path meet, the new mapping is added to the cache instead of replacing the old one [14].

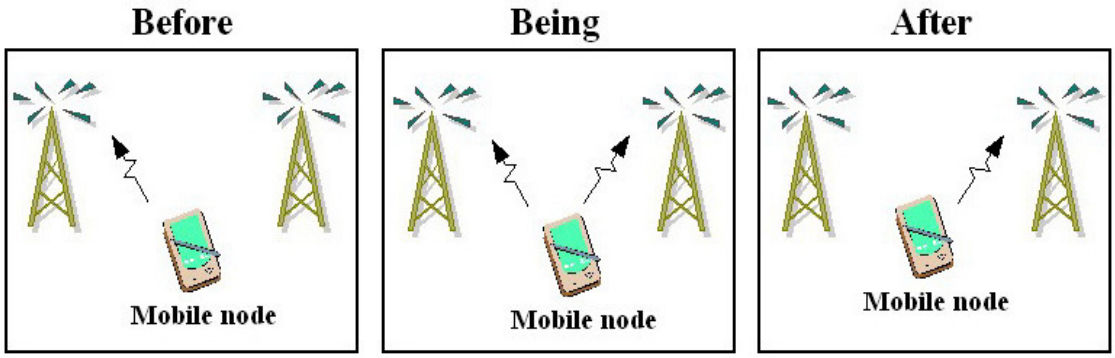

Figure 2-9. Soft Handoff Scheme.

Packets sent to the mobile host are transmitted to both downlink neighbors. When the mobile host eventually moves, the packets will already be moving to the new base station, and the handoff can be performed with minimal packet loss. After migration, the mobile host sends a route-update packet to the new base station. This route-update packet will remove all mappings in the route cache except for the ones pointing to the new base station. The soft handoff is then complete.

2.3.2 Conventional Handoff Scheme in WLAN

In IEEE 802.11 Wireless LANs, a mobile station leaving its current AP coverage area is required to initiate the handoff process in order to find the next AP and establish a link with that AP. The handoff is a function or process referring to the mechanism or sequence of messages generally exchanged by two APs and one mobile station, resulting in a transfer of physical layer connectivity and state information on the mobile station in consideration from one AP to another. In IEEE 802.11 (see Figure 2-10), the conventional handoff process is a kind of hard handoff [9]; as described in [15] the process is divided into three phases: detection, search, and execution. The three phases are explained in more detail below.

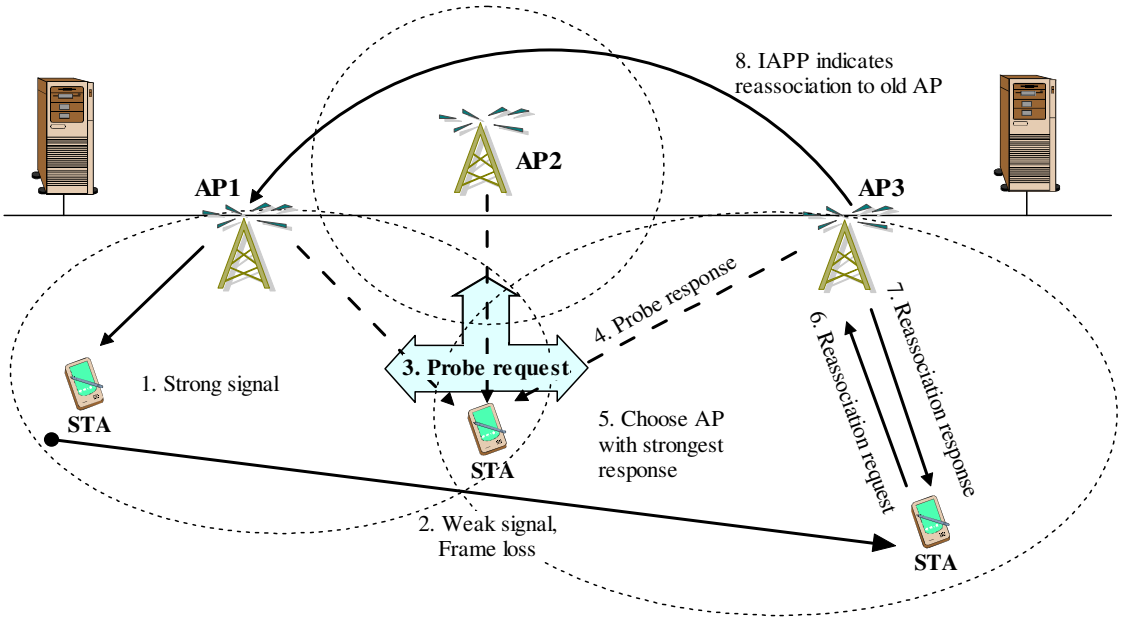

Figure 2-10. The Conventional Handoff Process.

Detection phase

The detection phase discovers the need for a handoff. The mobile station detects the reason for current frame loss among the following options: packet collision, interference, radio signal fading, or the mobile station being out of the AP's transmission range. As shown in Fig. 2-10, when the mobile station moves too far away from AP1, the signal strength received from AP1 becomes weak, and frame loss occurs. The mobile station then tries to retransmit data by reducing its data rate. If the mobile station does not receive any response after a specified period of time, the reason for the frame loss is determined as the mobile station is out of transmission range, and the mobile station decides to start a handoff. The time elapsed until the reason for the frame loss has been clarified is the delay time in this phase. Different wireless LAN cards use different assumptions depending on their purpose. Some wireless LAN cards reduce the bit rate and use the RTS/CTS mechanism after frame loss to overcome possible radio fading or collisions in an overloaded cell (see Fig. 2-11).

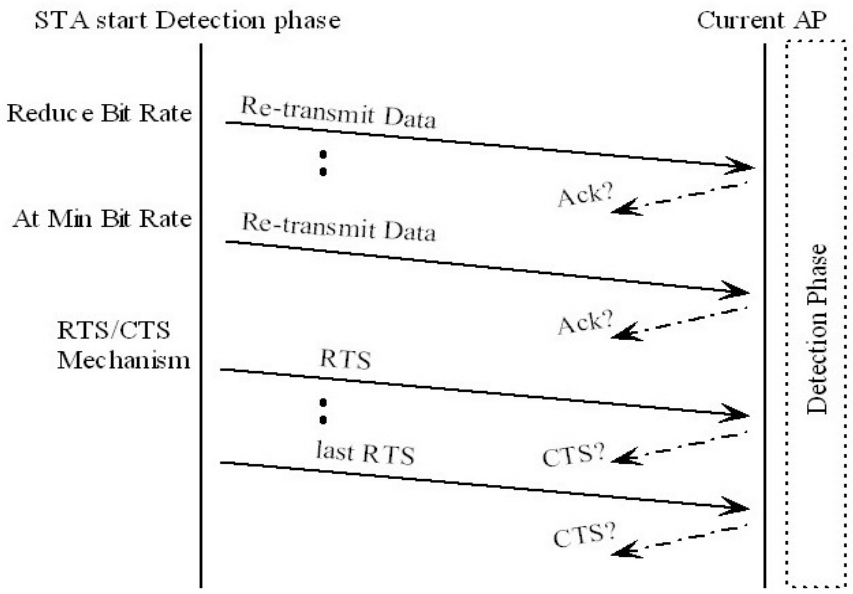

Figure 2-11. Process of Detection Phase in IEEE 802.11.

Search phase

The search phase includes a set of actions performed by the mobile station to find the information needed to perform the handoff. First, the mobile station scans for stronger signals from neighboring APs (see Figure 2-10). The scanning process can be either active or passive [9]. In passive scanning, the mobile station listens to each channel for the beacon frames. The main inconvenience of this method is how to calculate the time that it takes to listen to each channel. This time period must be longer than the beacon period, but the beacon period is unknown to the mobile station until the first beacon is received. Incidentally, the mobile station cannot switch to another channel when the first beacon arrives; it must wait for the whole beacon period, because several access points of different WLANs can operate in the same channel. Since the standard mandates that the entire set of allowed channels must be scanned, mobile stations need more than one second to discover the access points in range with the default 100ms beacon interval. For instance, there are 14 allowed channels in Japan, so this it process takes 1.4 seconds.

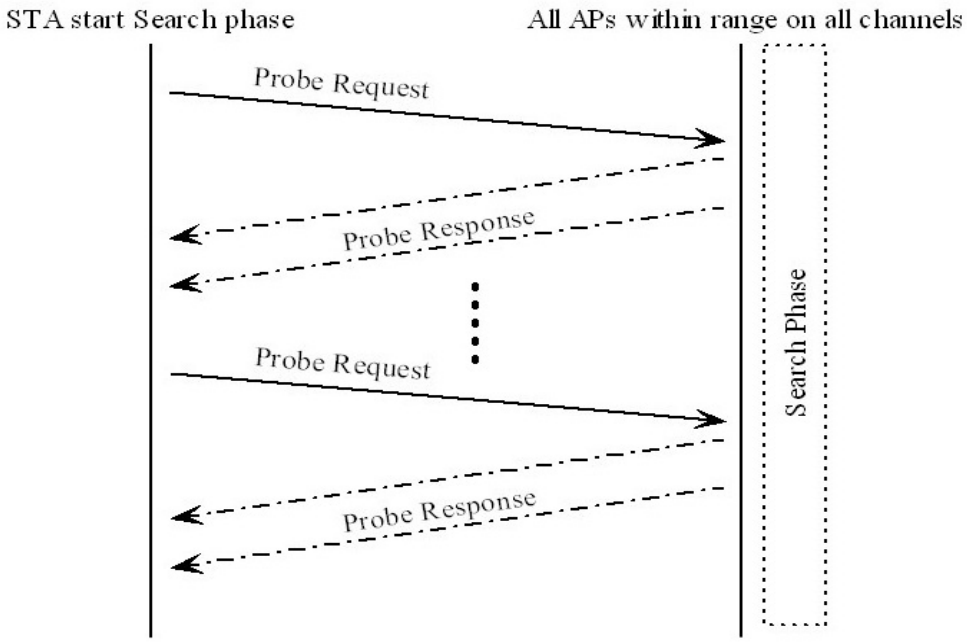

Figure 2-12. Search Phase using Active Scan.

In active scanning, the mobile station sends a probe request frame for each channel to scan and then waits for a probe response from every reachable AP. Each AP in range that receives the probe request will send back a probe response frame, which serves as a solicited beacon to the mobile station (see Figure 2-12) [9] [16]. The mobile station receives the neighbor APs' probe responses and then creates a report of all discovered APs and their characteristics. Next, the mobile station selects the most adequate AP to initiate the next handoff phase: execution. The delay time for active scaning corresponds to the amount of time needed to send the probe requests and receive the probe responses from all APs in range. The time that mobile stations should wait for responses in each channel is controlled by two timers: MinChannelTime and MaxChannelTime. The first refers to the time to wait for the first response in an idle channel. If there is neither response nor traffic in the channel during MinChannelTime, the channel is declared empty (no access point in range). The second timer, MaxChannelTime, indicates the time to wait

in order to collect all responses in a used channel. This limit is used when there was activity in the channel during MinChannelTime.

Execution phase

The simple execution phase is a two-step process. The mobile station sends a reassociation request to the new AP, which confirms the reassociation by sending a response with a status value of "successful." However, a typical execution phase takes a relatively long time to complete, because the new AP must authenticate the mobile station before the reassociation succeeds.

The 802.11 standard specifies two authentication algorithms: open system and shared key. The open system is the default and equals a null authentication algorithm, as previously explained. In the shared key algorithm, the execution process takes longer. It requires a four-step transaction (see Figure 2-13) that includes the inter access point protocol (IAPP). First, the mobile station sends a reassociation request to the new AP, which communicates with the current AP using the IAPP protocol. Finally, the new AP replies to the mobile station with a successful reassociation response.

The inter access-point protocol (IAPP) or IEEE 802.11f [17] is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless AP communications among multivendor systems. The protocol is designed for the enforcement of unique association throughout a extended service set (ESS) and for the secure exchange of the mobile station's security context between the current AP and the new AP during the handoff period. Based on security level, communication session keys between APs are distributed by a RADIUS server. The RADIUS server also provides a mapping service between the AP's MAC address and IP address.

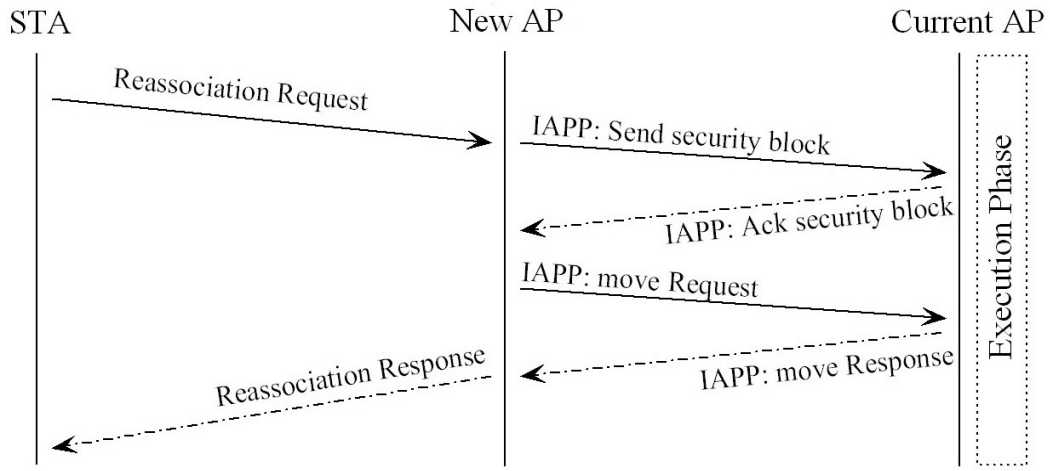

Figure 2-13. Execution Phase using IAPP.

2.3.3 Performance of the Handoff Process

Throughput and packet loss during handoff process

During the handoff process, the throughput is limited to sending and receiving data to/from the mobile host. According to various researches and simulation results, the throughput during handoff decreases in hard handoff schemes and increases in soft handoff schemes. This is because in soft handoff schemes, the mobile host can receive information from two base stations during handoff, so throughput is higher.

In terms of packet loss, the soft handoff scheme can receive packets from two base stations during the handoff process, so it is guaranteed to continue sending and receiving data. In contrast, the mobile host in the hard handoff disconnects from the old base station before starting the process to connect to the new base station. As a result, data packet loss occurs during the handoff process of switching to new base station. The number of packets lost during the handoff process depends on the mobility of the mobile host during that time; more packets will be lost if the mobile host is moving at a high speed [18].

Handoff Delay

Handoff delay refers to the time delay during the handoff process. This latency time depends on how long it takes the mobile station to initiate handoff, to find information for neighbor APs, and to connect to the new AP for authentication and reassociation.

Referring to the test-bed in Table 2-1 [15], the performance of the conventional handoff delay time does not meet the requirements of real-time applications. The detection phase is the longest phase in all cases, while the execution phase is the shortest phase and can be neglected. The search phase is also long compared to the execution phase. In this study, the detection phase and the search phase are focused in order to reduce the latency time during the handoff process.

Table 2-1. Handoff Time for Different IEEE 802.11 Cards.

	D-Link	Spectrum	Zoom Air	Orinoco
Detection	1630ms	1292ms	902ms	1016ms
Search	288ms	98ms	263ms	87ms
Execution	2ms	3ms	2ms	1ms
Total	**1920ms**	**1393ms**	**1167ms**	**1104ms**

Handoff Trigger

The handoff trigger decides whether to start handoff after completing the detection phase. In the conventional handoff scheme, the mobile station will start the detection phase after frame loss occurs; the mobile station will not start the search phase until the reason of frame loss is determined as the current AP

is out of range. The delay time before the mobile station starts handoff also affects the total handoff delay time. Most current wireless cards spend a lot of time proving the reason for frame loss [15], which causes a long delay time and is the main issue to be focused in order to reduce handoff time delay.

To study handoff trigger in more detail, the handoff start time in the conventional handoff scheme is evaluated by simulating the conventional handoff model in MATLAB [19] [20]. Two neighbor Access Points with cell radius of 300m and output power of 30mW (14dBm) are assumed. The distance between the centers of the neighbor APs is 400m. Hata's path loss model for urban areas [21] and Gaussian noise were used to calculate the signal power that the mobile station received. A mobile station moving from AP1 to AP2 at 50 times the normal speed of 10m/s (36 Km/h).

Figure 2-14 presents the results. The conventional handoff will start the search phase when there are some frame losses, meaning the signal strength from the base station received at the mobile station falls lower than the threshold level (-76dBm follow the IEEE 802.11 standard). In the conventional handoff scheme, the mobile station cannot start handoff to new base station, even it can provide better signal strength than the current base station. The results show the time differences in the conventional handoff scheme.

In order to support real-time applications with continuous mobility, the total latency provided at layer 2 and layer 3 during a handoff must be less than 50ms. In the other hand, the number of packets lost will decrease if the delay time decreases, meaning that data packet loss can be minimized by reducing the delay time during the handoff process. Thus, developing new technology to reduce handoff delay time is the first priority to provide real-time applications on wireless networks.

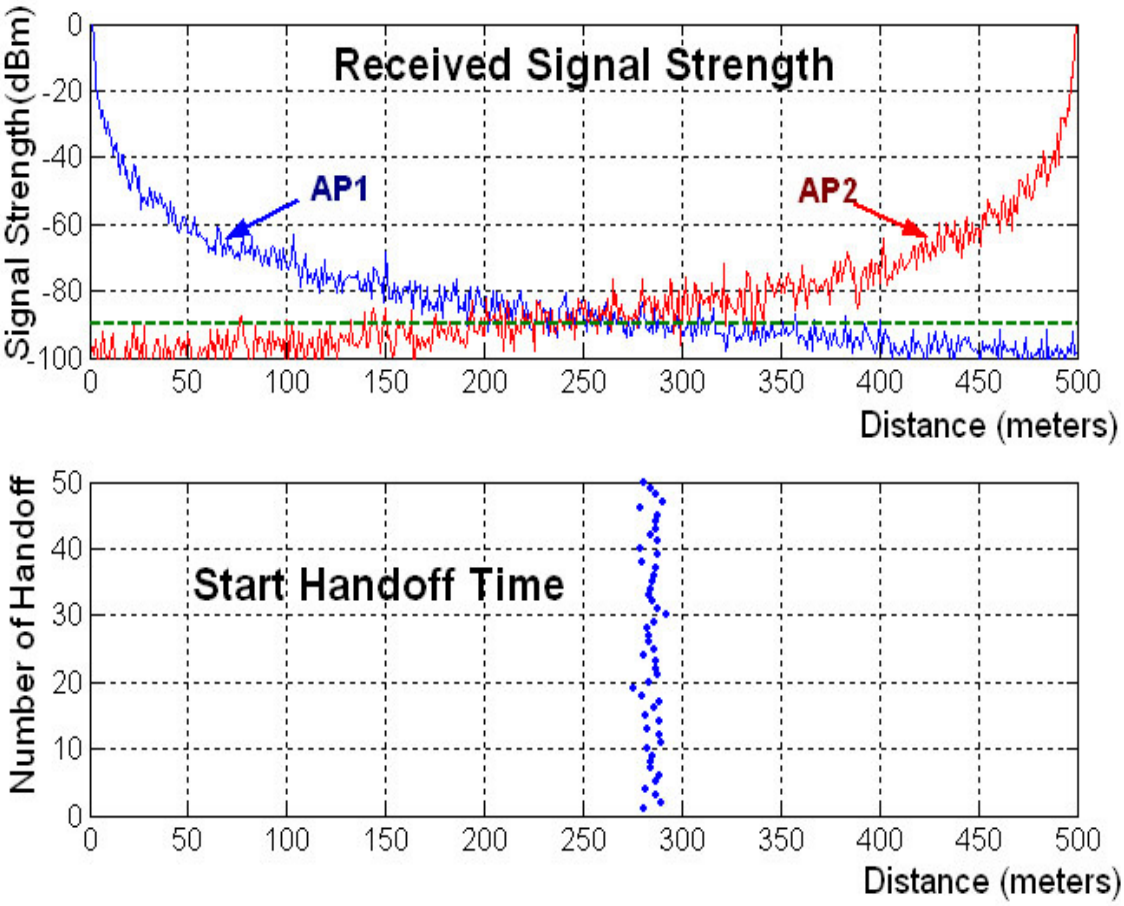

Figure 2-14. Start Handoff Time (Conventional Handoff).

2.4 Wireless Positioning System based on the WLAN Infrastructure

Localization using radio signals has been considered as an application of wireless communications since World War II, when locating soldiers in emergency situations was critical. This problem was addressed by the US Department of Defense during the war in Vietnam, when they launched a series of satellites under a project called the Global Positioning System (GPS). In the early days of GPS, these satellites were designated for military applications only. However, around 1990, they became partially available for commercial use. Today, GPS is widely used in commercial and personal applications. Although GPS has attracted numerous popular outdoor applications in open areas, it does not perform properly in highly dense, urban, and indoor areas.

In the late 1990s, around the same time that E-911 technologies were introduced, another independent initiative for accurate indoor geolocation was motivated by a variety of applications envisioned for indoor location-sensing in commercial, public safety, and military settings. In commercial applications, there is an increasing need for indoor location-sensing systems to track people with special needs, the elderly, and unsupervised children. Other applications include systems to assist the sight-impaired as well as to locate instrumentation and other equipment in hospitals, surgical equipment in operating rooms, and specific items in warehouses. For public safety and military applications, indoor location-sensing systems are needed to track inmates in prisons and to guide policemen, firefighters, and soldiers to accomplish missions inside buildings.

2.4.1 Positioning System Overview

A plethora of different positioning systems have been designed to determine and to track a user's location. These systems can be divided into outdoor positioning systems and indoor positioning systems (see Figure 2-15). The details of these location systems are explained below.

Outdoor Positioning Systems

Recently, outdoor positioning systems have become widely used. There are various technologies available for outdoor environments, for example, Global Positioning System (GPS), ground-based pseudo-satellite transmitter (GPS pseudolite), assisted GPS (A-GPS), time difference of arrival (TDOA), angle of arrival (AOA), and enhanced observed time difference of arrival (E-OTD).

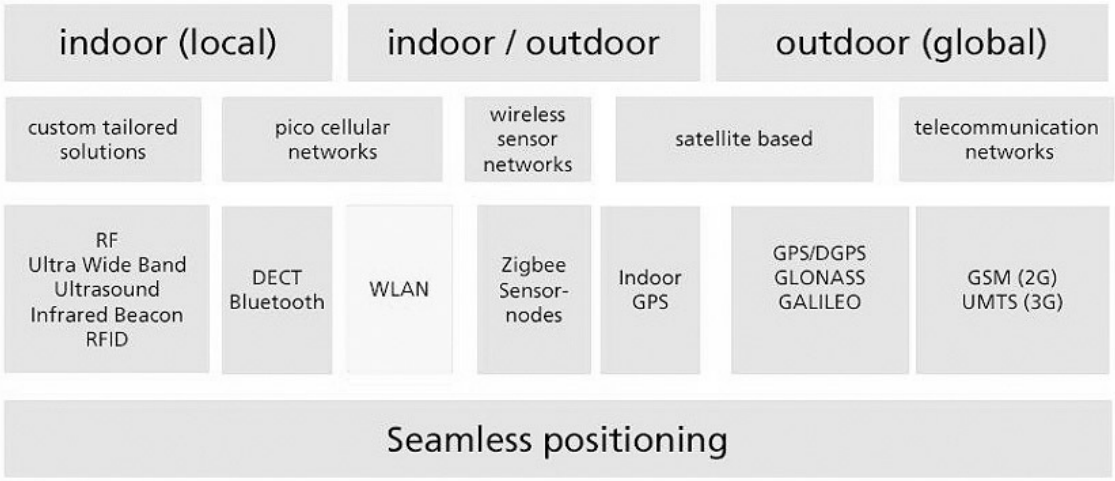

Figure 2-15. Overview of Positioning Technologies.

GPS is a satellite-based navigation system consisting of 24 or more satellites worldwide. Each satellite is placed about 20,000m above ground and transmits radio frequency (RF) signals to ground-based receivers. A GPS receiver calculates its position by measuring its distance from three or more GPS satellites. Measuring the time delay between transmission and reception of each GPS radio signal provides the distance to each satellite, since the signal travels at a known speed. The signals also carry information about the satellites' locations. By determining the position of (and distance to) at least three satellites, the receiver can compute its position using trilateration. The positioning accuracy of GPS after selective availability (SA) has been turned off typically ranges from 6 to 12m in 95% of cases [22]; however, GPS signals cannot be received close to high-elevation obstructions or inside buildings. To improve the GPS, Cobb [23] introduced a ground-based pseudo-satellite transmitter (GPS pseudolite) that is a device to transmit GPS satellite-like signals. Using a GPS pseudolite, a GPS receiver can determine its location even in the vicinity of obstructions that block GPS signals from orbiting satellites and can increase positioning accuracy.

Cellular phone carriers provide user location services using a number of systems, including assisted GPS (A-GPS), time difference of arrival (TDOA), angle of arrival (AOA), and enhanced observed time difference of arrival (E-OTD). A-GPS [24] is a technology that uses an assistance server to reduce the time needed to determine a location using GPS. A-GPS is assisted by base stations (BS) that provide information to the GPS processing a cellular phone, which can search for GPS signals quickly and can use the aiding information sensitively. The cellular phone sends the captured GPS signal to the base station, which then calculates the location of the cellular phone. TDOA, AOA/TDOA, and E-OTD are used by a few cellular phone carriers such as Cingular and AT&T wireless [25]. In geometric approaches, the RF signal measurements are transformed into angle and distance estimates, from which the signal source location is deduced using basic geometry and triangulation.

While these techniques have been found to provide good results outdoors, they are not so effective when deployed indoors due to multipath interference. The need for specialized hardware and fine-grain time synchronization leads to high costs for such solutions [26].

Indoor Positioning Systems

For an indoor environment, a number of different systems using infrared, ultrasound, radio frequency identification (RFID), and radio frequency (RF) devices have been designed to determine the user location (see Table 2-2 for a comparison of these technologies [22] [27]).

The Active Badges system [28] is an infrared-based location system that typically provides location information for small areas. A base station is placed in each room, and users carry a badge that emits an ID over infrared. The base

station senses the ID, and a central server collects the data from the base stations and determines the badge location.

The Active Bat system [29] is an ultrasonic-based location system that determines the bat tag position using time-of-flight measurement. In this system, users carry a bat that acts as an ultrasonic generator. Receivers mounted on the ceiling measure the distance to the bat, and a central controller determines the bat location. This system provides accuracy within 9cm of the true position in 95% of cases.

Table 2-2. Comparison of Indoor Positioning Technologies

Technology	*Accuracy*	*Note*
Infrared	0.7–2.5m	A clear view should be reserved between the IR transmitters and the IR receivers.
Ultrasound	3–30cm	Accuracy depends on the surrounding environment.
Passive RFID	10–30cm	Accuracy is affected by RFID readout errors and simultaneous readout of multiple tags.
Active RFID	5–7m	Covers a larger area than passive RFID, but need high internal power source.
RF-based Wireless LAN	3–5m	Accuracy depends on technologies and the surrounding environment.

RFID is an automatic identification method that relies on storing and remotely retrieving data using devices called RFID tags, which can also be used for location determination. In such systems, RFID tags are placed at key points, and the relation between tag ID and location is entered into a database. When the reader moves closer to a tag, it can report the tag's location to the user.

RF-based location system is mainly use IEEE 802.11 wireless local area networks and attempt to deal with the noisy characteristics of wireless radio that mainly result from multipath fading. The RADAR radio detection and ranging system [30] is one of the first examples of a wireless positioning system based on the WLAN infrastructure that uses an IEEE 802.11 network. This technique can provide location detection in urban areas and inside buildings; 75% of errors are less than 5m. In this method, a client device measures the amount of power that it receives from several access points and uses this information to discover its own location (x, y). The estimation process described in [30] is divided into an off-line phase (also called the calibration phase) and a online phase (estimation phase). During the off-line phase, the signal strength received from several APs is measured at fixed selected locations, forming a grid over the monitored area. This grid's positions and its respective received signal strength indicator (RSSI) values are recorded and stored in a database, resulting in a radio propagation map. During the online phase, the wireless client measures the RSSI values from all of the APs in range and tries to match them with the RSSI values in the propagation map to estimate the mobile station's location. The main problem with map-based techniques is the calibration effort in the off-line phase, addressed in [31]. The accuracy of such systems depends on this procedure, which consists of physically moving a wireless device over each radio map grid point and capturing RSSI values from APs. This kind of procedure is considered impractical and serves as a barrier to wider adoption.

Positioning Methods and Accuracy

If the manual input of the position is not considered as a location method, then positioning methods can be generally classified into two groups. The first

group is called network-based positioning. Here, the user location is tracked and evaluated using the base station network (see Image A in the Figure 2-16). The mobile device either sends a signal or is sensed by the network. The second positioning group is called terminal-based positioning (see Image B in the Figure 2-16). Here, the location is calculated by the user device itself from signals received from base stations. The most well-known example of a terminal-based system is the Global Positioning System (GPS). The base stations for the GPS system are GPS-satellites (see Image B in the Figure 2-16). If there is third group in future, this group of positioning techniques should be emerged from a combination of network and terminal positioning techniques.

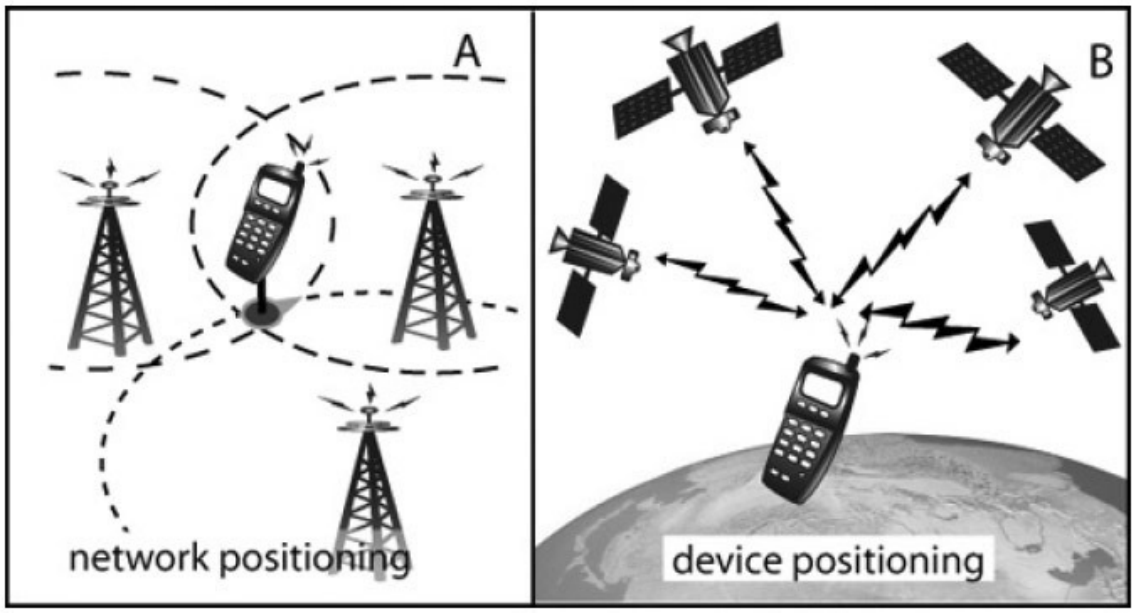

Figure 2-16. Types of Mobile Positioning.

The basic principles for the calculation of the user position, valid for all groups, are: 1) base Stations have a known position; 2) information from a signal is transformed into distances (not valid for angle of arrival); and 3) calculation of position using the obtained distances to the base stations (e.g. arc intersection in Image A of Figure 2-16). Several techniques are used in

combination for positioning. This chapter will discuss some of these techniques in the following sections

Cell of origin (COO), location signature, and location beacons: The cell ID usually identifies the nearest base station, e.g. a mobile phone antenna. With this technique, the position is known within a defined circle (or cell) around the base station's known position. This technique can use infrared, ultrasound, or RFID to estimate locations for indoor environments. Here, these beacons have an ID or transmit their exact position to the mobile device in reach.

Time of Arrival (TOA): Electromagnetic signals move at light speed (approximately 300,000km/s). Knowing the speed and the time difference between sending and receiving, the distance from user to AP can be computed. Runtimes are very short, and exact timers are needed. The same principle can also be used for slower signals like ultrasound.

Time Difference of Arrival (TDOA) and Enhanced Observed Time Difference (E-OTD): These techniques also compute the distance by measuring the runtime, but they use the time difference between the signals of three different base stations to triangulate the position. In the case of TDOA, the position is calculated by the network provider; in the case of E-ODT, it is calculated by the mobile device.

Angle of Arrival (AOA) and Direction of Arrival (DOA): Using antennas with direction characteristics, the angle of arrival in the mobile device can be detected; however, this is not exact. In addition, many base stations have segment antennas (usually two to four) that divide the circum-circle of the base station in segments of 90, 120, or 180 degrees.

The currently two most common positioning technologies are the already mentioned GPS and the position evaluation using the Cell-ID from the nearest

base transceiver station, a network method. Whereas GPS delivers position accuracy up to 5m, the Cell-ID delivers position accuracy between 100m to 1 km. Moreover, GPS is currently an outdoor positioning method. To obtain indoor positions with high accuracy, needed in museums or shopping malls, for instance, localization methods based on WLAN, Bluetooth, or infrared technologies should be applied.

In general, it is important to note that the position technology and its accuracy influence the application of different location-based services. Figure 2-17 shows a number of positioning methods along with their accuracy and their applicability to indoor and outdoor user activities. As a rule of thumb, one can say that network positioning is useful for LBS when precision is not critical. Figure 2-17 shows the positioning accuracy of network methods. Terminal based positioning is recommended for LBS when precision is important (e.g. dispatch, driving directions, or billing).

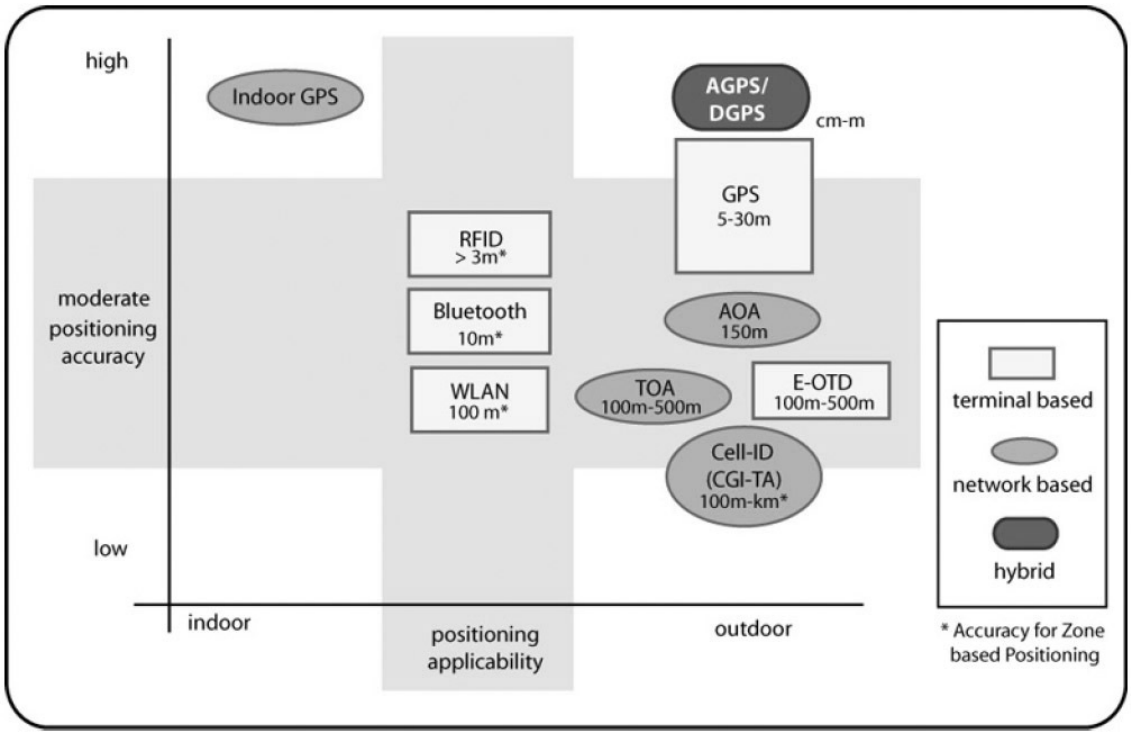

Figure 2-17. Positioning Methods, Accuracy, and Application.

2.4.2 WLAN Positioning System

With the advent of wireless Internet access, more and more WLANs are being deployed in offices and in homes. WLAN has quickly become the method of choice for wireless access in indoor and public areas. The IEEE 802.11b standard is the most widely used and is based on the 2.4GHz band, which can be used without license but is subject to a certain number of rules. It is the only ISM band that is globally available [32].

WLAN is not limited to communication use; it can also be used as a means of wireless positioning. Various received signal strength (RSS) techniques have been proposed. Due to its low cost and easy installment, WLAN offers the possibility of fulfilling the need for location-based services without additional equipment. There are various measurement techniques that can be used to determine the position of a mobile station. They are divided into three main groups:

- Distance Measurements: Time of Arrival (TOA), Time Difference of Arrival (TDOA), and Received Signal Strength (RSS) path loss;
- Angle Measurements: Angle of Arrival (AOA) and Direction of Arrival (DOA); and
- Fingerprinting: Received Signal Strength (RSS) patterns.

Distance and angle measurements are the most widely used for outdoor location systems, as they support high accuracy compared to other techniques. Angle measurements are based on the angle of incidence of the received signal. Distance measurements use the path loss model and Time-of-Flight (ToF) measurements to determine location.

The TDOA technique offers many advantages. Since all the processing takes place at the infrastructure level, no modifications are needed in the existing handsets; thus, this solution is more cost-effective. It also does not require knowledge of the absolute time of the transmission from the handset, unlike the modified handset TOA method. Since this technique does not require any special type of antennas, it is cheaper to put in place than the DOA methods. It can also provide some immunity against timing errors if the source of major signal reflections is near the mobile. If a major reflector affects the signal components going to all receivers, the timing error may become cancelled or reduced in the time difference operation. Hence, TDOA methods may work accurately in some situations where there is no LOS signal component. In this respect, it is superior to the DOA method and the TOA method.

Due to its simplicity, fingerprinting is the most widely used method for WLAN based indoor positioning system. This technique requires a training phase in which fingerprints are acquired by measuring the RSS values at particular locations and storing them in a database. In the online phase, the system measures the RSS values and matches the measured value to the closest location in the database. The drawback here is the extensive training values that must be predetermined, depending on the indoor environment.

This dissertation will focus on integrating fingerprinting and TDOA techniques to provide high location accuracy and automatic updating of the location database. The basic principles and algorithms of these two techniques are rigorously described below.

Location Fingerprinting

Location fingerprinting is a technique that exploits the relationship between a certain location and its corresponding radio signature. The RADAR system [30]

is one example. It employs a RF-based fingerprinting technique using received signal strength values. This type of system does not require any dedicated hardware other than the network system with wireless interfaces already in place. Hence, it is much easier to install compared to other systems.

A fingerprinting localization system consists of two phases: offline (calibration) and online (estimation). During the offline phase, a site survey is performed by measuring the RSS values from multiple APs. The floor is divided into predefined grid points, and then the RSS values are measured at predefined locations on the grid. Multiple measurements are taken, and the average values are stored in a database. The location fingerprint *F* refers to the vector of RSS values from each AP and their corresponding location *L* on the grid. A reference carpet refers to the collection of fingerprints and their associated locations for a given area (*L, F*).

To create a reference carpet, fingerprint vectors must be collected at particular locations. At a given location, the RSS values from every received AP are recorded over a specified period of time. This time window depends on the sampling rate of the WLAN card; it should be long enough for the mean ρ_i and standard deviation σ_i to be adequately described. Assuming that *N* access points can be heard at a given location, the fingerprint vector can be described as shown in Eq. 2-1.

$$\mathcal{F} = (\rho_1, \rho_2, \ldots, \rho_N)^T \quad \textbf{(2-1)}$$

In addition, the standard deviation may be added to describe the fingerprint in another vector as follows in Eq. 2-2.

$$\mathcal{D} = (\sigma_1, \sigma_2, \ldots, \sigma_N)^T \quad \textbf{(2-2)}$$

Preprocessing is the final process of the offline phase that much be completed before the location estimation phase. This is necessary to clean raw data such as dimensionality reduction using RSS values from predetermined APs, removing noise and feature extraction to significantly reduce the detection error.

In the online (estimation) phase, the RSS values are compared to the recorded samples in the offline phase and used to estimate the position. Position calculation is completely done on the mobile device. First, the mobile device scans for available APs and determines the RSS. The position is then calculated based on the carpet values, and the results are displayed. This avoids the need for communication with a central server. No additional access to the network is needed; thus, it provides a standalone localization solution independent of the environment.

A fingerprinting algorithm uses the Euclidean distance as an error metric to choose the reference point with minimum error. The Euclidean distance in signal space is computed for each RSS value against every reference point on the carpet. The reference point that is smallest in Euclidean distance to the RSS vector is chosen as the estimated position. However, this procedure alone is inefficient when the number of reference points increases. In addition, there is constant switching between matched reference points at room boundaries; hence, a more robust method needs to developed.

Time Difference of Arrival (TDOA) Technique

TDOA techniques estimate the difference in the arrival times of the signal from the source at multiple receivers. This is usually accomplished by taking a snapshot of the signal at a synchronized time period at multiple receivers. The cross-correlation of the two versions of the signal at pairs of base stations is completed, and the peak of the cross correlation output gives the time

difference for the signal arrival at those two base stations. A particular value of the time difference estimate defines a hyperbola between the two receivers on which the mobile may exist, assuming that the source and the receivers are coplanar. If this procedure is conducted again with another receiver in combination with any of the previously used receivers, another hyperbola is defined, and the intersection of the two hyperbolas results in the position location estimate of the source. This method is sometimes called a hyperbolic position estimation technique (see Figure 2-18).

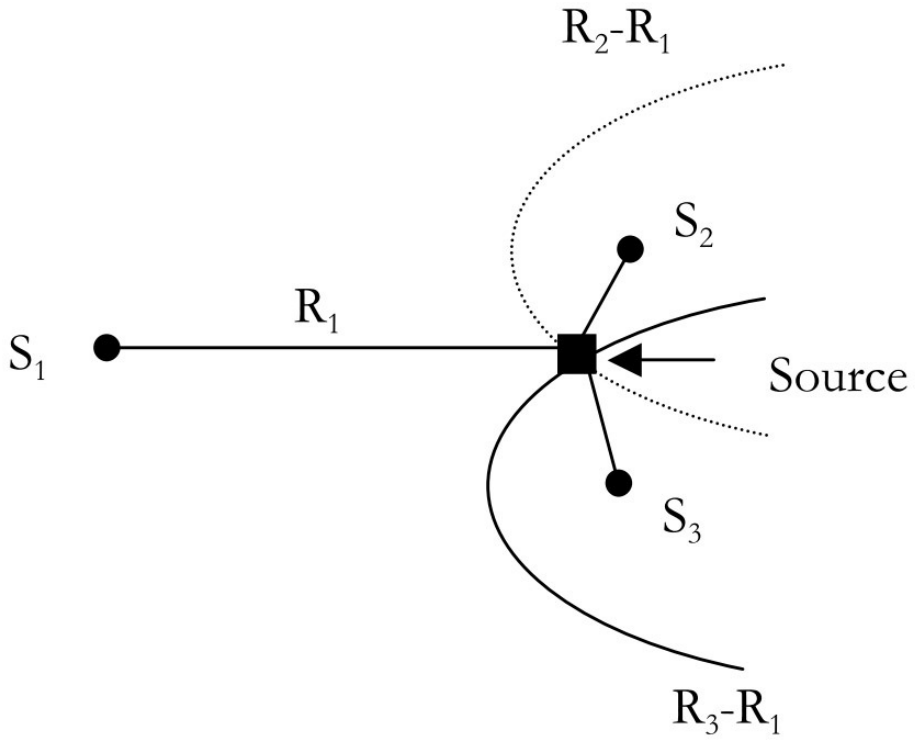

Figure 2-18. Hyperbolic Position Location Solution

Two distinct stages are involved in the hyperbolic position estimation technique. In the first stage, time delay estimation is used to find the time difference of arrival (TDOA) of acknowledgement signals from mobile stations to base stations. This TDOA estimate is used to calculate the range of distance difference measurements between the base stations. In the second stage, an

efficient algorithm is used to determine the position location estimation by solving the nonlinear hyperbolic equations resulting from the first stage.

TDOA can be estimated by subtracting the TOA measurements from the two base stations or correlating two versions of the acknowledgement signal at the two base stations. The latter method, commonly known as the generalized cross-correlation (GCC) method [17], is more robust and will be considered for this research.

Figure 2-19 shows the block diagram for determining the TDOA estimate using the GCC technique.

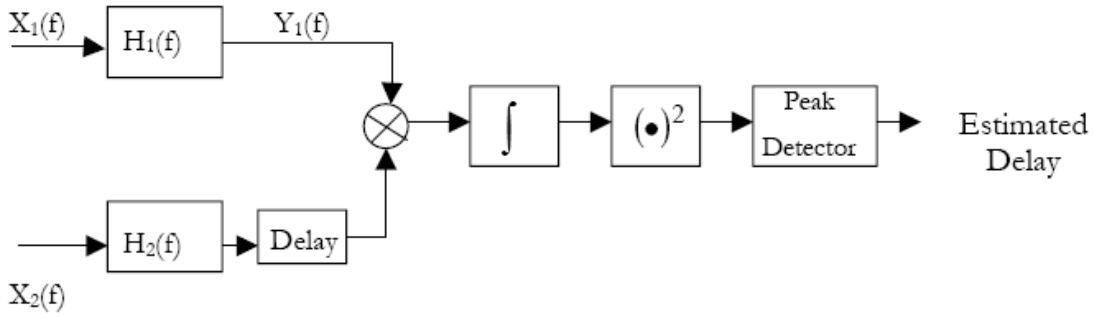

Figure 2-19. Delay Estimation by GCC Method

Mathematical Model for Hyperbolic Position Location: Let (*x, y*) be the source location and (*Xi, Yi*) be the known location of the i^{th} BS, where *I* = 2, 3…*M* and *M* is the total number of BS taking part in position location. Moreover, assume that BS1 is the controlling BS. The range difference between source and the i^{th} BS is

$$\begin{aligned} R_i &= \sqrt{(X_i - x)^2 + (Y_i - y)^2} \\ &= \sqrt{X_i^2 + x^2 - 2X_i x + Y_i^2 + y^2 - 2Y_i y} \\ &= \sqrt{X_i^2 + Y_i^2 - 2X_i x - 2Y_i y + x^2 + y^2}. \end{aligned} \qquad \textbf{(2-3)}$$

The range difference between the base stations with respect to BS1 is given as:

$$R_{i,1} = cd_{i,1} = R_i - R_1 = \sqrt{(X_i - x)^2 + (Y_i - y)^2} - \sqrt{(X_1 - x)^2 + (Y_i - y)^2}, \quad \textbf{(2-4)}$$

Where c = velocity of electromagnetic wave ($3x10^8$ m/sec) and $d_{i,1}$ = TDOA between i^{th} BS and BS1

Using Eq. 2-3 and Eq. 2-4,

$$\begin{aligned}
&R_{i,1} = R_i - R_1 \\
&\Rightarrow R_i = R_{i,1} + R_1 \\
&\Rightarrow R_i^2 = (R_{i,1} + R_1)^2 \\
&\Rightarrow R_{i,1}^2 + 2R_{i,1}R_1 + R_1^2 = X_i^2 + Y_i^2 - 2X_i x - 2Y_i y + x^2 + y^2 \\
&\Rightarrow R_{i,1}^2 + 2R_{i,1}R_1 = X_i^2 + Y_i^2 - 2X_i x - 2Y_i y + x^2 + y^2 - R_1^2 \\
&\Rightarrow R_{i,1}^2 + 2R_{i,1}R_1 \\
&= X_i^2 + Y_i^2 - 2X_i x - 2Y_i y + x^2 + y^2 - X_1^2 + Y_1^2 - 2X_1 x - 2Y_1 y + x^2 + y^2 \\
&\Rightarrow R_{i,1}^2 + 2R_{i,1}R_1 = X_i^2 + Y_i^2 - 2X_{i,1} x - 2Y_{i,1} y + x^2 + y^2 \quad \begin{bmatrix} (X_1, Y_1) = (0,0) \\ X_{i,1} = X_i - X_1 \\ Y_{i,1} = Y_i - Y_1 \end{bmatrix}.
\end{aligned}$$

(2-5)

Suppose the above Eq. 2-5 is linear, with the source location (*x, y*) and the range of the mobile from the controlling base station R_1 as the unknown variables. If *x* and *y* can be expressed in terms of R_1, then the solution for R_1 can be obtained from the following equation:

$$R_1^2 = x^2 + y^2 \qquad [\text{since, } (X_1, Y_1) = (0,0)] \qquad \textbf{(2-6)}$$

Knowing R_1, the position location of the mobile station can be estimated.

This chapter has identified some problems and reviewed techniques to address these issues, next chapters will focus on developing new wireless network architecture to improve WLAN support seamless handoff and balance traffic load. Furthermore, the WLAN-based positioning system can support high location accuracy and uninterrupted Internet connectivity.

Chapter 3

A Seamless Handoff Scheme with Access Point Load Balance

This chapter discusses issues related to mobility engineering and resource allocation management, and presents a novel wireless network architecture. This architecture is analyzed through the simulations and compared with the conventional and relative works.

3.1 Introduction

Wireless LANs based on the IEEE 802.11 standard have become popular and widely used for mobile Internet services. There are many Wi-Fi hotspots to support Internet access in many convenient areas such as airports, hotels, and coffee shops. Currently, these wireless networks can provide high-speed Internet connectivity of up to 11Mbps (IEEE 802.11b) or 54Mbps (IEEE 802.11a/g), which can support real-time services. However, recent works [1] address the problem of a mobile station (STA) that moves from one WLAN access point (AP) to another while remaining connected to the Internet. In this

case, the delay time involved in the handoff process when a STA switches from its current AP to an adjacent AP becomes an important issue for supporting seamless connectivity for a mobile host in IEEE 802.11-compliant wireless networks, especially for real-time applications such as voice over IP (VoIP), e-conference, and e-learning services.

In order to support real-time applications with continuous mobility, there must be a small total latency provided at layer 2 and layer 3 during a handoff. In more specific terms, the overall latency should not exceed 50ms to prevent excessive delay and jitter [33]. Unfortunately, the vast majority of Wi-Fi based networks do not currently meet this goal. Layer 2-related latencies contribute to approximately 90% of overall latency times, which exceed 100ms [25], while handoff-related latencies in layer 3 have an average of 15.37ms.

One method of reducing the handoff latency in IEEE 802.11 wireless networks is the proactive neighbor caching (PNC) scheme, which was proposed in [34]. The PNC scheme uses a neighbor graph that dynamically captures the mobility topology of a wireless network as a means for pre-positioning the station's context (i.e. session and QoS related state information). The PNC scheme ensures that the station's context is always dispatched to all of the current AP's neighbors, thereby reducing the handoff latency. This proposed scheme is enhanced by the selective neighbor caching scheme introduced in [35]. However, in these schemes, when the signal strength from the current AP is higher than the threshold value, the STA will not be able to start the handoff to a neighbor AP that provides better quality, even when there is high traffic load in the current AP. Therefore, the PNC scheme may result in packet dropping due to high traffic load in one basic service set (BSS), especially when there are a considerable number of STAs. Furthermore, the PNC scheme does not focus

on the delay time during the detection phase, which has the highest impact on the total handoff latency time.

This research propose a novel wireless network architecture that effective manages networked data by means of a multi-radio AP with fast passive scan phase to improve network efficiency by reducing the latency time at layer 2 and layer 3 during the handoff process and supports AP traffic load balancing. The multi-radio AP uses the second transceiver to scan and find neighboring STAs in the transmission range and then sends the result to associated APs. This information is useful for the AP to control associated STAs in order to initiate a handoff process whenever a neighbor AP can provide higher quality of service and/or better traffic load sharing with other APs. Besides the advantages provided by the latency time reduction and the traffic balance among APs, the proposed system does not require customers to change or upgrade their wireless LAN devices. Instead, users are only required to update the firmware in their WLAN cards to support the novel handoff scheme.

The rest of this chapter is organized as follows. In Section 3.2, related works are described. Section 3.3 explains the proposed scheme in detail. Section 3.4 presents the analysis and simulation results of the proposed handoff scheme. The conclusion is presented in Section 3.5.

3.2 Recent Work

Recent research has focused on improving the performance of wireless LANs through the reduction of delay time during the handoff process. Most of these studies intend to reduce the time spent in the search and execution phases. As described in [33], the time spent in the search phase is dominant compared to the execution delay time and should be considered; in [36] a new scheme was

proposed to reduce this delay time. The proposed scheme attempts to reduce the time spent in the search phase using the selective scanning algorithm [36] to decrease the total number of scanned channels as well as the total time spent on each channel during the search phase. The current AP provides the STA with information on neighbor APs. When the STA starts the handoff, it will scan only APs on the list provided by the current AP.

Conversely, the technique described in [37] focuses on reducing the latency time in the execution phase using the frequent handoff region (FHR) selection algorithm. The FHR is a set of APs with greater probabilities that STAs will visit them in the near future. The FHR is constructed based on handoff frequency and user priority. The STA that enters the area covered by the AP performs authentication procedures for multiple APs rather than just for the current AP. These multiple APs are selected using a FHR selection algorithm that takes into account user mobility patterns, service classes, etc. Since the STA is registered and authenticated for the FHR in advance, the handoff latency resulting from reauthentication can be minimized.

Multi-radio systems [38] [39] are also emerging as a practical way to implement multi-channel protocols to reduce the latency time in the handoff process. An STA with multiple radios is used for better mobility management, capacity enhancement, and avoiding channel failures. This STA can communicate with multiple APs at the same time without experiencing any delay or packet loss as it moves from one AP to another. The STA completes the authentication before the link with the current AP breaks down; this condition provides an upper bound on the authentication time of a security protocol. Thus, with proper network design, a dual radio system will not result in packet loss and only minimal packet delay, which is similar to the results that soft

handoff provides. However, since the STA uses the second transceiver to communicate with another AP, the traffic load increases. To use this system, customers will need to buy a new wireless LAN card with multiple-radio support.

Currently, to the best of the author's knowledge, there is no research focusing on reducing the handoff latency time as well as improving the performance of wireless networks through traffic load balancing among neighbor APs. Thus, the idea of a novel handoff scheme that provides seamless handoff and supports traffic load sharing becomes attractive.

3.3 Theoretical Modeling [40] [41]

As mentioned in [15], the main difficulty in deciding whether to perform the handoff is determining the reason for frame loss. The techniques used by most WLAN cards spend a lot of time in the detection phase to verify that the AP is out of range before starting the search phase. In the search phase, the STA also spends a long time broadcasting a probe request frame in each channel and then waiting for probe responses from neighbor APs in order to find information about them. These high delay times prohibit the smooth handoff needed to support real-time services.

Using the conventional handoff scheme, the STAs cannot start the handoff until there are frame losses, because there is no information regarding neighbor APs, and the handoff process is controlled by the STAs. Thus, in order to improve the performance of wireless LANs and reduce the latency time in the handoff process, a novel wireless network architecture is introduced. In this architecture, the AP will have all of the information of its own STAs and can control the handoff process. This architecture effective manages wireless

network by using the multi-radio AP with fast passive scan phase, an effective handoff process, and a handoff decision technique using the fuzzy logic rule base. These techniques work simultaneously to reduce latency time and shares traffic load among neighbor APs to support real-time applications.

Figure 3-1 shows a block diagram of the multi-radio AP with two transceivers, both using the same transceiver utilized in standard wireless LAN cards. The AP uses the second transceiver to scan and find information about neighboring STAs in its range using a fast passive scan mode (see Fig. 3-2), while the first transceiver works as a normal transceiver by sending and receiving data as in the conventional scheme. The information on neighbor STAs received from the second transceiver is sent to associated APs, which compare this information to their own data. As shown in the block diagram of the new AP module (Fig. 3-1), the AP has two transceivers that include RF filters, RF switches, up-and-down converters, as well as digital-to-analog and analog-to-digital converters. Each transceiver is the normal transceiver of wireless LAN cards, but both of them are connected to a MAC layer that allow us to control by programming the firmware. Recent studies have used one antenna to send and receive multi-radio frequencies for MIMO systems. However, the AP with two antennas is used in this research to prevent the reflective noise and interference. In the proposed scheme, the AP will use the second transceiver only for listening to nearby STAs in the transmission range without sending any information, so traffic load does not increase. The second transceiver listens to each channel by switching the central frequency to any of a number of frequencies that it has on a list.

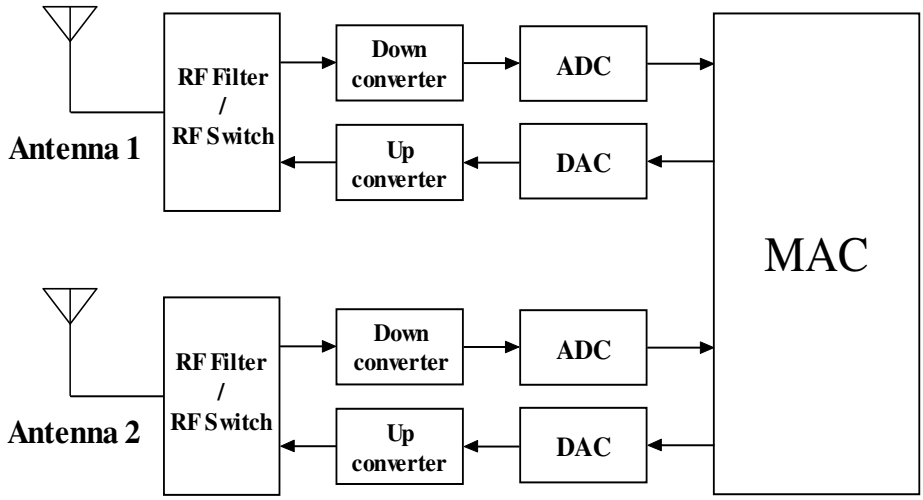

Figure 3-1. Block Diagram of a New AP Module.

Fig. 3-2 shows the flow diagram of the multi-radio AP used to scan and find information about neighboring STAs in its range. First, the AP checks the list of channels that the neighbor APs in the network are currently using (the presence of a gateway server that records information about all APs in the network is assumed). Next, starting from the first channel on the list, the AP scans each channel, skipping the channel that is currently being used by its first transceiver to prevent reflective noise and interference. The AP listens for data frames on each channel (every STA is transmitting real-time packets with a packet inter-arrival time of less than 50ms). Upon receiving data frames from any STA, the AP analyzes them and then sends the in-advance information, including the average signal strength of packets sent by the STA and its own traffic load conditions, to the AP associated with the STA. The address of the AP associated with the STA can be directly extracted from the header of the data frame sent by the STA. This procedure is carried out separately for each channel.

Fig. 3-3 shows the message flow of the proposed handoff process. Using the second transceiver, AP2 overhears a data frame from the STA when the STA sends a data frame to its associated AP1. AP2 analyzes this information and

then sends information in-advance to the associated AP1 via a gateway; this information includes the received signal strength from the STA and the traffic load condition of AP2. AP1 analyzes and compares this information with its own data using a handoff decision technique with the fuzzy logic rule base to decide whether to order the STA to initiate a handoff process. In addition, an hysteresis factor is used to compare the signal strength between AP1 and AP2 in order to avoid the ping-pong effect, which takes a severe toll on the user's quality perception and the network load (for details of this effect, see [42] and [43]).

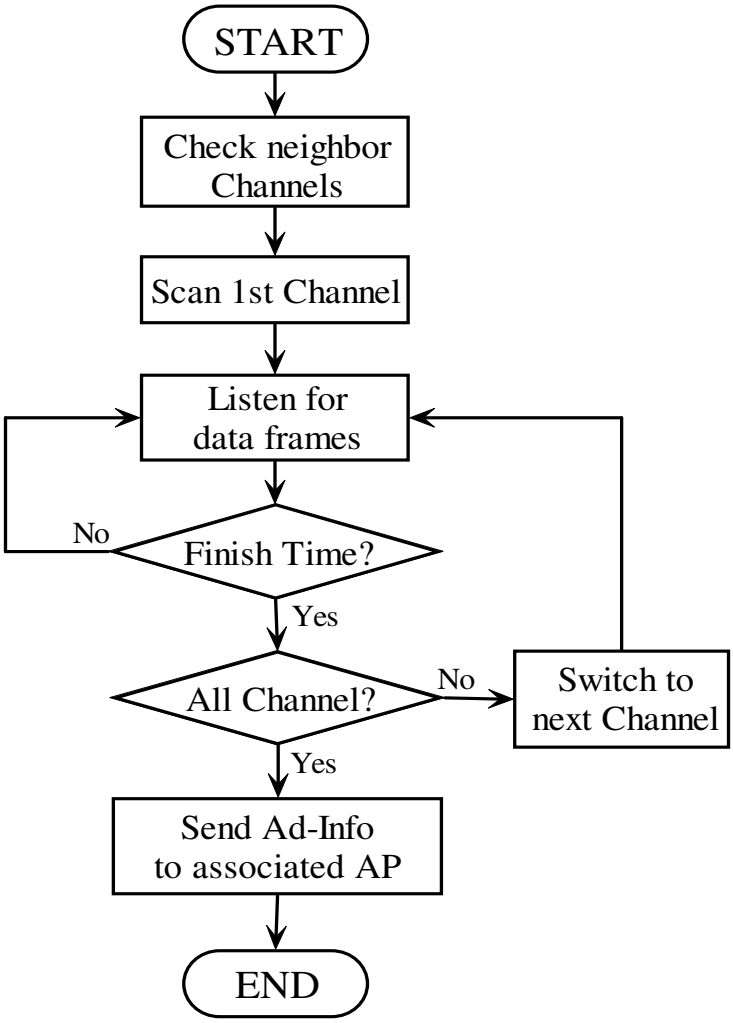

Figure 3-2. Fast Passive Scan.

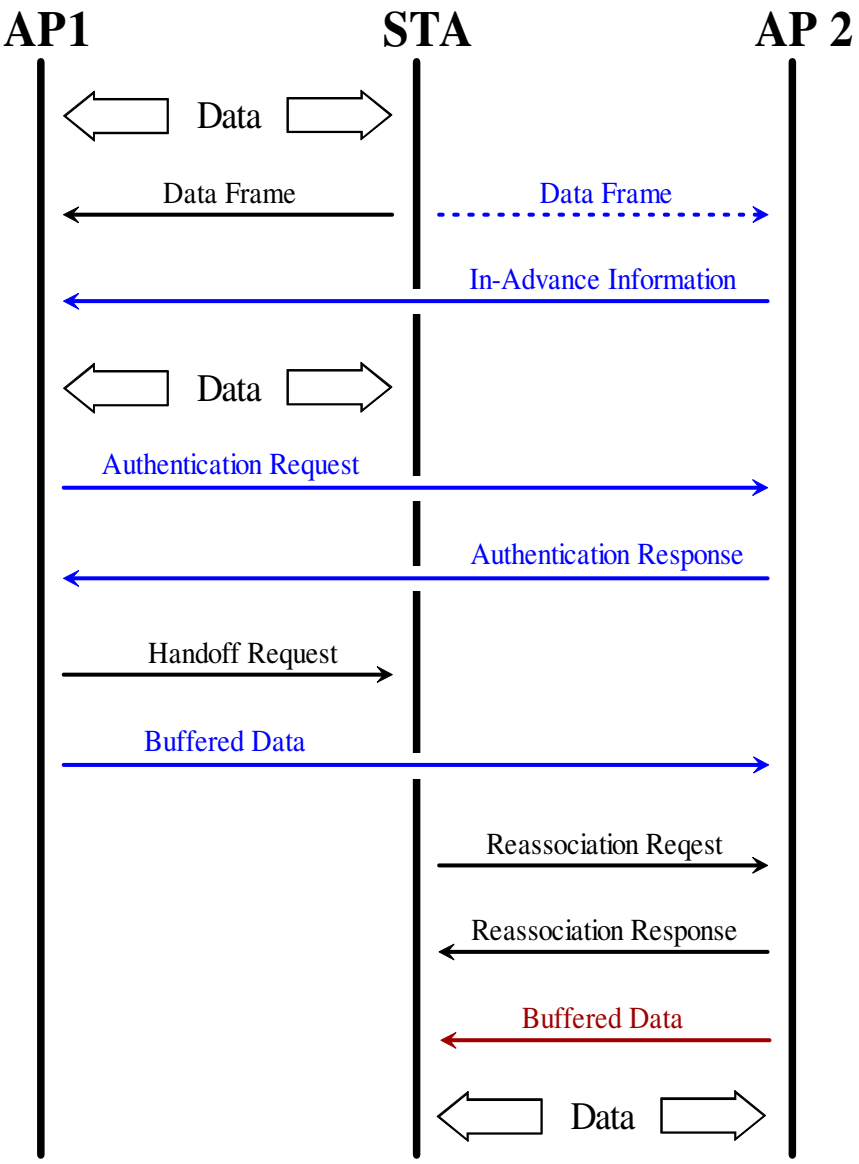

Figure 3-3. Proposed Handoff Process.

Regarding the process to inform the STA, AP1 first performs the pre-authentication process with AP2 (Fig. 3-3). AP1 sends an authentication request message to AP2 that includes the STA's identity. AP2 receives the message, performs an authentication procedure for the STA, and then sends back an authentication response to AP1, indicating acceptance or rejection (this message contains several pieces of security-related information, including the session key and WEP or WPA key). Upon receiving a positive response from AP2, AP1 sends a handoff request to the STA that includes information about AP2. At the

same time, AP1 sends all buffered data for the STA to AP2. The STA starts the reassociation process to the new AP (AP2) by sending a reassociation request frame to AP2 and then waiting for a response. Finally, AP2 replies to the STA with a reassociation response frame and then sends all the buffered data previously sent by AP1.

In the proposed scheme, the handoff process is controlled by the network instead of by the STAs. The APs not only compare the signal strength but also analyze the traffic load conditions of neighboring APs. Table 3-1 presents the handoff algorithm and its associated terminology. Algorithm 1 is used by an AP to analyze the data sent by neighboring APs and compare it with its own data. The data on traffic load at every AP allows us to balance the load among neighbor APs by controlling the number of STAs and/or the total throughput for the MAC layer in each cell. This assures a higher quality of service (QoS) for real-time services.

Table 3-1. Data Analysis and Comparison

ALGORITHM 1
1: ***RSSc***: Signal strength measured by current AP ***RSSn***: Signal strength measured by neighbor AP ***RSSth1***: Signal strength threshold for current AP ***RSSth2***: Signal strength threshold for neighbor AP ***Trc***: Current AP's traffic load ***Trn***: Neighbor AP's traffic load ***Trd***: Traffic load difference ***H***: Hysteresis 2: ***Trd = Trc - Trn*** 3: **(RSSc, RSSn, Trd) = Fuzzy (Low, Middle, High)** 4: **IF** "Result from Fuzzy Logic Rule" = "Handoff", **THEN** 5: **START HANDOFF** 6: **END IF**

In algorithm 1, the average received signal strength from the STA is calculated in the current AP (RSSc) and the neighboring AP (RSSn) using the weighted average shown in Eq. 3-1. The wireless channel conditions are highly variable, especially in urban areas and high-mobility scenarios. Thus, the weighted average is intended to smooth the variable conditions of the signal strength along the time axis. At the same time, the average traffic load of the current AP (Trc) and neighboring APs (Trn) are calculated using Eq. 3-2. Table 3-2 shows an example of comparison data in AP1.

$$RSSc = \frac{\sum_{i=1}^{n} w_i Xc_i}{\sum_{i=1}^{n} w_i} \quad ; \quad RSSn = \frac{\sum_{i=1}^{n} w_i Xn_i}{\sum_{i=1}^{n} w_i} \tag{3-1}$$

$$Trc = \frac{\sum_{i=1}^{n} w_i Tc_i}{\sum_{i=1}^{n} w_i} \quad ; \quad Trn = \frac{\sum_{i=1}^{n} w_i Tn_i}{\sum_{i=1}^{n} w_i} \tag{3-2}$$

where $w_i = \frac{1+(n-i)}{n+i}$ and $n = 4$

Table 3-2. Example of Comparison Data

	FROM	*SIGNAL POWER*	*TRAFFIC LOAD*
STA_1	**AP1**	**- 87 dBm**	**42 %**
STA_1	**AP2**	**- 73 dBm**	**38 %**
STA_1	**AP3**	**- 98 dBm**	**43 %**
STA_2	**AP1**	**- 56 dBm**	**24 %**
STA_2	**AP2**	**- 98 dBm**	**42 %**
STA_2	**AP3**	**- 93 dBm**	**38 %**
.	.	.	.
.	.	.	.
STA_n	**APn**	**-x dBm**	**y %**

Consider the information of STA_1 in Table 3-2, AP2 can receive higher signal power from STA_1 than from AP1 and AP3. The traffic load in AP2 is lower than that of AP1 and AP3. Thus, it is clear that STA_1 should start handoff to AP2 as soon as possible. However, manually compare all data in the AP is impossible. Thus, a weighted combination of received signal strength (RSS) and traffic load (Tr) based on generic fuzzy logic [13] [44] is used to compare the capabilities of current and neighbor APs[1]. This technique gives us a practical way to compare two APs taking into account both the signal strength and the traffic load conditions. A fuzzy logic rule base, shown in Table 3-3, is created based on the known sensitivity of handoff algorithm parameters: RSSc, RSSn, and traffic load difference (Trd = Trc – Trn). Each of the input fuzzy variables is assigned to one of three fuzzy sets: high, medium, or low (for details, see Appendix A). To understand how to use this fuzzy logic rule base, assume the RSS from the STA is lower than the threshold in the current AP (i.e. RSSc is low) and higher than the threshold in a neighbor AP (i.e. RSSn is high), and traffic load difference (Trd = Trc – Trn) is nearly same or positive, then the handoff should be encouraged as much as possible (rules 31 through 34). Consider that the received signal strength from the STA is higher than the threshold in the current AP (RSSc is middle or high). The handoff decision is also based on other input parameters. For example, considering rule 15, if RSSc is high, RSSn is low, and Trd is negative large, then handoff is discouraged as much as possible.

[1] A more complicated technique should be considered in future works to improve the performance of the system, for example, nonlinear combination with neural networks and fuzzy logic [36]

Table 3-3. Fuzzy Logic Rule Base

Rule No.	RSSc	RSSn	[Trc-Trn]	**Decision**
1	*High*	*High*	*+ Large*	***Handoff***
2	*High*	*High*	*+ Middle*	***Handoff***
3	*High*	*High*	*Nearly Same*	**-**
4	*High*	*High*	*- Middle*	**-**
5	*High*	*High*	*- Large*	**-**
6	*High*	*Middle*	*+ Large*	***Handoff***
7	*High*	*Middle*	*+ Middle*	**-**
8	*High*	*Middle*	*Nearly Same*	**-**
9	*High*	*Middle*	*- Middle*	**-**
10	*High*	*Middle*	*- Large*	**-**
11	*High*	*Low*	*+ Large*	***Handoff***
12	*High*	*Low*	*+ Middle*	**-**
13	*High*	*Low*	*Nearly Same*	**-**
14	*High*	*Low*	*- Middle*	**-**
15	*High*	*Low*	*- Large*	**-**
16	*Middle*	*High*	*+ Large*	***Handoff***
17	*Middle*	*High*	*+ Middle*	***Handoff***
18	*Middle*	*High*	*Nearly Same*	**-**
19	*Middle*	*High*	*- Middle*	**-**
20	*Middle*	*High*	*- Large*	**-**
21	*Middle*	*Middle*	*+ Large*	***Handoff***
22	*Middle*	*Middle*	*+ Middle*	***Handoff***
23	*Middle*	*Middle*	*Nearly Same*	**-**
24	*Middle*	*Middle*	*- Middle*	**-**
25	*Middle*	*Middle*	*- Large*	**-**
26	*Middle*	*Low*	*+ Large*	***Handoff***
27	*Middle*	*Low*	*+ Middle*	**-**
28	*Middle*	*Low*	*Nearly Same*	**-**

29	*Middle*	*Low*	*- Middle*	***-***
30	*Middle*	*Low*	*- Large*	***-***
31	*Low*	*High*	*+ Large*	***Handoff***
32	*Low*	*High*	*+ Middle*	***Handoff***
33	*Low*	*High*	*Nearly Same*	***Handoff***
34	*Low*	*High*	*- Middle*	***Handoff***
35	*Low*	*High*	*- Large*	***-***
36	*Low*	*Middle*	*+ Large*	***Handoff***
37	*Low*	*Middle*	*+ Middle*	***Handoff***
38	*Low*	*Middle*	*Nearly Same*	***Handoff***
39	*Low*	*Middle*	*- Middle*	***-***
40	*Low*	*Middle*	*- Large*	***-***
41	*Low*	*Low*	*+ Large*	***Handoff***
42	*Low*	*Low*	*+ Middle*	***Handoff***
43	*Low*	*Low*	*Nearly Same*	***-***
44	*Low*	*Low*	*- Middle*	***-***
45	*Low*	*Low*	*- Large*	***-***

3.3.1 Advantage

A novel wireless network architecture can reduce the latency time in the handoff process to support real-time services in a wireless network such as Voice-over-IP (VoIP), e-conference, and e-learning. In the proposed scheme, the STA can switch to a new AP with higher quality by comparing the signal strength and traffic load conditions.

The handoff process is controlled by the AP, which makes it easy to manage the wireless network in terms of traffic load sharing (traffic load balance among neighbor APs). This feature can reduce the number of packets dropped due to

traffic overload in one cell, thereby improving the performance of the overall network.

The proposed wireless network is compatible with all commercial wireless LAN cards. Customers might need to update the firmware, which can be generally downloaded from the vendor's website without adding or changing any hardware component. This is an advantage compared to other related works [38] [39] that require changes in wireless LAN cards.

3.3.2 Disadvantage

The disadvantage of the proposed handoff scheme is that every AP in the system requires at least two radio interfaces, resulting in inter-channel interference and more expensive costs. The effect of the reception of the first radio channel's transmitting signal by the second radio channel's receiver is a huge concern for engineers. There are two types of interference, one is the signal from 802.11 radios generates side band emissions, energy outside of its approved spectrum band. These emissions affect the nearby channels and are restricted as low as possible, but the careful hardware design is required in order to prevent the degradation of Desired signal to Undesired signal Ratio (D/U). Another interference is that one radio receiving the far terminals' signals can also receive the adjacent radio channel's main transmitting signal even though the transmitting signal is weakened by the attenuation of Band-Pass Filter (BPF). In order to prevent this interference, sophisticated BPF design is required to realize sharp cutoff filtering and very large attenuation at the adjacent radio frequency band. These two types of interference are illustrated in Figure 3-4.

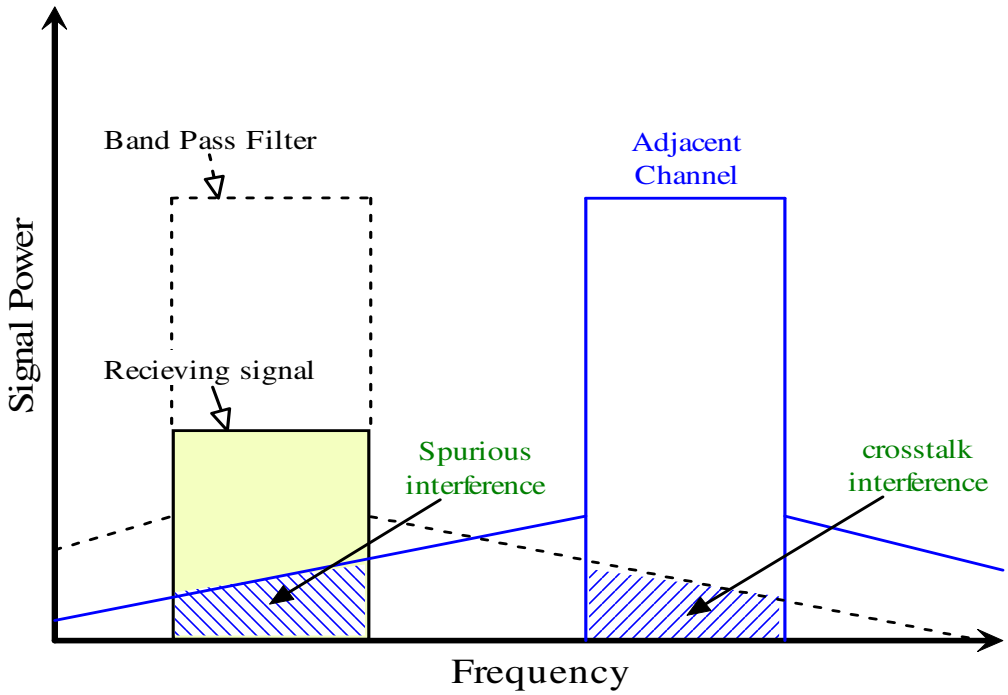

Figure 3-4. Interference from adjacent channel receiver.

The ability of an RF system to reject interference emanating from adjacent channels is highly dependent on the transceiver architecture. In WLAN systems, the dual conversion or super heterodyne (super-het) [45] [46] [47] and direct conversion (DC) [48] architectures are the most prevalent. Van Erven [49] introduced a dual-band WLAN AP using super-het (see Fig. 3-5). This transceiver uses an RF block to convert an incoming signal to an IF where image suppression and channel selection are performed with a narrow channel-select filter to reduce the transmit noise leakage. Moreover, additional external filtering, such as a SAW or ceramic filters, is applied to reduce transmitting signal's side band emissions in order to allow the two radios to work simultaneously, uncoordinated in the same band. However, this comes at the expense of more complexity and costs.

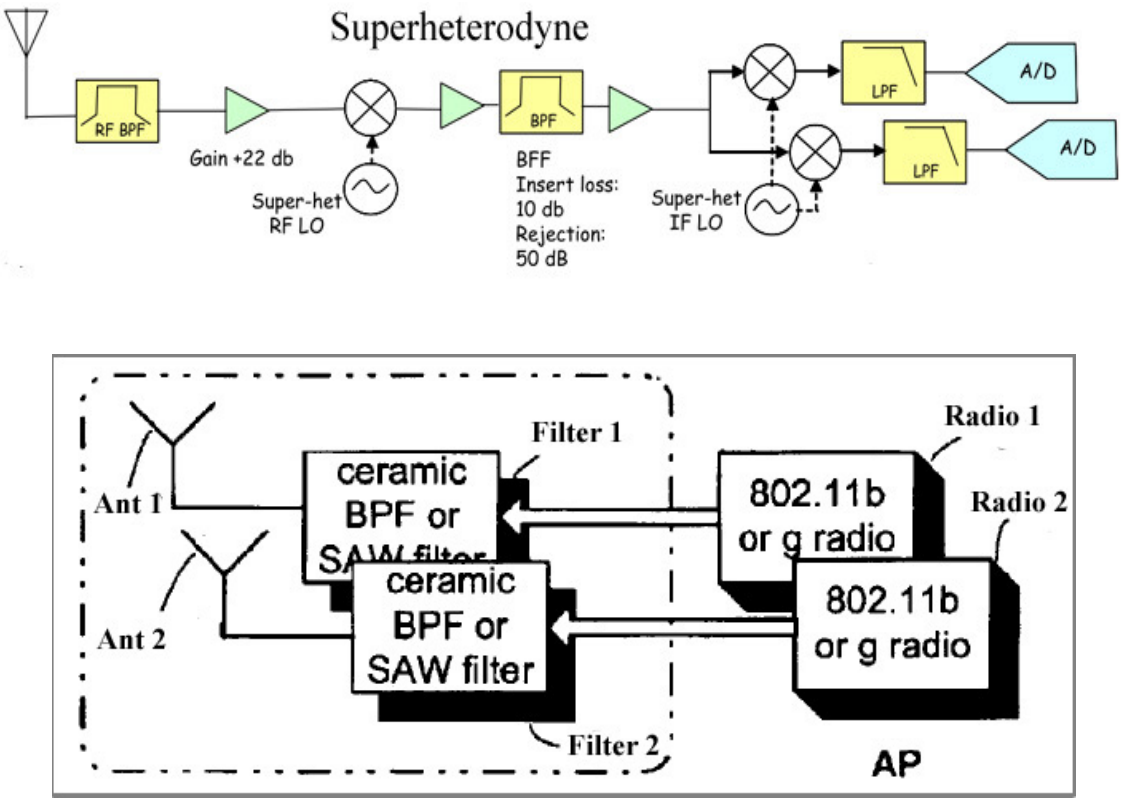

Figure 3-5. Dual Radio Block Diagram.

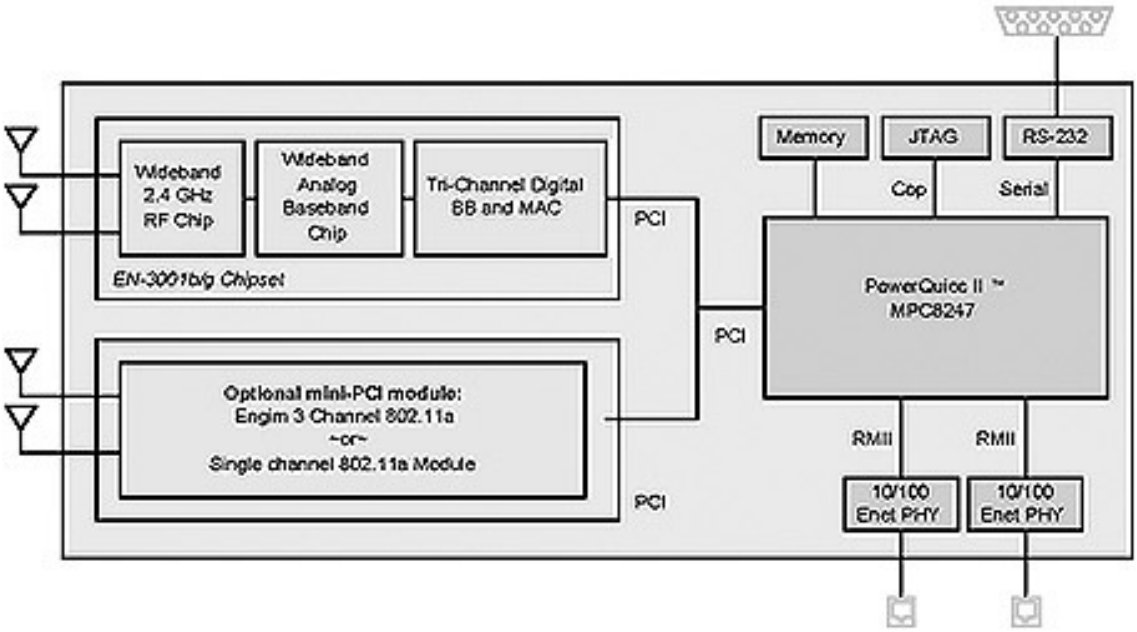

Figure 3-6. Dual band AP using EN-3001-Chipset.

Markus Zannoth [50] introduced a dual-band WLAN AP using direct conversion (DC) architecture [48]. DC architecture enables a low cost dual band

capability for the worldwide radio due to its lack of spurious problems and its low part count. Multiple commercial vendors are developing multi-band chipsets, e.g., EN-3001 intelligent wideband WLAN chipset for 802.11 networks (see Fig. 3-6) [51]. This chipset uses DC architecture to enable simultaneous communication across multiple channels of 802.11b/g and multiple channels of 802.11a.

Two radio interface increases the expense of the AP. However, this is not a large problem compared to other approaches (e.g. [38] [39]) that require changes in current wireless LAN cards, since it is always more viable to introduce changes on the network operator side.

3.4 Performance Evaluation

In this section, the performance of the proposed scheme is evaluated and compared with the conventional scheme and the multiple-radio scheme [37]. Five simulation scenarios were built to observe the throughput as well as the end-to-end delay time of the STA (Fig. 3-7) and the traffic load of the network (Figs. 3-11, 3-16, 3-21, and 3-26). The OPNET Modeler program [52] is used to implement the simulations and compare the results.

VoIP traffic based on the G.711 codec standard [53] is used to generate a VoIP packet every 20ms with 160-byte data, 12-byte RTP header, 8-byte UDP header, and 20-byte IP header. The VoIP packet's total size is 200 bytes, and the data rate is 80 kbps at the IEEE 802.11 MAC layer per packet.

The proposed scheme is simulated and compared with the conventional and multiple-radio schemes in every simulation scenarios in order to evaluate the handoff delay and the traffic load of the network. These simulations and results are explained in more detail in the following section.

3.4.1 Throughput

First, the throughput of the STA are compared using the simulation environment shown in Fig. 3-7, which consists of two APs with a cell radius of 300m and a transmission power of 200mW connected to each other via a gateway. The distance between the centers of two neighboring APs is 500m. The simulations consider a STA using real-time applications to communicate to AP1 and moving from AP1 to AP2 at a walking speed (5Km/h). In the conventional scheme, the STA initiates the search and execution phases of a handoff to AP2 whenever frame losses are detected. In the multiple-radio scheme, the STA uses the second wireless interface to scan neighbor APs, then selects and authenticates to the neighbor AP (AP2). The STA starts a handoff process when the received signal strength from AP2 is higher than the simple sum of the received signal strength from AP1 and the hysteresis. Table 3-4 lists the WLAN parameters used in this simulation.

Table 3-4. Throughput Simulation Parameters.

Number of APs	2	Cell radius	300 m
Data Type	Real-Time	Channels	1, 6
Data rate	2 Mbps	Radio Propagation	Hata Model

In the proposed scheme, the AP2 with two transceivers overhears a data frame sent by the STA and sends the corresponding in-advance information to AP1. AP1 compares this information with its own data through the fuzzy logic rule base and then orders the STA to start the handoff to AP2, which can provide better quality than AP1 in this case. The initial results from the simulations (see Fig. 3-8) show that the STA in the proposed scheme can start the handoff faster than that of the conventional scheme and nearly as fast as that of the multiple-radio scheme. Moreover, a small latency time was

associated with the throughput drop during the handoff process in the proposed scheme. In the multiple-radio scheme and the proposed scheme, there is no delay time associated with the detection and search phases; moreover, the delay time in the execution phase is reduced, because the authentication process is completed before the STA switches to AP2. The total delay time in the proposed scheme yields between 3 and 5ms, which is the same range for the multiple-radio scheme; it is between 1700 and 1900ms for the conventional scheme.

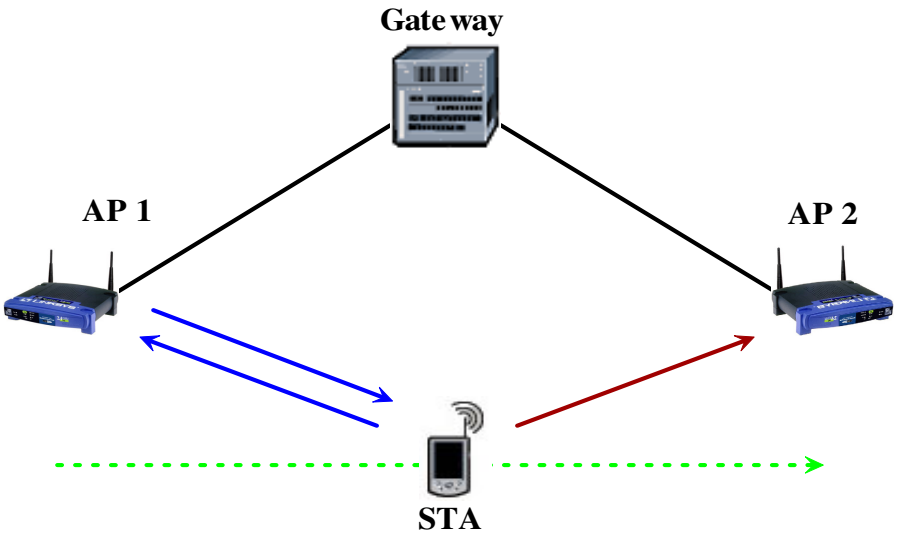

Figure 3-7. Simulation Environment 1.

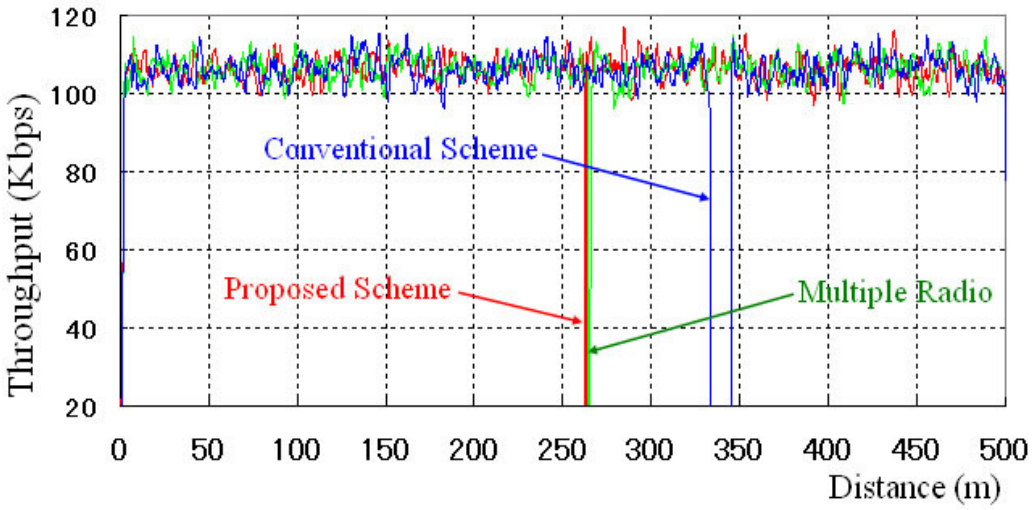

Figure 3-8. Comparison of Throughput.

3.4.2 Delay Time

Using the same simulation environment described in the previous section (see Figure 3-7), the end-to-end packet delay time between the proposed, multiple-radio, and conventional schemes are compared. The results in Fig. 3-9 show the comparison of handoff delay time, the proposed scheme can provide handoff delay time a little lower than the multiple-radio schemes (2 - 5ms). This is because in the proposed scheme, the authentication process is done before the execution phase start. Furthermore, the proposed scheme can reduce a number of handoff delay time compare to the conventional scheme (1 - 2 seconds).

In addition to finding the handoff delay time, the waiting time for each channel in the fast passive scan is analyzed to find the best value. Using the same simulation environment previously described, 20 STAs moving cross to border area and adjust the waiting time in the fast passive scan mode. The results from the simulation (see Fig. 3-10) show that 200ms should be the best choice to reduce handoff delay time for this assumption and provide handoff delay time that does not exceed 5ms.

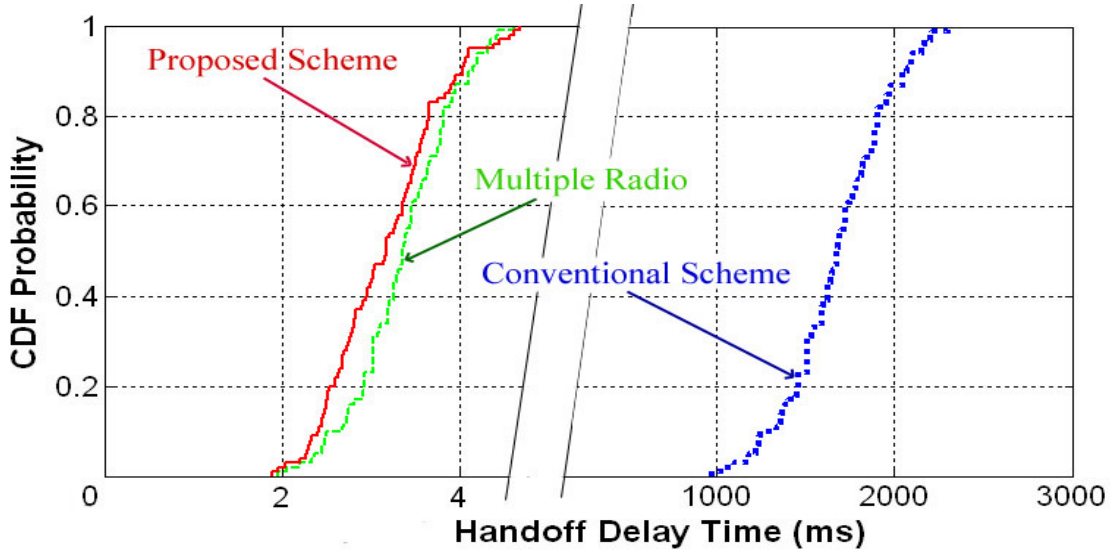

Figure 3-9. Comparison of Delay Time.

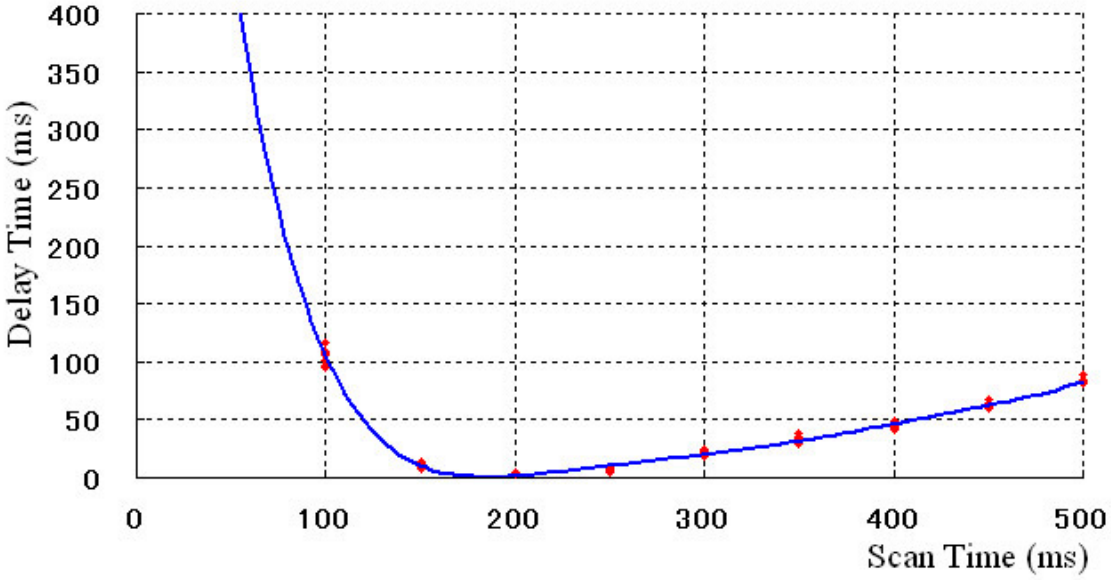

Figure 3-10. Fast Passive Scan Time.

3.4.3 Traffic Load

Traffic Load for STAs moving in a particular direction

This part evaluate the performance of the proposed handoff scheme in terms of traffic load balancing compared with the conventional and multiple-radio schemes. In the simulation environment shown in Fig. 3-11, three APs are assumed with different traffic loads: AP1 has three associated STAs; AP2 has two associated STAs; and AP3 has one associated STA. Each STA is running a real-time video application with a required data rate of 768Kbps. A STA moving at walking speed (5Km/hr) in a particular direction (see Fig. 3-11) using the conventional, multiple-radio, and proposed schemes. Table 3-5 lists the WLAN parameters used in this simulation.

In the simulation using the conventional and multiple-radio schemes, the STA starts handoff based on signal strength measured at the STA. The STA using the conventional scheme begins handoff if (and only if) there are frame losses. In the multiple-radio scheme, the STA compares the received signal strength from

the current AP and the neighbor AP and decides to start handoff if the neighbor AP can provide greater signal strength than the current AP. Using these techniques, the STA cannot measure the traffic load of the APs, since this function requests AP modification; thus, the decision to start a handoff is based only on received signal strength. The results in Figs. 3-12 and 3-13 show that the STA using the multiple-radio scheme can start the handoff process faster than the conventional scheme, and there is no data dropped during the handoff process (see Fig. 3-15).

Table 3-5. Traffic Load Simulation Parameters (1).

Number of APs	3	Moving STAs	1
Cell radius	300 m	Speed	5 Km/h
Data rate	11 Mbps	Data Type	Real-Time
Channels	1, 6, 11	Radio Propagation	Hata Model

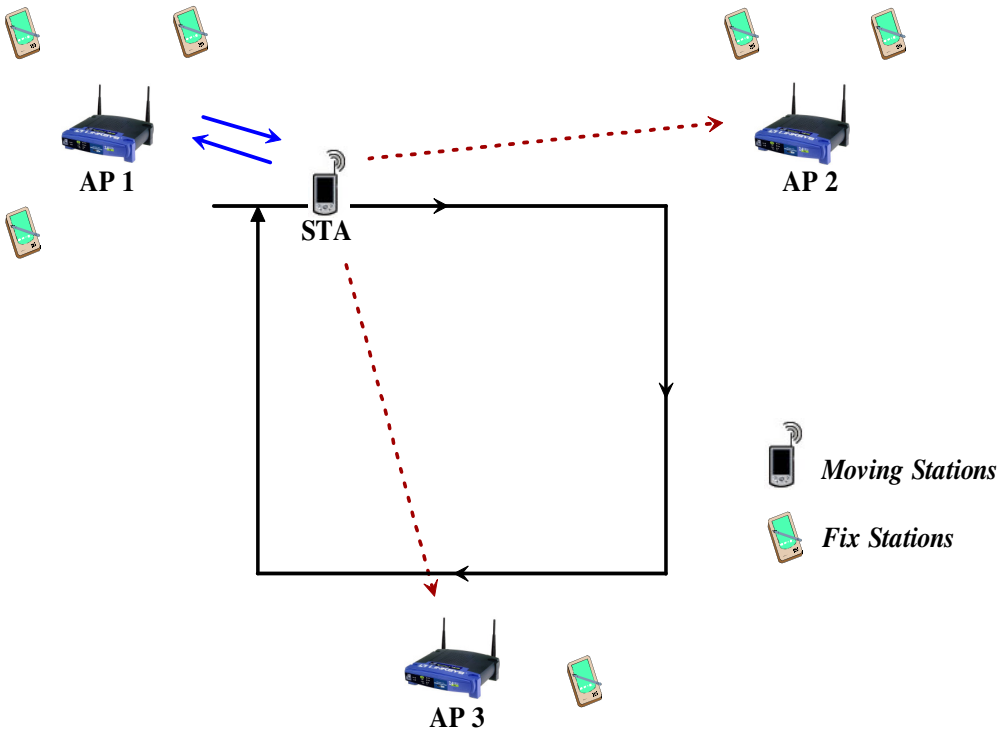

Figure 3-11. Simulation Environment 2.

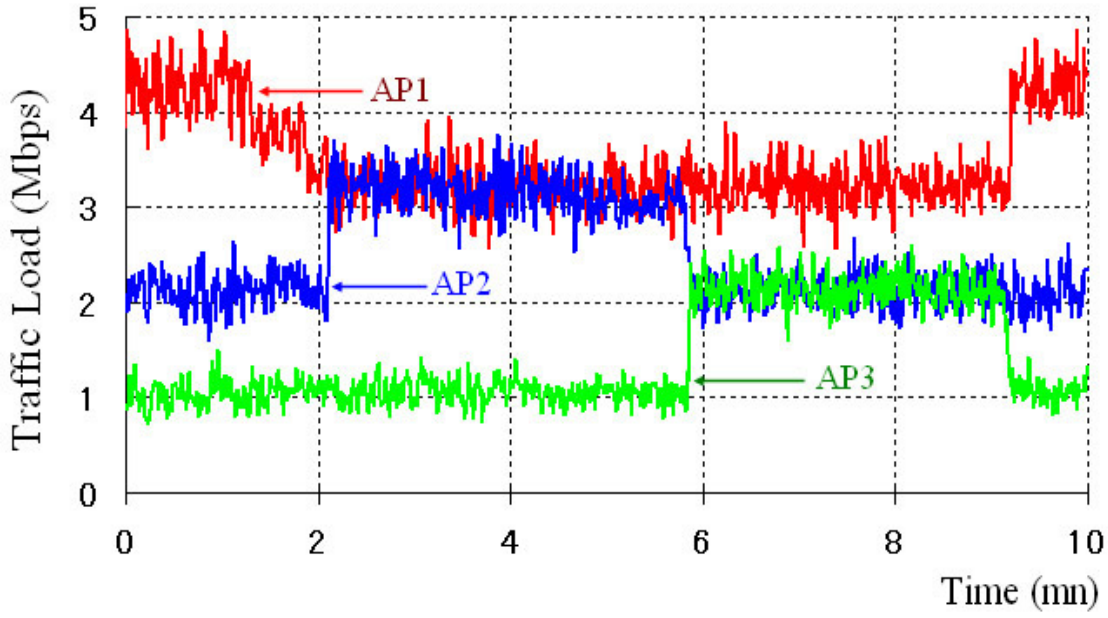

Figure 3-12. Traffic Load in AP (Conventional Scheme).

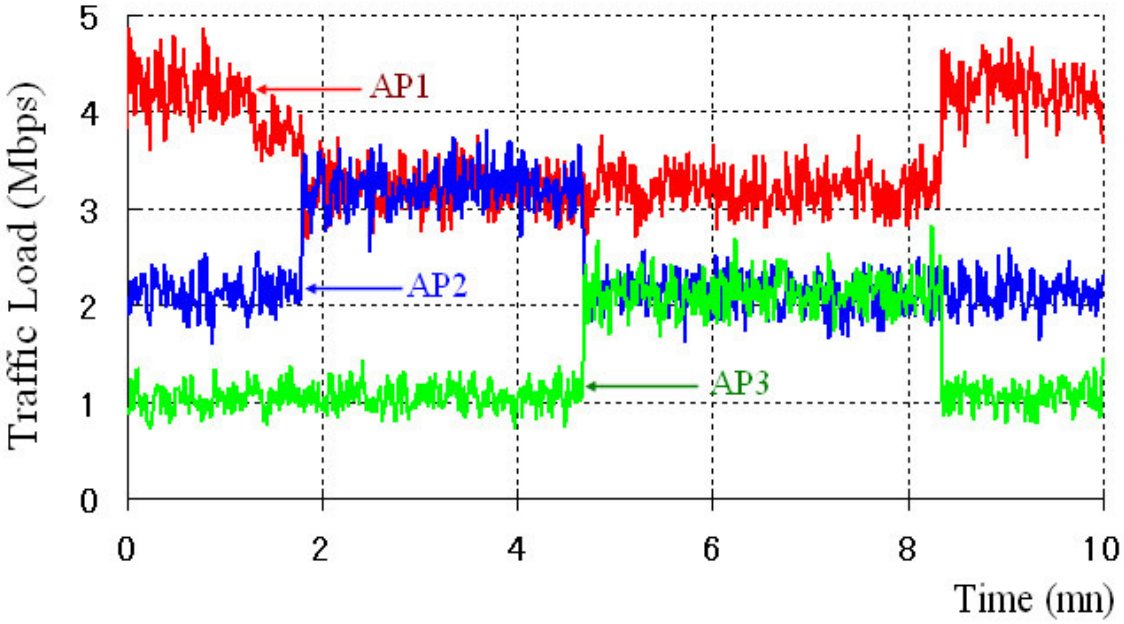

Figure 3-13. Traffic Load in AP (Multiple-Radio Scheme).

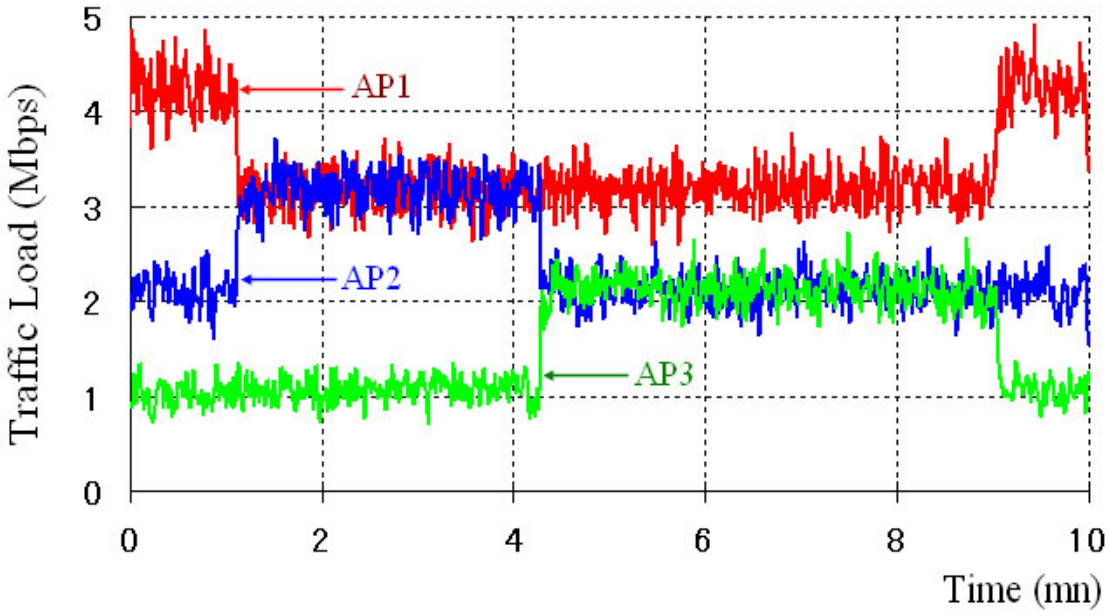

Figure 3-14. Traffic Load in AP (Proposed Scheme).

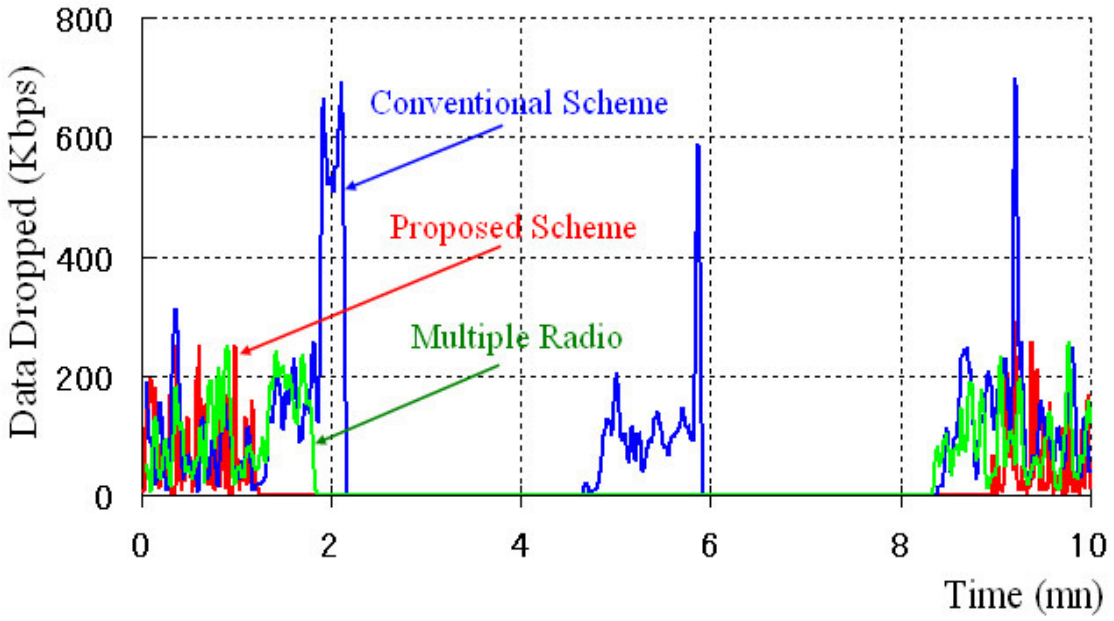

Figure 3-15. Comparison of Data Dropped.

In the simulation using the proposed scheme, the handoff process is controlled by the AP. When the STA moves to an area where AP2 can receive the data frame from the STA, AP2 analyzes and sends in-advance information to AP1. AP1 analyzes and compares this information with its own data and

then orders the STA to start the handoff to AP2; in this case, AP2 can provide higher performance than AP1 by offering a lower traffic load condition. The initial results (Fig. 3-14) show that the proposed scheme can start handoff from AP1 to AP2 faster than the conventional and multiple-radio schemes. Furthermore, the STA starts handoff from AP3 to AP1 later than the multiple-radio scheme, because AP3 finds that AP1 has a higher traffic load; in the multiple-radio scheme, the STA early starts handoff from AP3 to AP1, causing a very high traffic load and packets dropped. Thus, the proposed scheme can experience better performance in terms of traffic load balancing among APs compared with the conventional and multiple-radio schemes, because every AP controls the handoff process of its own associated STAs to balance the traffic load of the overall network.

Fig. 3-15 shows the total number of dropped packets in the network. Unlike the conventional and multiple-radio schemes, the proposed scheme can reduce the number of dropped packets resulting from traffic overload in AP1. When the traffic load increases in AP1, it compares the traffic load with its neighbor APs and eventually commands its own STA to handoff to a neighbor AP that is able to provide higher quality. In contrast, the STA in the conventional and multiple-radio schemes initiate handoff to a neighboring AP based on the received signal strength irrespective of the traffic load of its associated AP.

Traffic Load for STAs moving in a small area (Case 1)

The performance of the proposed scheme is evaluated in terms of traffic load balancing when STAs moving in a small area (Fig. 3-16). Three simulation scenarios were built (case 1, 2, and 3). In case 1, a group of ten STAs was moving in a 40m by 30m meeting room with three neighboring APs. AP1 has three associated STAs; AP2 has two associated STAs; and AP3 has one

associated STA. For this simulation scenario, the proposed scheme was compared with the conventional and related works. Table 3-6 lists the WLAN parameters used in this simulation.

Table 3-6. Traffic Load Simulation Parameters (2).

Number of APs	3	Moving STAs	10
Cell radius	300 m	Moving Area	30x40m
Data rate	11 Mbps	Data Type	Real-Time
Channels	1, 6, 11	Radio Propagation	Hata Model

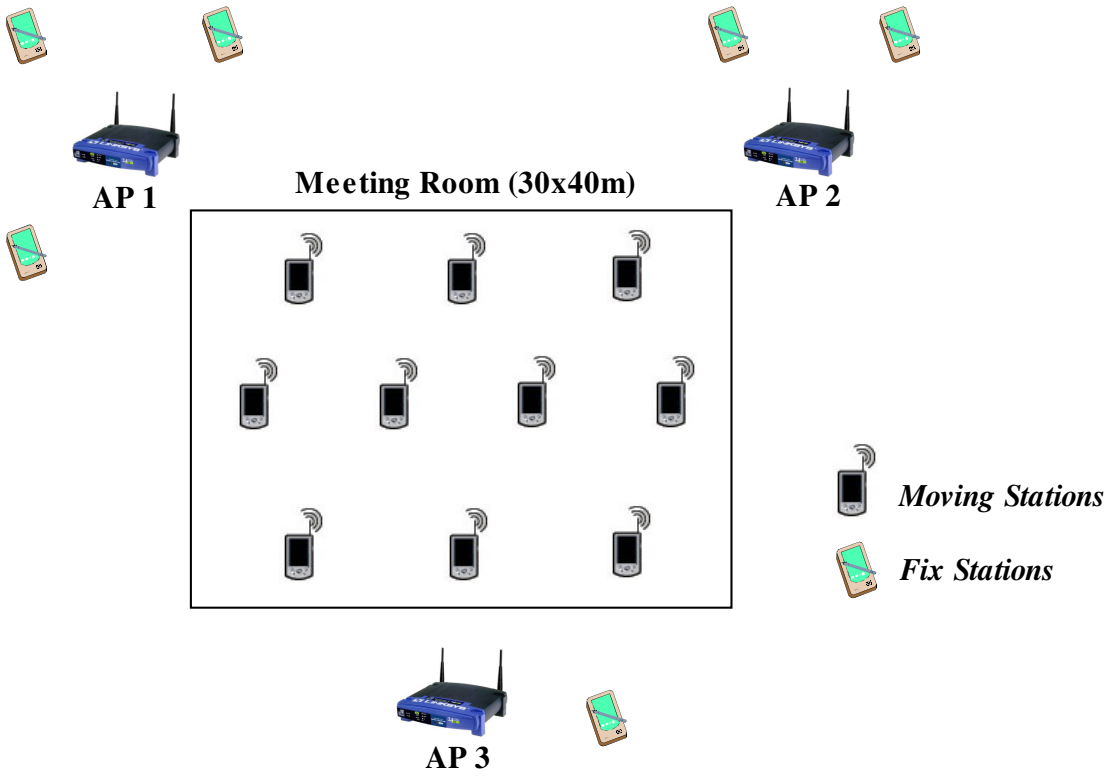

Figure 3-16. Simulation Environment 3.

The initial results from the simulations (Figs. 3-17 through 3-19) show that the proposed scheme provides a very good level of traffic load balancing among APs. Every AP controls the handoff process of its own associated STAs to balance the traffic load of the overall network, allowing traffic load sharing with its neighbor APs as shown in Figure 3-19. In contrast, as shown in Figs. 3-17 and 3-18, the conventional and multi-radio schemes do not provide any sort of load balancing, since the STA-initiated handoff mainly depends on the signal strength measured at the STA. In AP1, which presented the highest traffic load, the proposed scheme can reduce 13.97% of the traffic load compared to the conventional scheme and 7.77% compared to the related work.

Furthermore, Figure 3-20 shows the total number of dropped packets in the network. The proposed scheme can reduce the number of dropped packets resulting from traffic overload in APs. This is due to the fact that when the traffic load increases in any AP, it compares the traffic load with its neighbor APs and eventually commands its own STA to handoff to a neighbor AP that is able to provide higher quality, meaning a lower traffic load in comparison with the current AP. In contrast, the STA in the conventional and multi-radio schemes initiates a handoff to a neighboring AP based on the received signal strength, irrespective of the traffic load of its associated AP. The results from simulations show the proposed scheme can reduce the number of the total dropped packets by 93.92% compared to the conventional scheme and 84.95% compared to the related work.

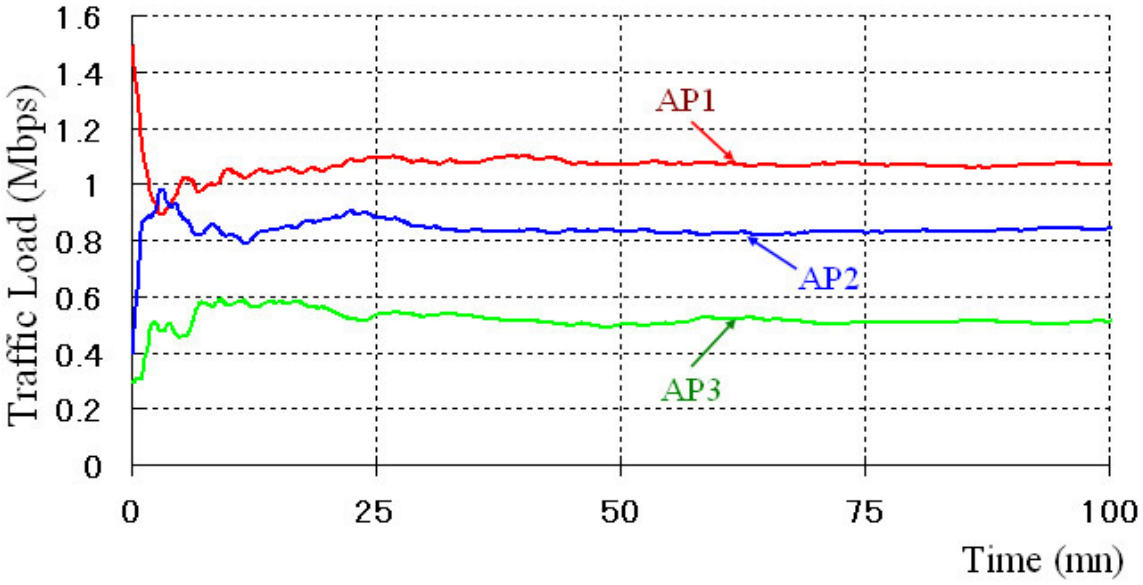

Figure 3-17. Traffic Load in AP (Conventional Scheme)

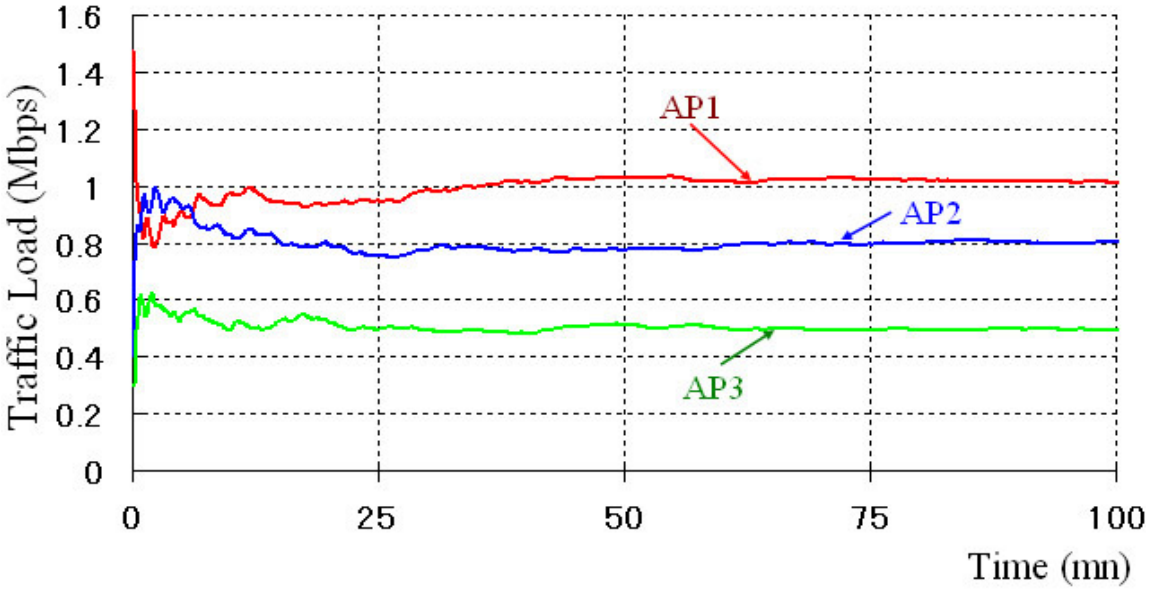

Figure 3-18. Traffic Load in AP (Multi-Radio Scheme)

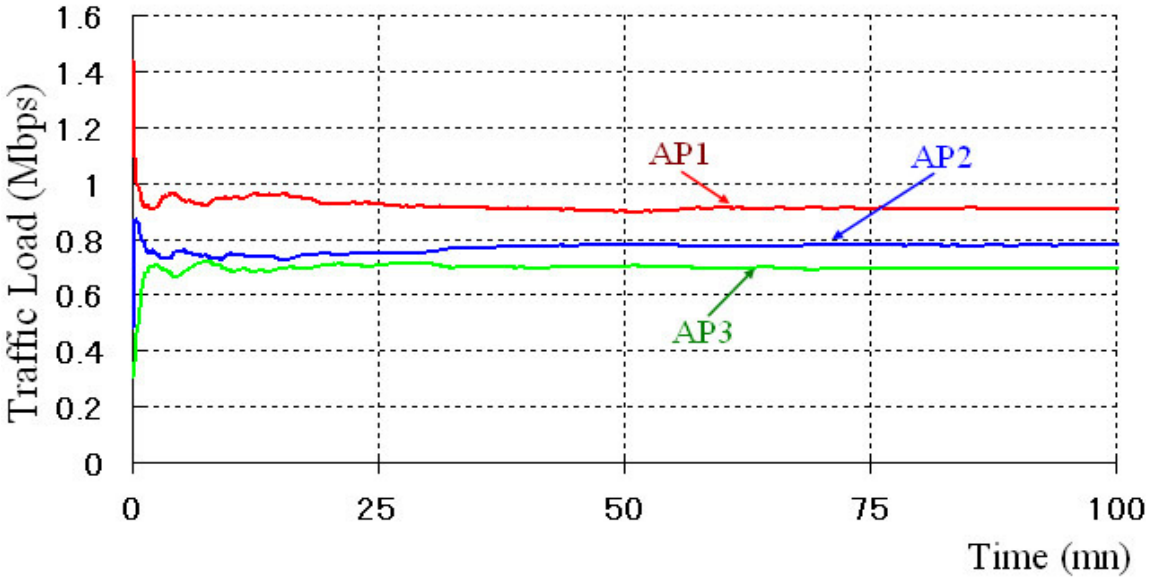

Figure 3-19. Traffic Load in AP (Proposed Scheme)

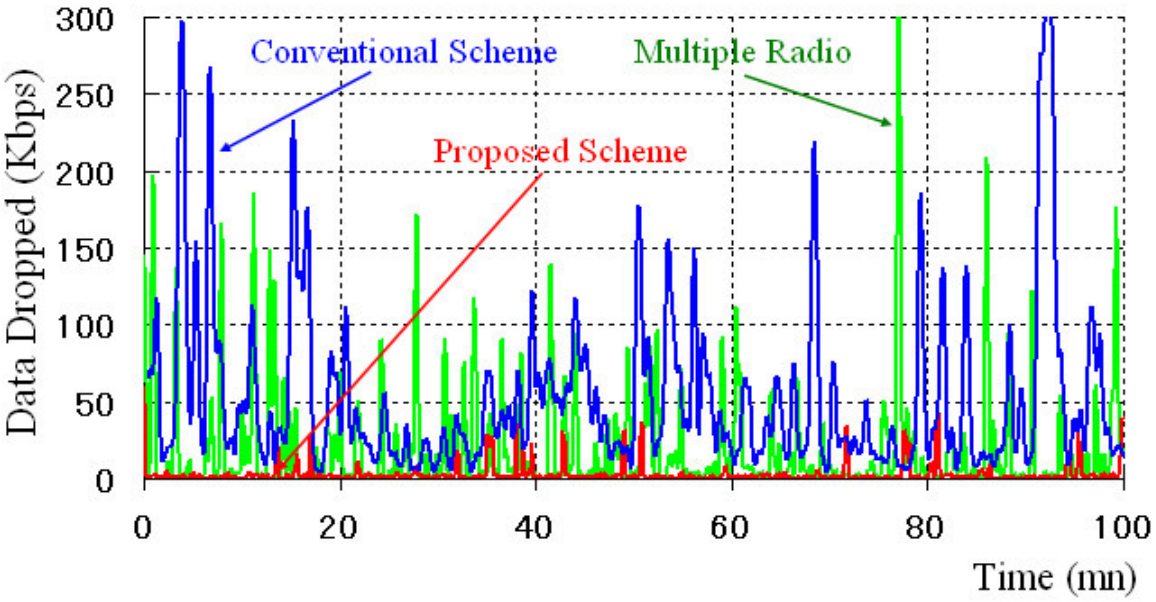

Figure 3-20. Comparison of Dropped Data

Traffic Load for STAs moving in a small area (Case 2)

In case 2, a group of ten STAs was moving in a 40m by 30m meeting room with three neighboring APs. AP1 has very high traffic load (6 associated STAs), but AP2 and AP3 has no associated STA (no traffic load). For this simulation scenario, the proposed scheme was compared with the conventional and related works.

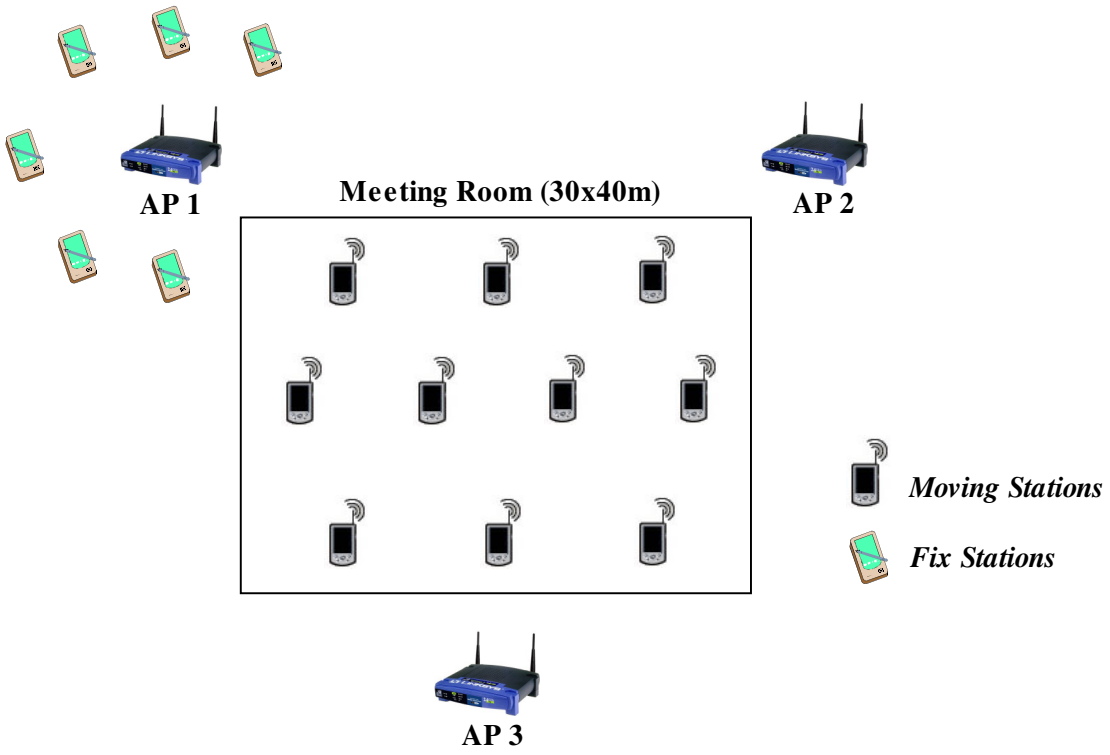

Figure 3-21. Simulation Environment 4.

The initial results from the simulations (Figs. 3-22 through 3-24) show that the proposed scheme can reduce traffic overload in highest traffic AP (AP1). In contrast, as shown in Figs. 3-22 and 3-23, the conventional and multi-radio schemes do not provide any sort of load balancing to reduce traffic load in AP1. In AP1, which presented the highest traffic load, the proposed scheme can reduce 6.31% of the traffic load compared to the conventional scheme and 5.51% compared to the related work.

Furthermore, Figure 3-25 shows the results of total number of dropped packets in the network. The proposed scheme can reduce the number of the total dropped packets by 95.66% compared to the conventional scheme and 88.33% compared to the related work.

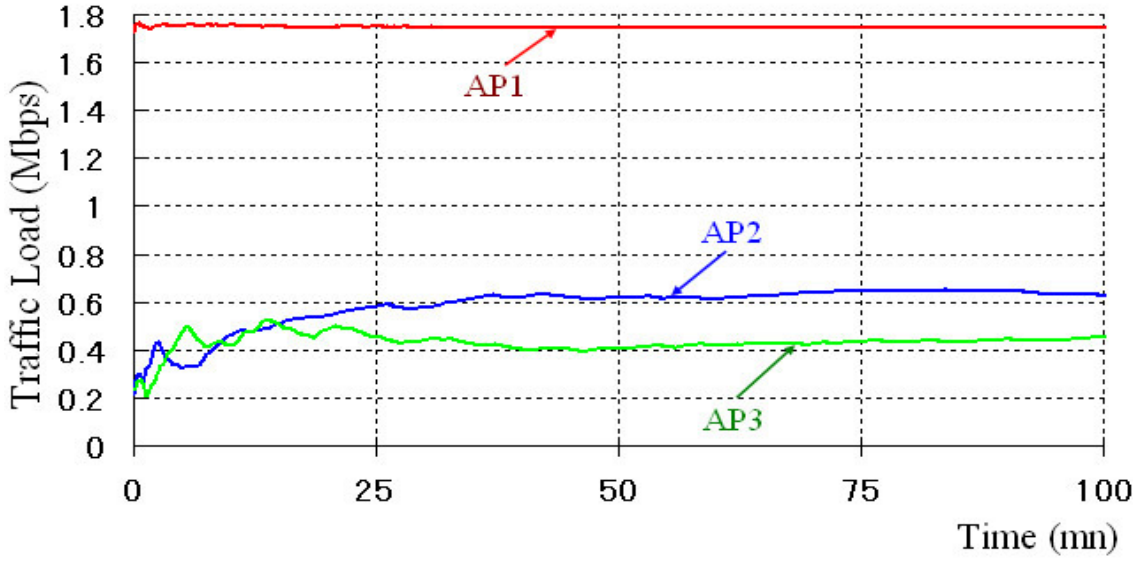

Figure 3-22. Traffic Load in AP (Conventional Scheme)

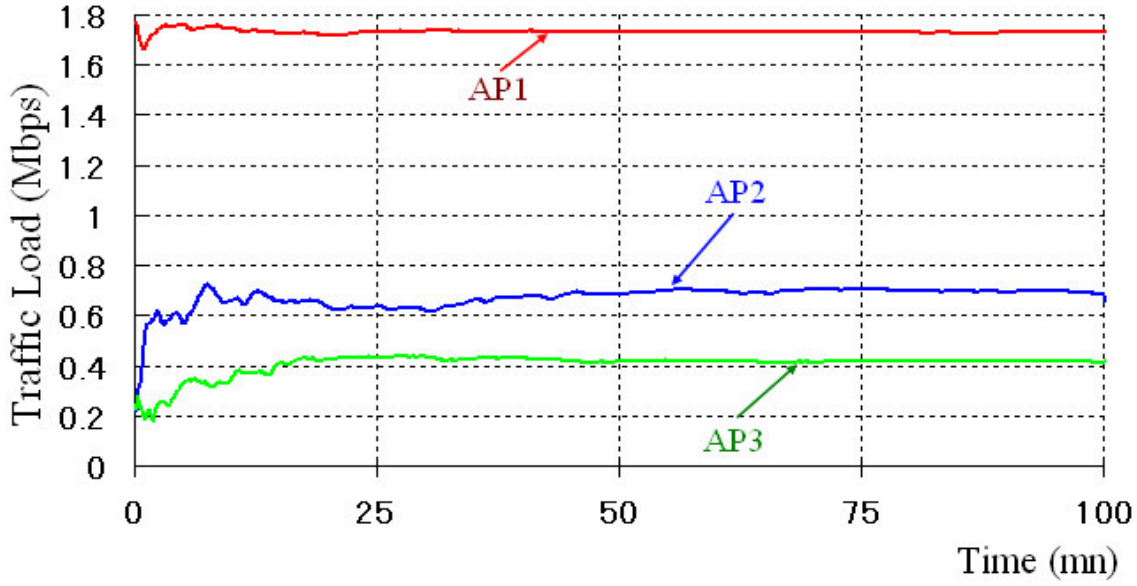

Figure 3-23. Traffic Load in AP (Multi-Radio Scheme)

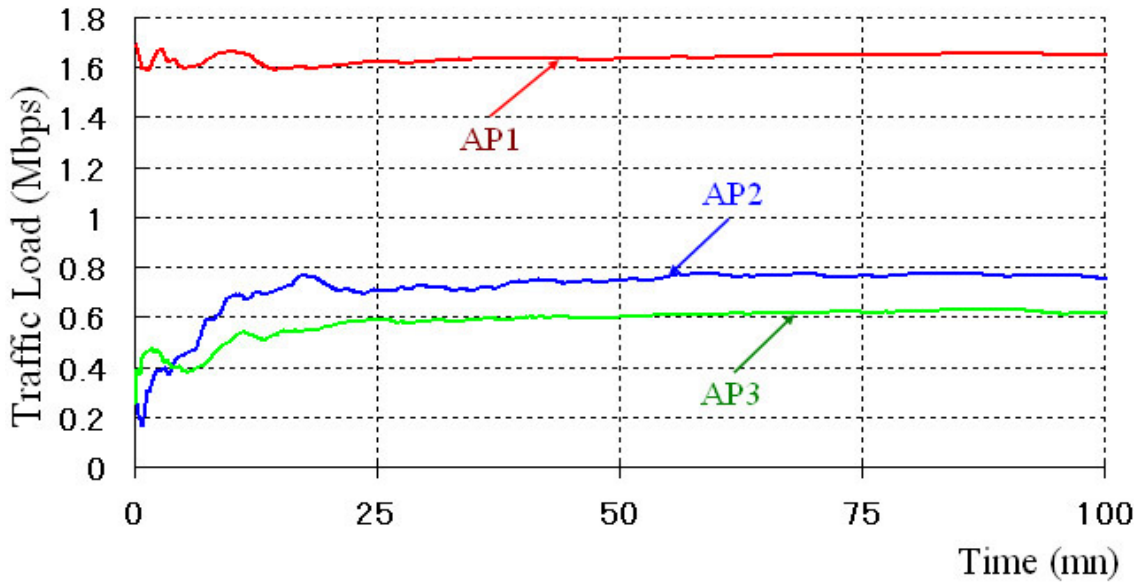

Figure 3-24. Traffic Load in AP (Proposed Scheme)

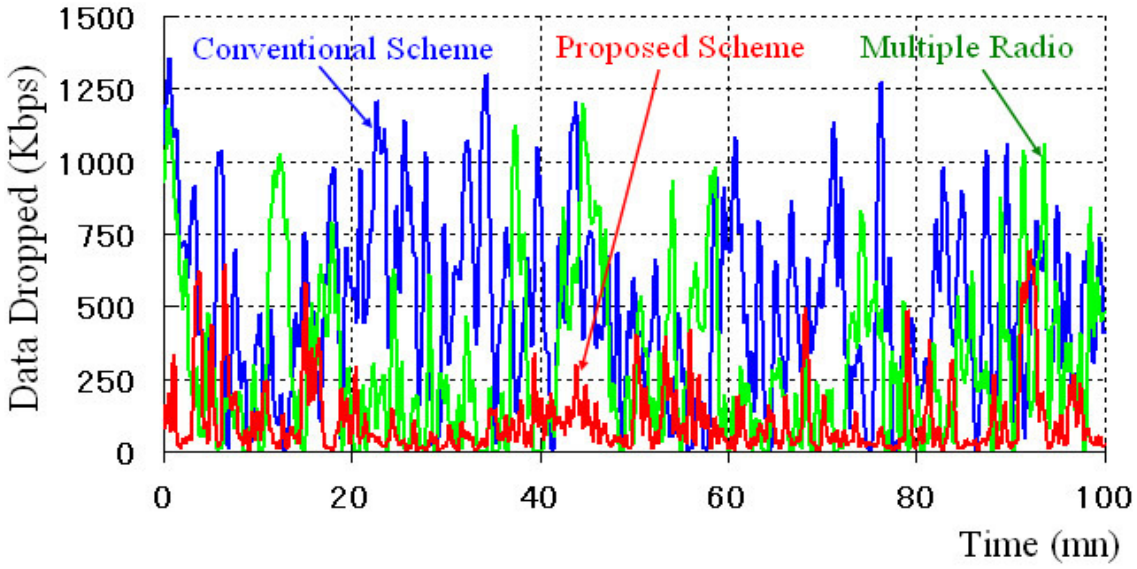

Figure 3-25. Comparison of Dropped Data

Traffic Load for STAs moving in a small area (Case 3)

In case 3, a group of ten STAs was moving in a 40m by 30m meeting room with three neighboring APs with same traffic load (AP1, AP2 and AP3 has two associated STAs). For this simulation scenario, the proposed scheme was compared with the conventional and related works.

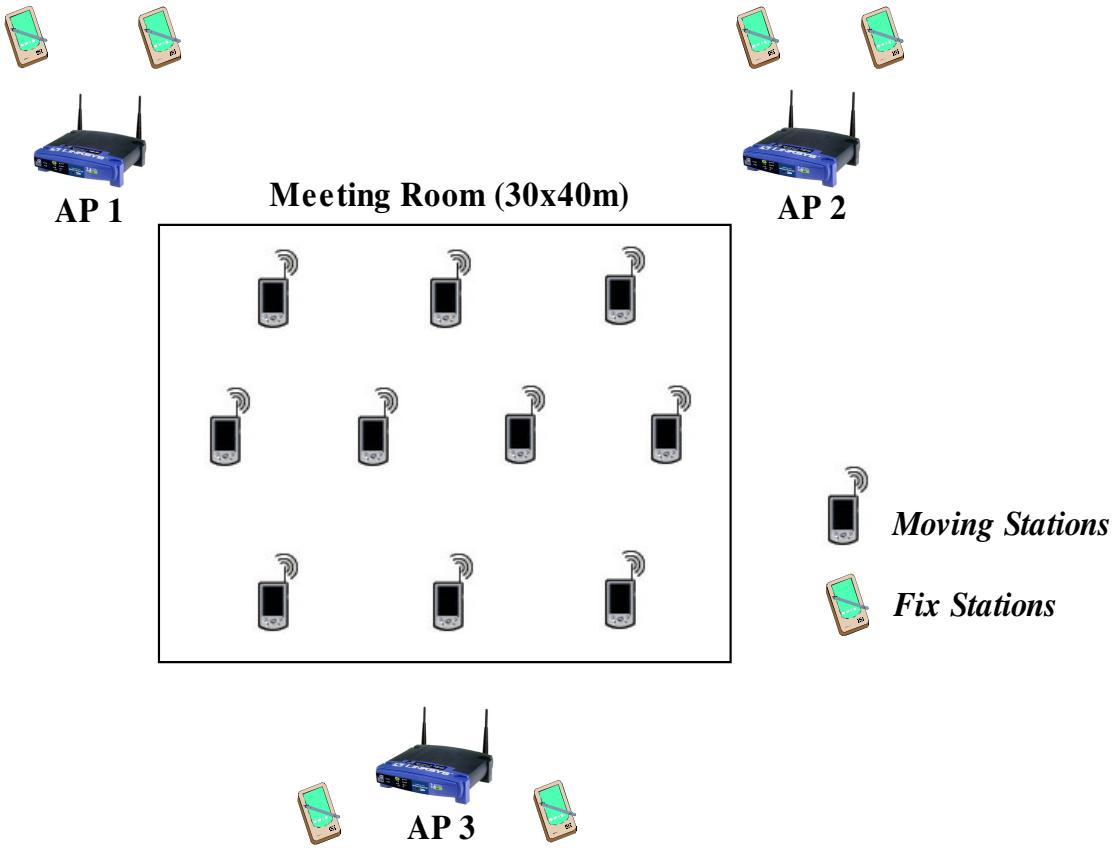

Figure 3-26. Simulation Environment 5.

The initial results from the simulations (Figs. 3-27 through 3-30) show that the proposed scheme can balance traffic load among neighbor APs (AP1, AP2, and AP3) when compare to the conventional and multi-radio schemes (Figs. 3-27 and 3-28). In AP1, the proposed scheme can reduce 3.57% of the traffic load compared to the conventional scheme and 1.06% compared to the related work.

Furthermore, Figure 3-30 shows the results of total number of dropped packets in the network. The proposed scheme can reduce the number of the total dropped packets by 78.73% compared to the conventional scheme and 73.52% compared to the related work.

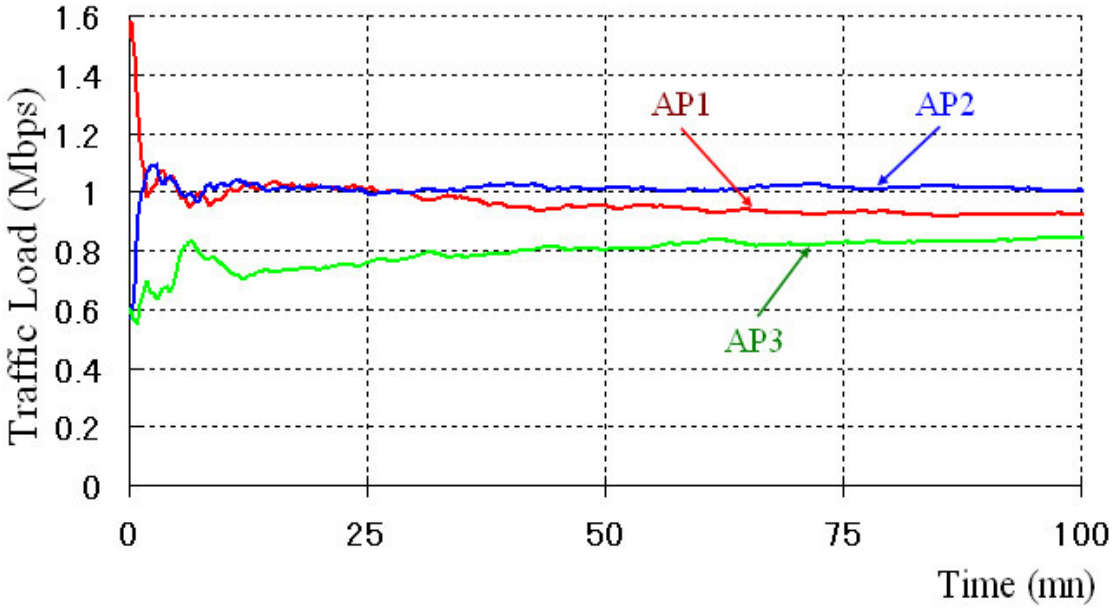

Figure 3-27. Traffic Load in AP (Conventional Scheme)

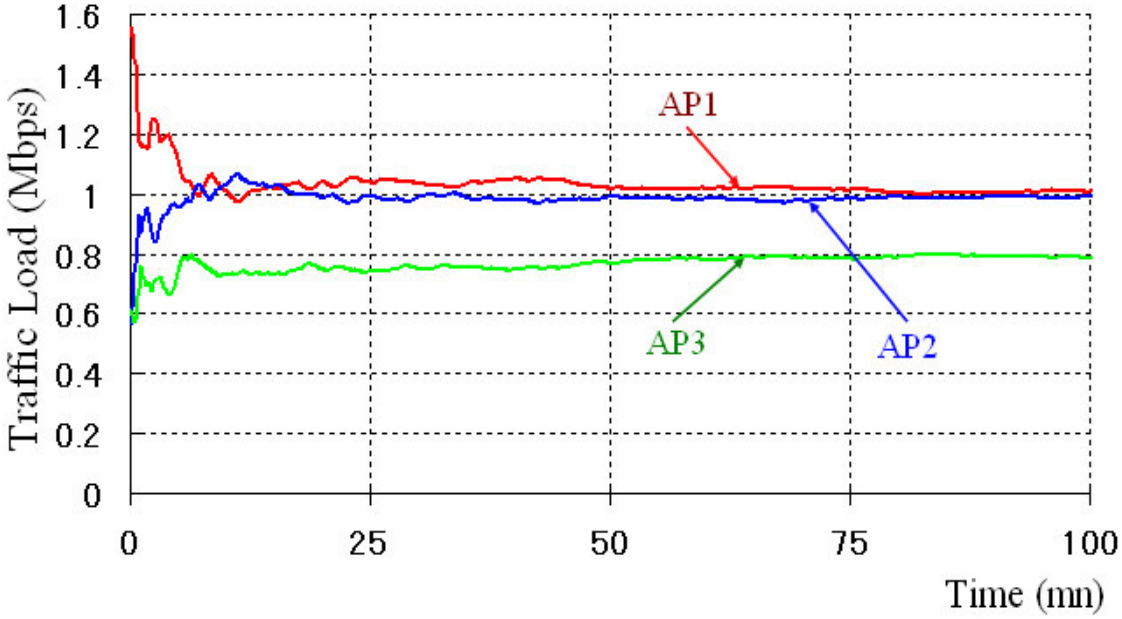

Figure 3-28. Traffic Load in AP (Multi-Radio Scheme)

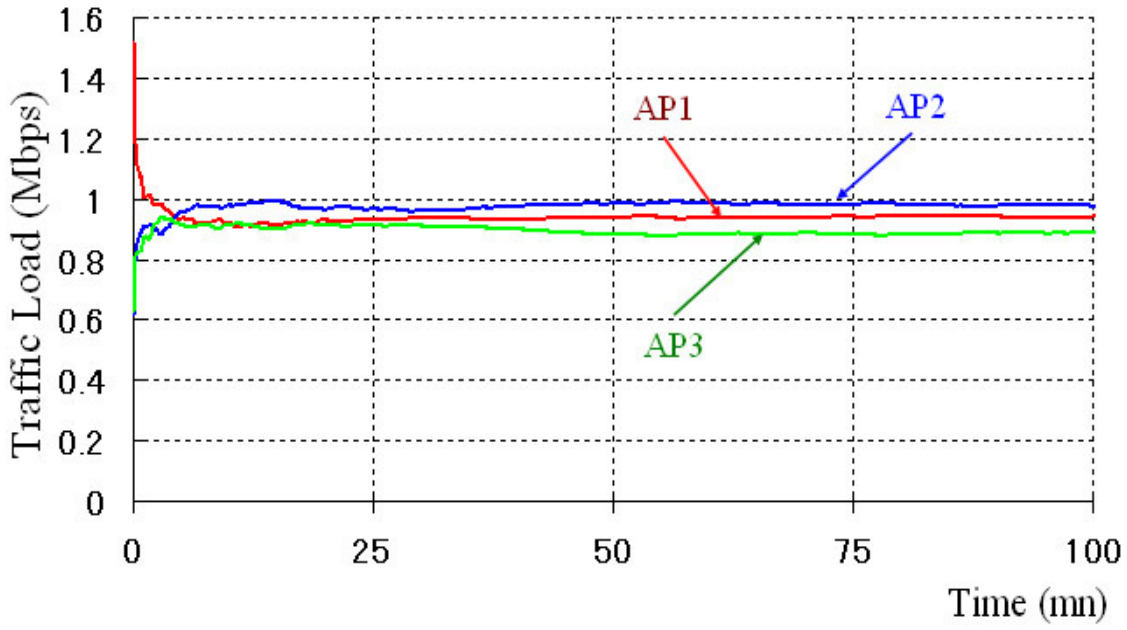

Figure 3-29. Traffic Load in AP (Proposed Scheme)

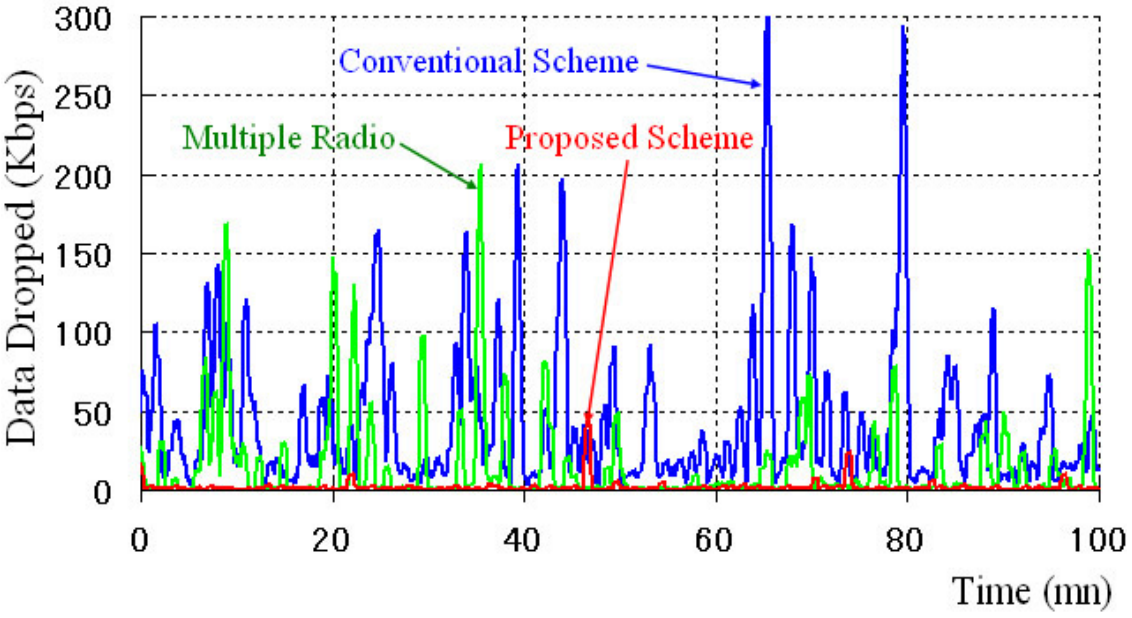

Figure 3-30. Comparison of Dropped Data

3.5 Conclusion

This chapter has proposed a novel wireless network architecture. This system largely improves the performance of wireless LANs in terms of latency time during the handoff and also provides traffic load balance among APs in the network. The STAs in the proposed scheme perform a handoff that is faster and smoother than those of the conventional and multiple-radio schemes. The handoff delay time of both the detection and search phases are omitted, and the delay time of the execution phase is largely reduced. Furthermore, as the handoff process is controlled by the AP instead of the STA, the network is able to provide traffic load balancing among neighbor APs, thus allowing the proposed scheme to reduce the number of dropped packets due to traffic overload. The simulation results show a large reduction in delay time and fair traffic load sharing among neighbor APs.

The disadvantages of the proposed method are that the APs must be equipped with two radios, and users might need to update the firmware for their wireless LAN cards. However, the seamless handoff scheme provided by the proposed mechanism largely compensates for these disadvantages by improving the support of real-time services and the distribution of traffic load inside a WLAN. Furthermore, this scheme can be enhanced in the future to support higher data rates.

Chapter 4

A Novel Wireless Positioning System for Seamless Internet Connectivity

This chapter introduces a novel wireless positioning algorithm for seamless Internet connectivity. The issues of the wireless LAN positioning system are explained in detail. The proposed system is analyzed through simulations and compared with traditional and related works.

4.1 Introduction

A relatively recent branch of mobile networking, location-based services (LBS) have expanded rapidly since mobile networks were enabled to determine the locations of mobile devices. LBS provide navigation, service information, targeted advertising, notification, and other services in which the awareness of user location is critical [2]-[3].

Some critical applications and services based on indoor localization—such as emergency rescue, fire brigade, or incident management—require an easily deployable location system that provides high positioning accuracy (i.e., about

1m of error [4]) in medium and deep indoor environments. Since global (GPS) and wide-area (cellular networks) location systems remain inefficient indoors, alternative positioning technologies are required. Obtaining the location of a user without interrupting his or her Internet connection is a key issue related to the level of user satisfaction. Thus, it would be desirable, for example, if a user could have a voice-over-IP (VoIP) conversation with a friend while running an LBS application that guides him or her to a gathering place. The research challenge is the design and implementation of an indoor location system capable of providing accurate tracking and continuous Internet connection using the existing wireless local area network (WLAN) infrastructure (i.e., taking advantage of the wide deployment of IEEE 802.11b networks).

This research proposes a novel wireless positioning system based on the WLAN infrastructure. The main motivation for this approach is twofold: to improve the accuracy of the location estimation and to avoid Internet connectivity interruption for end users. Novel wireless network architecture is proposed that effective manages networked data by means of a multi-radio AP with a fast passive scan technique [40]. The AP uses the second transceiver to scan neighbor mobile stations (STAs) in the coverage area and the information regarding the STA is sent to its associated AP, which analyzes and searches a database in order to estimate the location of the STA.

The novel wireless positioning system interfaces two location estimation methods working simultaneously to improve the position system; the fingerprinting technique is used to continually estimate the location of the STA, while the time difference of arrival (TDOA) technique is used to estimate the location of the STA when there is not enough information in the database, as is the case when the STA moves to a new area where the system has not yet run

the calibration phase. After the position of the STA has been estimated using the TDOA technique, all correlations between coordinate values of this position will be recorded in the database. Using this interface technique, the database can be generated and updated automatically. The simulations show the proposed system outperforms other related works [5] [6] in terms of accuracy without disrupting the Internet connection of end users. Using other related approaches, the STA must switch to another channel in order to measure the signal power from neighbor APs, thus disrupting the Internet connection. The proposed system does not require customers to change or to upgrade their wireless LAN devices, but users might need to update the firmware in their devices to support this novel wireless positioning system.

The rest of this chapter is organized as follows. Section 4.2 discusses related work. Section 4.3 explains the proposed system. In Section 4.4, analysis and simulation results of the proposed system are shown. The conclusions of this work are presented in Section 4.5.

4.2 Recent Work

Several techniques demonstrate how location accuracy to improve indoor positioning systems. Youssef et al. [5] show that the RADAR system, the original fingerprinting technique used to estimate the location of the STA indoors [30], can be improved using the perturbation technique (joint clustering technique) to handle the small-scale variations problem. This technique can improve the RADAR system and provide location accuracy up to 3m.

The triangulation mapping interpolation system (CMU-TMI) [54] performs a location calculation based on signal strength and access point information from the IEEE 802.11 wireless network, interpolates that data with the information in

the database, and then returns a location estimate based on this interpolation. However, power consumption increases to measure the signal strength on the client side.

The Ekahau Positioning Engine 4.0 [55], released in October 2006, also uses the IEEE 802.11 network to provide location information. It achieves an average accuracy of 1m with at least three audible channels at each location. This system requires site calibration up to 1 hour per 1,200m^2. While calibration-based efforts present good accuracy results, there is still room for performance enhancements. Due to the very dynamic nature of the RF signal, the assumption that the radio map built in the calibration phase remains consistent with the measurements performed in the real-time phase does not hold in practice; thus, at times, there is a need to rebuild the radio map. It seems more reasonable to design a fully-automatic system capable of acknowledging RSSI characteristics and variations in both spatial and time domains.

Yamasaki [56] proposes a location technology based on TDOA in March 2005. This system uses two types of access points: a master AP and a slave AP. Slave APs synchronize their clocks with that of a master AP and measure the arrival time from a mobile terminal; the master AP determines the location of the mobile terminal using the TDOA between the signal reception times at multiple slave APs. While this technique has been found to achieve good results in indoor environments, it requires specialized hardware and fine-grain time synchronization, which increases the cost of this type of solution.

Kanaan [6] proposes a closest-neighbor with TOA grid algorithm (CN-TOAG). This geolocation algorithm presents a TDOA-based position detection technique to improve location accuracy in the indoor environment by estimating the location of the user as the grid point. This technique is similar to

the previous method [56], as it needs specialized hardware and fine-grain time synchronization, which increases costs.

To date, there are various techniques to improve the accuracy of user location, but there is no positioning technology that supports seamless Internet connection to end users while providing location services. This is an important design issue, since end users do not need to stop their Internet connection before using the positioning service. This research presents a novel wireless LAN based positioning system that provides high accuracy of user locations without disrupting the Internet connection.

4.3 Theoretical Modeling [57]

This section describes the proposed positioning system that uses a novel wireless network architecture and combines a positioning technique using received power information with a technique using TDOA information collected from neighbor APs. It explains the general architecture of the proposed system, which encompasses two position detection methods working in parallel to estimate user location; detail each position detection method, including the system synchronization and the location estimation for the TDOA-based technique; and then briefly discuss the advantages and disadvantages of the proposed system.

4.3.1 System Architecture

The proposed technique is designed for two dimensions (2D); at least three access points are needed to determine each position; for three dimensions (3D), at least four access points are needed to determine the position, and the mathematical solution becomes more complicated. Most current positioning systems rely on mobile stations for processing. Mobile devices must constantly

switch channels in order to measure the signal power from neighbor APs and estimate their own position, thus disrupting the Internet connection of end users. In order to provide both continuous Internet connection and location detection services, the novel wireless network architecture that uses a multi-radio AP with two transceivers is proposed (Fig. 4-1). The novel AP contains two IEEE 802.11-compliant transceivers. The first transceiver uses a normal IEEE 802.11 infrastructure communication transceiver (exchanging frames with associated STAs), while the second transceiver is used to scan and gather information on neighbor STAs that are located in its transmission range using fast passive scan [40].

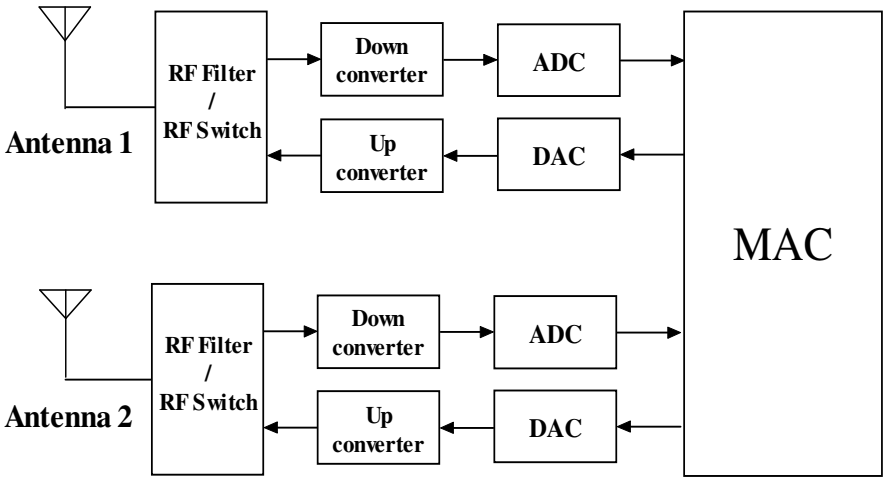

Figure 4-1. Block Diagram of the New AP Module.

Fig. 4-2 illustrates the fast passive scan that the second transceiver uses to obtain information on neighboring STAs. The AP checks the list of channels that neighbor APs are using and begins to scan from the first channel in the list. Note that the AP will not scan the channel that is currently being used by its first transceiver to prevent the interference problem. The AP uses the second transceiver to listen and wait for a data frame on the first channel; the waiting time of 200ms is used based on the assumption that the STA running real-time

services has a packet interarrival time of 50ms or less (more details in Chapter 3). After scanning the first channel, the AP switches the second transceiver to the second channel and then repeats the same procedure until all channels in the list are scanned. Based on the IEEE 802.11b standard, only three channels (Ch1, Ch6, and Ch11) that do not interference with each other are used; thus, the time period for this phase cannot exceed 600ms. The AP finally sends back the advanced information to the associated AP of the STA to report the received signal strength and time. Using the fast passive scan can reduce the time needed to gather information from neighboring STAs by scanning only two or three channels instead of all 13 channels.

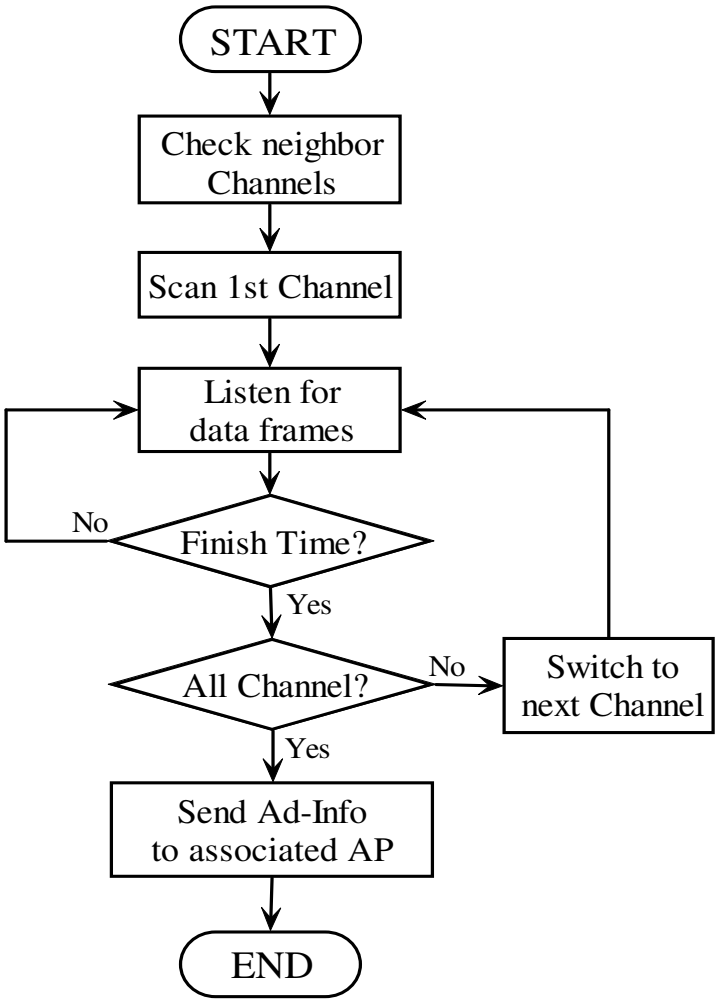

Figure 4-2. Fast Passive Scan.

The proposed system uses two position detection methods based on i) received power information and ii) signal arrival time difference. Both mechanisms work in parallel to estimate the location of the STA. The received power information method consists of two phases: calibration (data correction) and estimation. In the calibration phase (Figs. 4-3 and 4-4), the AP uses the first transceiver to communicate with the associated STA and the second transceiver to gather information on nearby STAs in its transmission range. The STA associated with AP1 moves to an area where AP2 and AP3 can also receive a packet sent by the STA.

When the STA sends the packet to AP1, AP2 can receive the same packet using the second transceiver. The information about the packet transmitted from the STAs will be sent back to its associated AP (AP1) in the form of advanced information, including the received power and reception time. At the same time, AP3 receives the same packet from the STA using its second transceiver and sends back the advanced information regarding the packet to AP1. AP1 analyzes this information and records all correlations between the coordinate values of each known position and the received powers in a database. Note that because the second transceiver is used to continuously gather information on neighbor STAs, the sample signal strength is obtained every second. The obtained samples are smoothed using a moving average filter centered at the current time step and automatically update to the database every time that the position of the STA is estimated by the TDOA-based detection method. Since the position of the STA updates often, more historical data can be used to calculate the location, thus improving the accuracy.

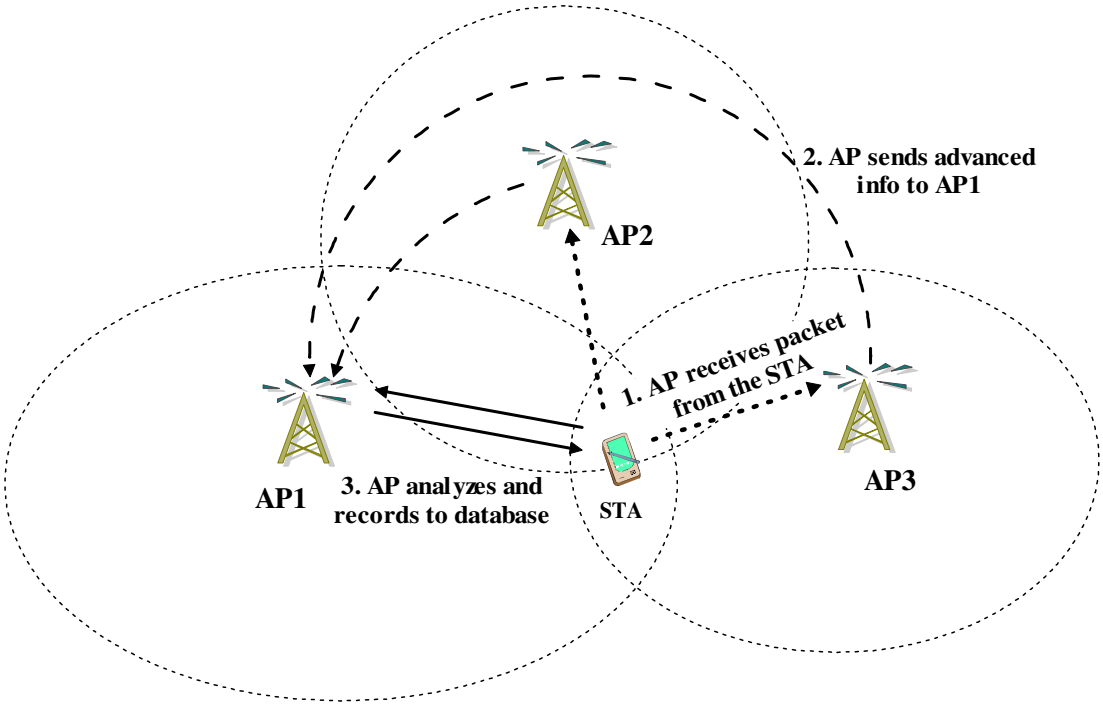

Figure 4-3. Proposed WPS using the Novel AP.

In the estimation phase (Fig. 4-4), the correlation between the information from the produced database and the average received powers measured by the AP and neighbor APs are compared using a weighted least square method [58] [59]. Coordinate values of the position with the highest correlation are chosen as the position coordinates. Because the AP uses the second transceiver continue scan on neighbor STAs, the location of the STA can be continue estimated; more history of the STA's location can improve the accuracy of the next location using Kalman's filter [60] [61]. If the difference between the corresponding data is higher than a given threshold (e.g., $1m^2$ difference error), then the system will use the TDOA technique to estimate the location of the mobile station.

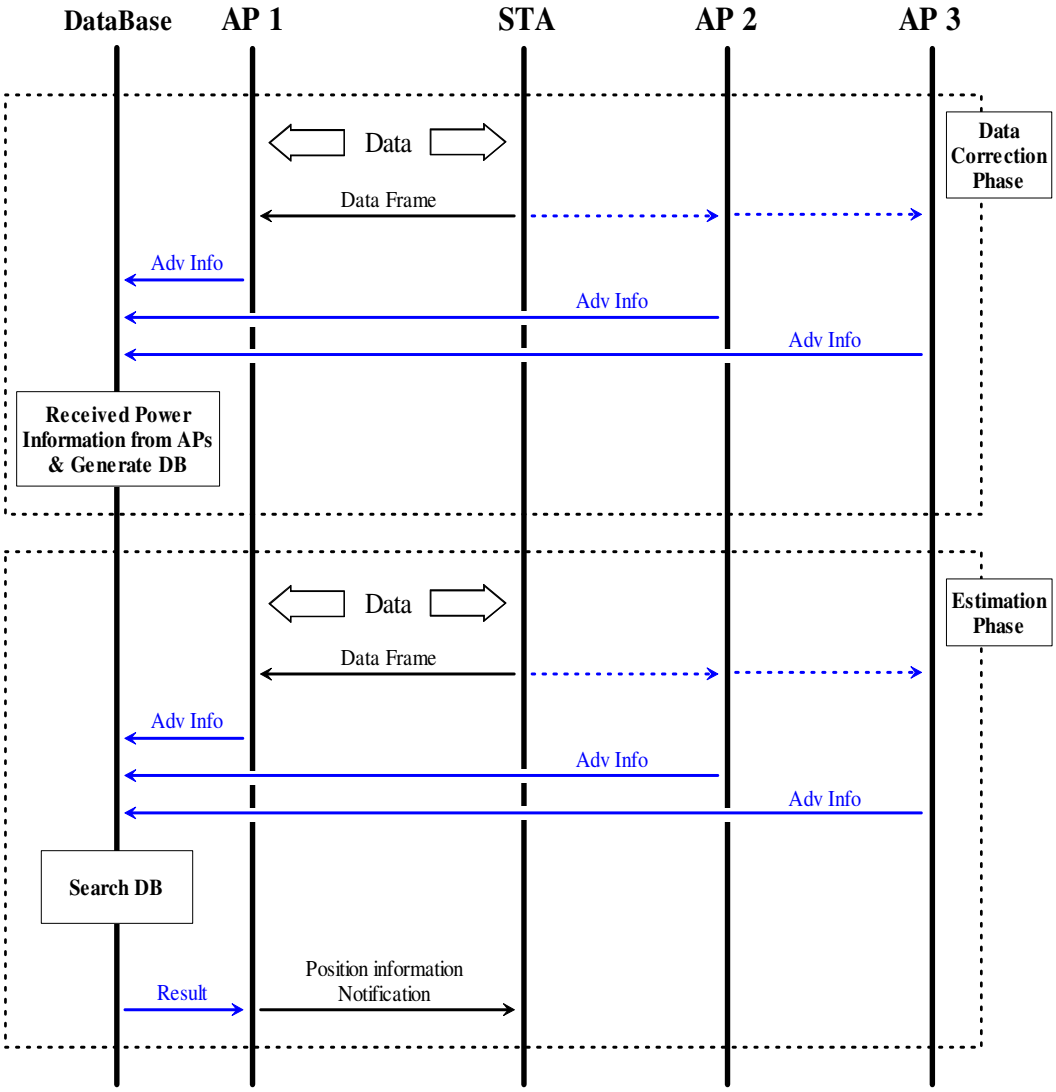

Figure 4-4. Process Flow of the Proposed System.

The position detection method using signal arrival time difference is used when there is not enough information in the database to estimate the STA's location, i.e. the difference between the corresponding data is higher than a given threshold. In this method (Fig. 4-5), the AP first sends a request message through a wired infrastructure to neighbors AP2 and AP3, which can also receive packets transmitted from the STA in order to set their second transceivers to the same channel, and then sends a positioning request signal to

the STA. When the STA receives the positioning request signal from the AP, it sends the position packet back to the AP. During this time, the neighbor AP2 and AP3 can also receive and capture the position packet from the STA. The neighbor APs complete the capture mode and send back the advanced information to the associated AP, which calculates the TDOA values based on the position packets from the STA and estimates the location of the STA using the hyperbolic positioning algorithm (see Section 4.3.3). Finally, the AP informs the STA of its location.

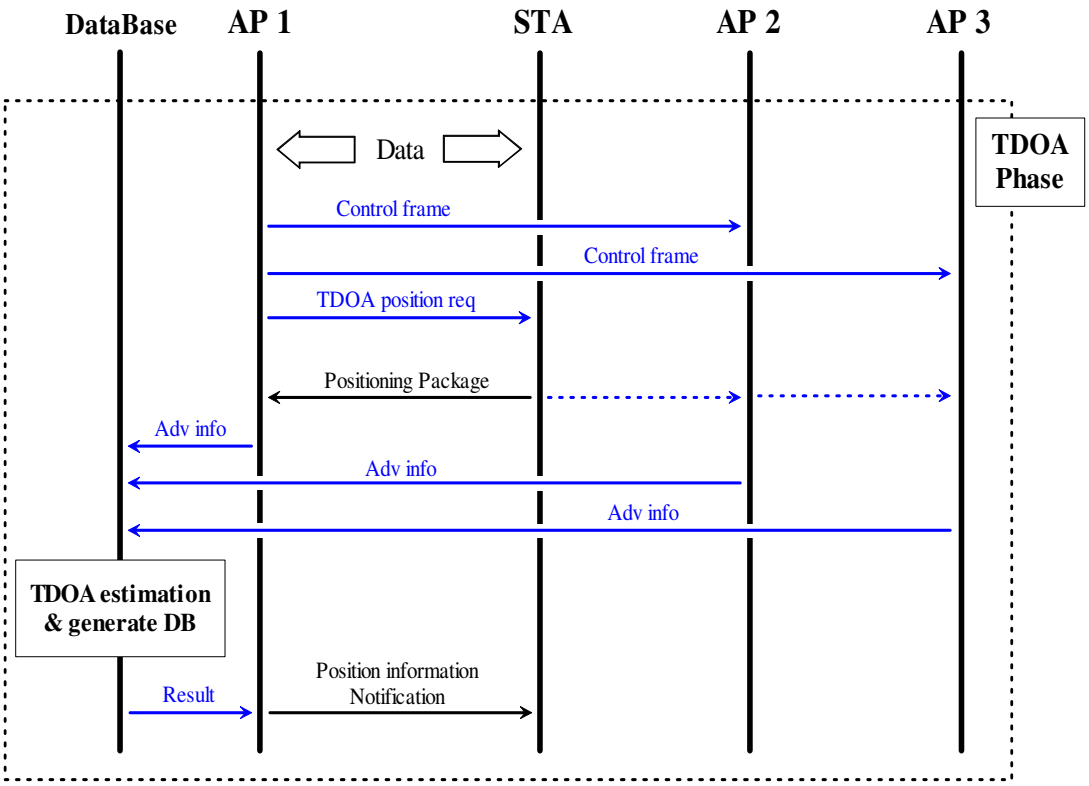

Figure 4-5. Process Flow of the Proposed System.

4.3.2 Synchronization

Using signal arrival time difference can estimate the location of the STA from the location of the APs and the TDOA measurements received at the associated AP and neighbor APs. In this detection method, synchronization of the network APs is important to determine a precise location. Since the proposed system is based on a wireless LAN infrastructure in which all APs are interconnected via a gateway, the synchronization of all APs is provided by the gateway. Using the IEEE 1588 precision time protocol in combination with hardware-based timestamping can improve the synchronization time error to less than 2.5ns [62], resulting in a positioning location error of 0.75m, which is acceptable.

4.3.3 TDOA Location Estimator

In general, the basic problem with TDOA-based techniques is how to accurately estimate the propagation delay of the radio signal arriving from the direct line-of-sight (DLOS) propagation path. Assuming that the STA moves at a low speed, the effect from the Doppler spread is negligible. Considering the system in terms of delay spread, which results from multipath signals, the performance of TDOA estimation can be improved by using super-resolution techniques [63]. The super-resolution technique allows us to separate different propagation paths in an indoor scenario to accurately estimate the TDOA from all APs. In environments with many multipath signals, however, a training phase might be required for positioning calibration.

The position detection method using signal arrival time difference employs the hyperbolic positioning algorithm [25] to calculate the location of the STA from the location of its associated AP and neighbor APs as well as the TDOA measurements. In a 2D hyperbolic positioning system (see Fig. 4-6), an STA at an unknown location (x, y) and three APs at known locations are

considered. The travel time T of pulses from the STA to each of the receiver locations is the distance from the STA to the APs divided by the pulse propagation speed (C = 299,792,458 m/s)

$$T_1 = \frac{1}{C}\sqrt{(x - x_1)^2 + (y - y_1)^2}$$
$$T_2 = \frac{1}{C}\sqrt{(x - x_2)^2 + (y - y_2)^2} \quad \textbf{(4-1)}$$
$$T_3 = \frac{1}{C}\sqrt{(x - x_3)^2 + (y - y_3)^2}$$

Let AP1 be at the coordinate system origin.

$$T_1 = \frac{1}{C}\sqrt{x^2 + y^2} \quad \textbf{(4-2)}$$

The time difference of arrival is calculated as shown in Eq. 4-3.

$$T_2 - T_1 = \frac{1}{C}\left(\sqrt{(x - x_2)^2 + (y - y_2)^2} - \sqrt{x^2 + y^2}\right)$$
$$T_3 - T_1 = \frac{1}{C}\left(\sqrt{(x - x_3)^2 + (y - y_3)^2} - \sqrt{x^2 + y^2}\right) \quad \textbf{(4-3)}$$

Knowing the time differences ($T2 - T1$) and ($T3 - T1$) from the information exchange among AP1, AP2, and AP3, the linear equations (Eq. 4-3) can be solved by using Chan's Method [64] and thus the location of the STA (x, y) is estimated.

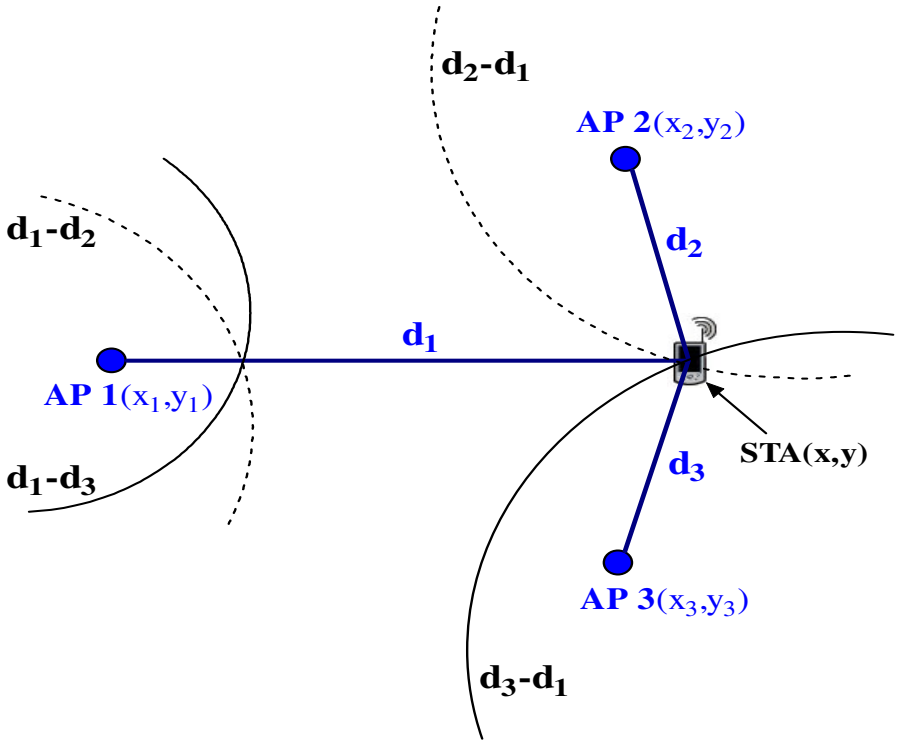

Figure 4-6. 2D Hyperbolic Positioning.

4.3.4 Kalman Filter

The Kalman filter is a set of mathematical equations that provides an efficient computational (recursive) means to estimate the state of a process, in a way that minimizes the mean of the squared error. The filter is very powerful in several aspects: it supports estimations of past, present, and even future states, and it can do so even when the precise nature of the modeled system is unknown. Thus, the Kalman filter is selected to use in the proposed system to improve the location accuracy. The Kalman filter was developed by Rudolf Kalman [60].

The state of the Kalman filter is represented by two variables:

$\hat{x}_k$, the estimate of the state at time k.

P_k , the error covariance matrix (a measure of the estimated accuracy of the state estimate).

The Kalman filter has two distinct phases: ***Predict*** and ***Correct***. (See Fig 4-7) The predict phase uses the state estimate from the previous time step to produce an estimate of the state at the current time step. In the correct phase, measurement information at the current time step is used to refine this prediction to arrive at a new, (hopefully) more accurate state estimate, again for the current time step.

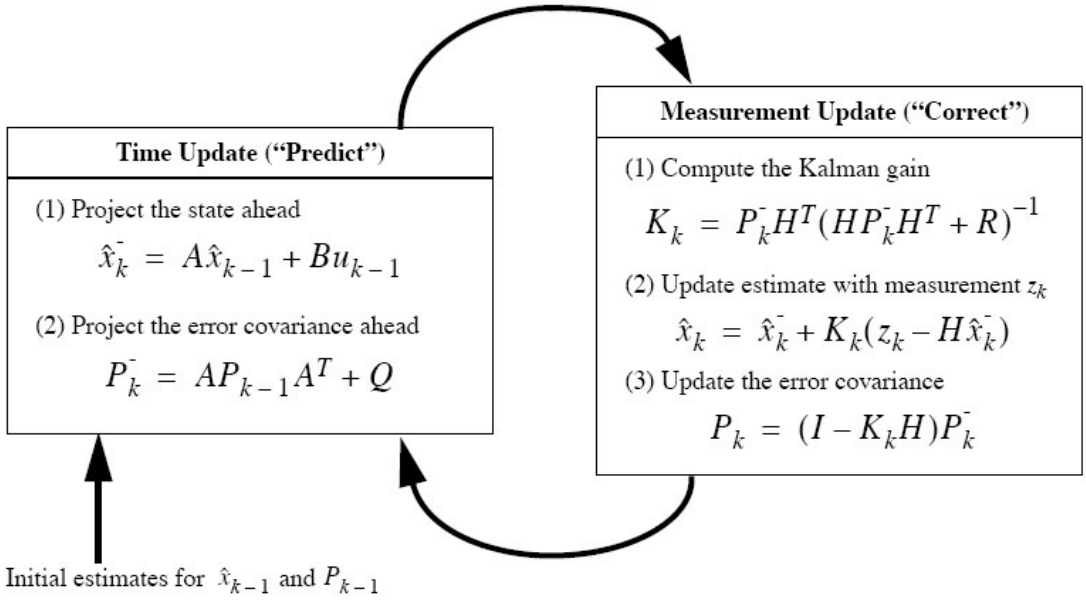

Figure 4-7. The Operation of the Kalman filter.

4.3.5 Advantage

Both position detection methods are processed simultaneously. The result of the position detection determined earlier by the received power information method narrows the solution range of the time difference of arrival method, thus decreasing calculation time and improving accuracy.

Since the STA does not need to collect the received power information from several APs during the position detection process, few functions are required for the STA; consequently, users can connect to the Internet without any interruption due to the position estimation process.

Additionally, the database in which the value pairs (position of the STA and RSS values received at neighbor APs) are stored obtain feedback from the position estimation using signal arrival time difference; thus, the database can be automatically generated and updated. As a result, the database does not need to be manually generated before the installation of the APs. Furthermore, even when the neighboring layouts change, the database is automatically updated.

4.3.6 Disadvantage

The disadvantage of the proposed system is that two radio interfaces are required for every AP in the system. Thus, the proposed system is more expensive and affects the system in term of inter-channel interference. However, as explained in Chapter 3, this is not a large problem when compared to other proposals that require changes in current wireless LAN cards, since it is always more viable to introduce changes on the network operator side. Users do not need to buy new wireless LAN cards but may be required to update the firmware in their devices in order to support this novel wireless position system.

4.4 Performance Evaluation

To evaluate the performance of the proposed system, the OPNET simulator [52] is used. This paper considers an environment with a very low multipath channel and perfect synchronization system with time error less than 2.5ns that allows us to estimate the TDOA accurately. For more severe multipath channel conditions, additional mechanisms, such as the super-resolution technique or a training phase, may be required. Table 4-1 lists the WLAN parameters used in the simulation.

Table 4-1. Simulation Parameters.

Area size	30x40m	Number of APs	3
Data Type	Real-Time	Data rate	2 Mbps
Channels	1, 6, 11	Sync Error	± 2.5ns
Radio Propagation Model	Super-Solution	Multi-path Error	very low

The proposed system is compared with a joint clustering technique [5] and the CN-TOAG algorithm [6]. The next section analyzes the location estimation error and performance assessment, and then compares the results.

4.4.1 Location Estimation Error

The simulation environment of a wireless network with three APs and one STA (Fig. 4-8); a typical 30m x 40m meeting room is considered the target area. The STA connects to AP1 and moves at a walking speed (5Km/h) to a specific area. In the proposed system, the moving STA communicates with AP1, while AP2 and AP3 continue to receive data frames from the STA and to send the advanced information to AP1 in order to estimate the location of the STA; this process repeats to continuously estimate the location of the STA. The simulations of the STA using the joint clustering technique [5] and the CN-TOAG algorithm [6] are evaluated to estimate the position of the STA every 2 seconds. The initial results from the simulations (Figs. 4-9 and 4-10) show that the proposed system can better estimate the location of the STA than these approaches. The proposed system runs the received power information method to continually estimate the location of the STA, while the time difference of arrival method simultaneously calculates the location of the STA using the hyperbolic positioning algorithm. As a result, the position detection time decreases, and accuracy improves.

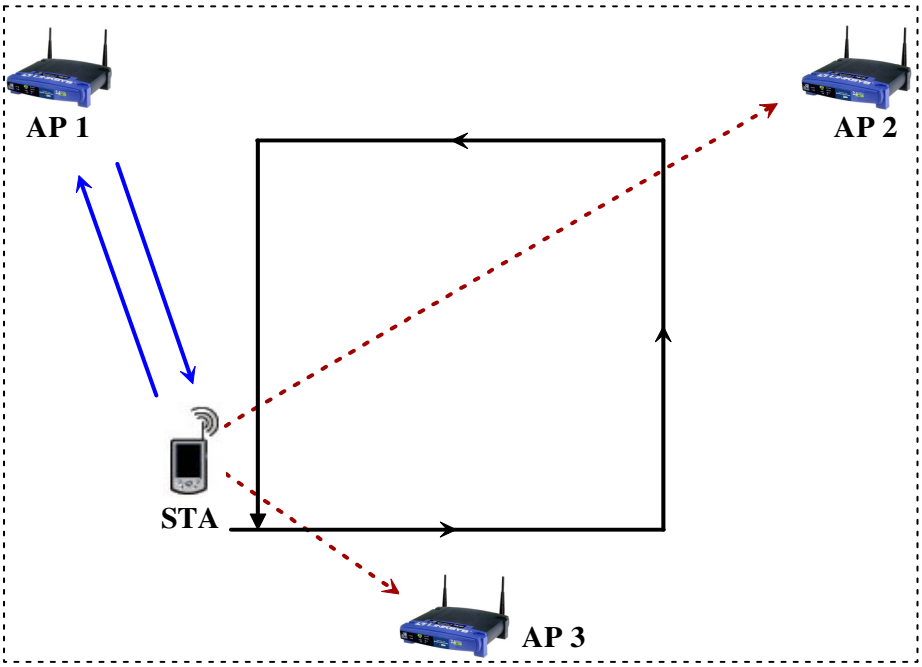

Figure 4-8. Simulation environment 1.

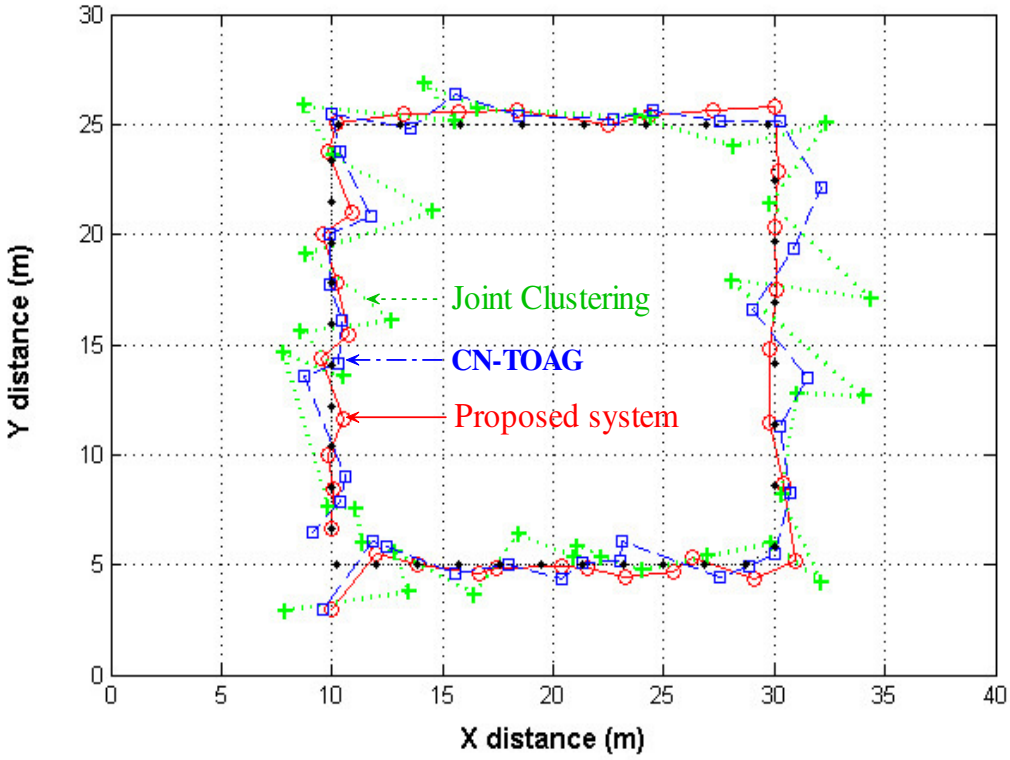

Figure 4-9. Track of movement.

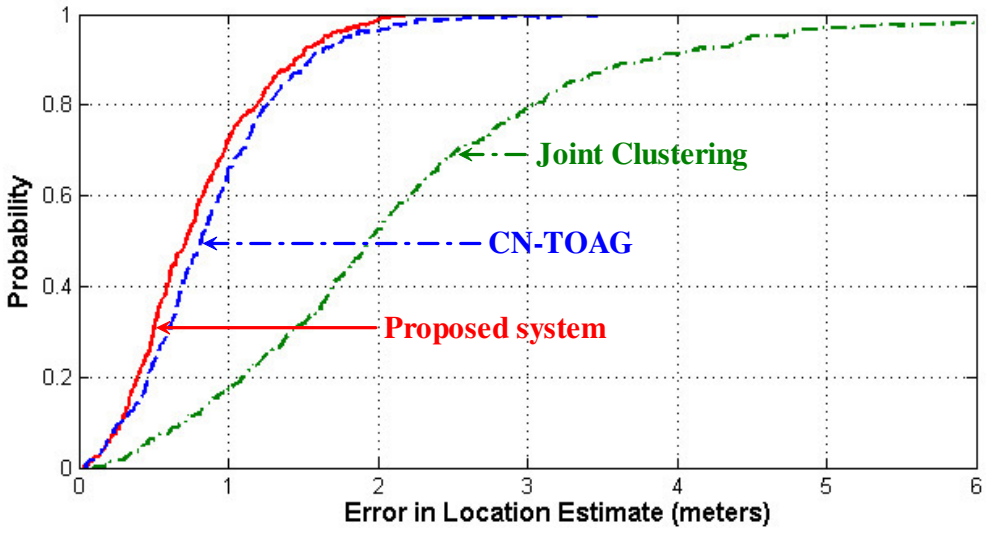

Figure 4-10. CDF of the Error in Location Estimation.

In Fig. 4-11, the STA communicates with AP1, moving in a triangle direction, to analyze the difference in moving direction. The simulations of the STA using the joint clustering technique and the CN-TOAG algorithm are evaluated and compared with the proposed system. The results from the simulations in Figs. 4-12 and 4-13 show that the proposed system can better estimate the location of the STA.

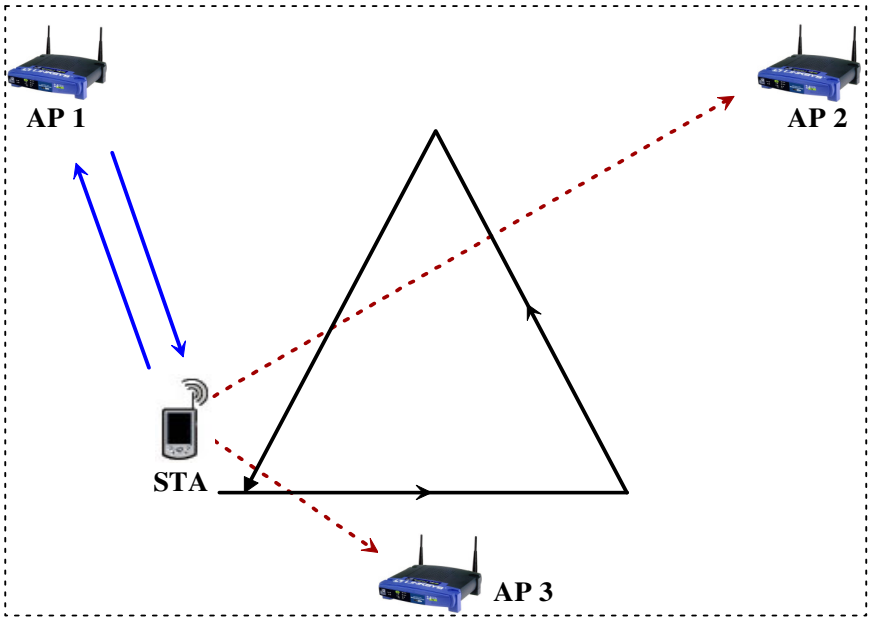

Figure 4-11. Simulation environment 2.

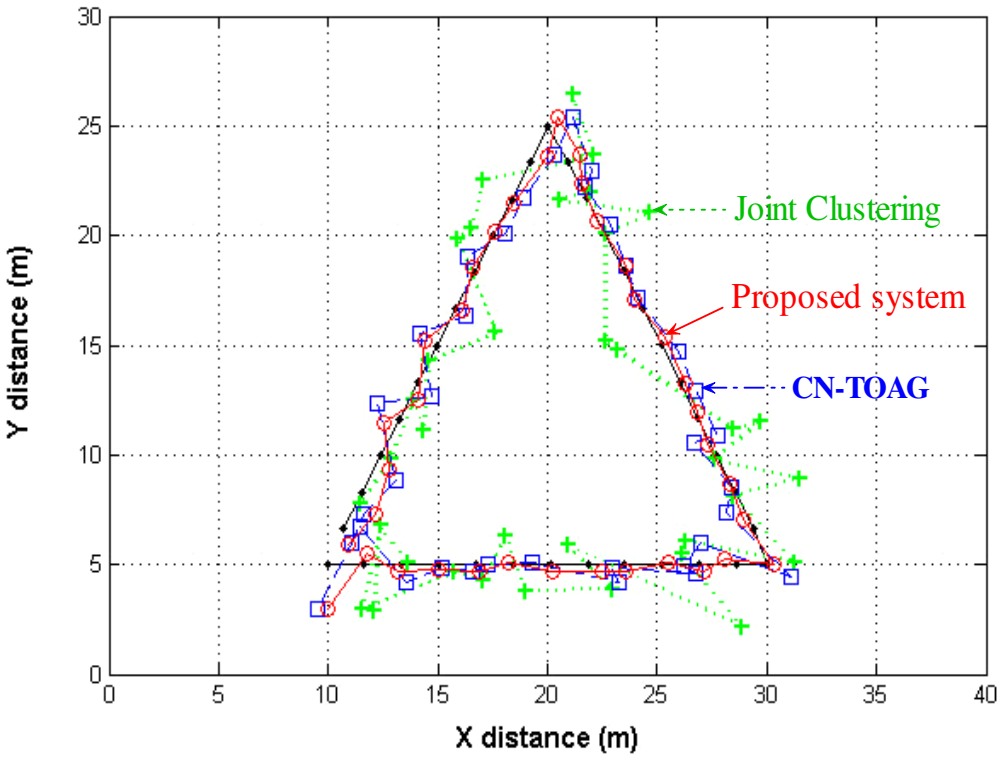

Figure 4-12. Track of movement.

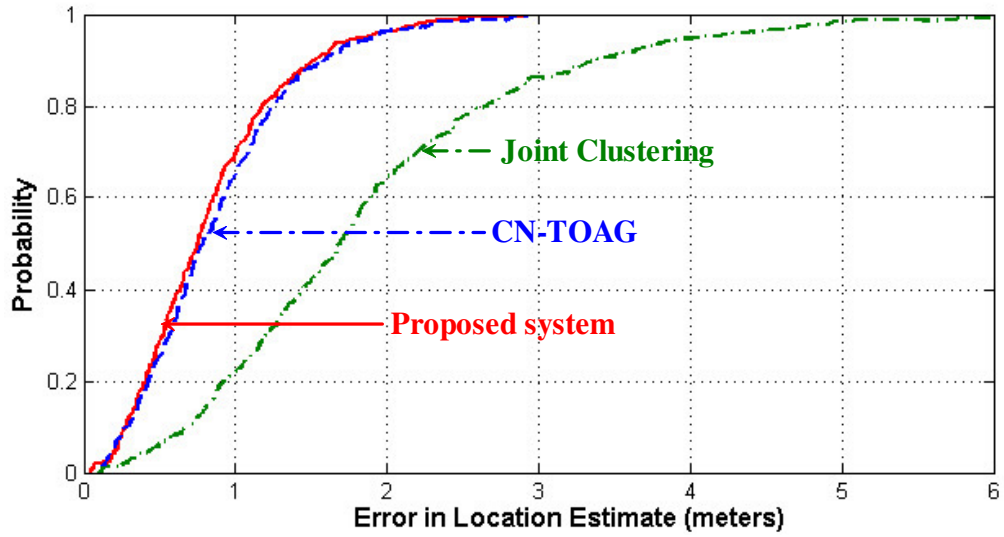

Figure 4-13. CDF of the Error in Location Estimation.

4.4.2 Performance Assessment

To evaluate the performance of the proposed system, VoIP traffic based on the G.711 codec standard [53] is used in the communication between the STA and AP1. A VoIP packet is generated every 20ms with 160-byte data, a 12-byte RTP header, an 8-byte UDP header, and a 20-byte IP header. The VoIP packet size for the IEEE 802.11 MAC layer becomes 200 bytes per packet with a data rate of 80 kbps (excluding the MAC header). The system using the proposed technique and the joint clustering technique [5] are simulated. The proposed method continuously estimates the location of the STA, while the joint clustering approaches estimates the location of the STA only once. In the proposed system, the STA does not scan the received power from neighbor APs in different channels; instead, neighbor APs use their second transceiver to continuously scan and gather information on neighboring STAs and then send the advanced information back to AP1.

Using the joint clustering technique, the Internet connection is disrupted when the positioning system is running, because the STA must switch its transceiver to each channel in order to scan and obtain the signal power information; this takes more than one second using passive scan mode. The results from the simulation (Fig. 4-14) show that there is no interruption of the Internet connection using the proposed technique. This is a necessity for real-time applications such as VoIP that require a delay time of less than 50ms.

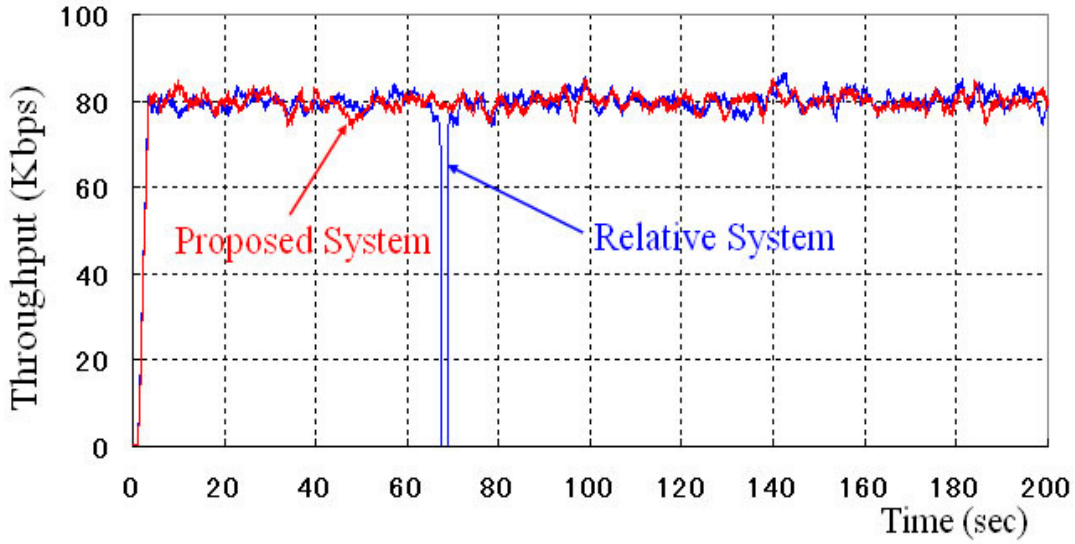

Figure 4-14. Throughput Performance.

4.5 Conclusion

A novel IEEE 802.11 WLAN-based positioning system provides high location accuracy without disrupting the network connection. The second transceiver scans nearby STAs in the transmission range and sends advanced information to their associated APs, which analyze and search a database to estimate the location of the STA. The TDOA technique is processed simultaneously to improve the accuracy of the location estimation. The initial results show that wireless networks are able to estimate the location of a STA without any interruption to the Internet connection; the accuracy of indoor wireless positioning systems is also improved. Although offering a number of advantages, the proposed system requires a novel AP with two transceivers, and users may need to update the firmware in their WLAN cards.

The cost of the proposed network is surveyed and compared to the conventional and related works. Table 4-2 shows the total cost of a small wireless network (3 APs and 20 STAs) using a difference technique. The

proposed system costs 7.9% more than the conventional scheme but 9.23% less than TDOA master-slave systems.

Table 4-2. Cost Comparison.

	Conventional	TDOA Master-Slave	Proposed
3 APs	$606 x3	$606 x4	$691 x3
10 STAs	$69 x20	$69 x20	$69 x20
Total	***$3198***	***$3804***	***$3453***

A high accuracy wireless positioning system that does not interrupt the Internet connection will be useful for future wireless LANs. Such systems are capable of supporting real-time services and can be enhanced to support higher data rates applications. The future work will focus on using the location of the STA to improve wireless network performance in terms of both seamless mobility and traffic load balance among neighbor APs in order to support real-time applications.

Chapter 5

Conclusion and Future Works

This chapter summarizes the results and concludes the dissertation, then provides directions for future research in this area.

5.1 Conclusion

IEEE 802.11 based wireless local area networks (WLANs) have seen immense growth in the last few years. In public places, such as college campuses and corporations, WLANs provide convenient network connectivity and a high speed link up to 11Mbps (IEEE 802.11b) or 54Mbps (IEEE 802.11a/g). The IEEE 802.11 network MAC specification allows for two operating modes, namely, the ad hoc and the infrastructure mode. In the ad hoc mode, two or more wireless stations (STAs) recognize each other and establish a peer-to-peer communication without any existing infrastructure, whereas in the infrastructure mode, there is a fixed entity called an access point (AP) that bridges all data between the mobile stations associated with it. The AP and associated mobile stations form a basic service set (BSS) communicating on the unlicensed RF spectrum.

In WLAN infrastructure mode, a handoff occurs when a mobile station moves beyond the radio range of one AP and enters another. During the handoff, management frames are exchanged between the STA and the AP. The APs involved may exchange certain context information specific to the handoff process, during which the STA is unable to send or receive traffic. Because of the mobility-enabling nature of wireless networks, there is opportunity for many promising real-time applications such as VoIP, 802.11 phones, mobile video conferencing and e-learning. Many believe that WLANs may become the next generation 4G wireless networks. These require seamless handoff to support services over wireless networks.

Recently, WLAN can provide Location-based services (LBS) that are expected to become a part of our everyday lives. Services like friend finders, weather information, or city event boards are already available for mobile phone users. Other location services like road tolling for trucks or fleet management are also operational LBS business applications. This dissertation describes how important WLAN based positioning systems can promote LBS in indoor (in-building) areas. While LBS can provide effective services, customers do not want to disconnect their mobile station from the Internet before receiving LBS.

This dissertation presents a holistic approach for system architecture design for seamless handoff over WLAN. The novel wireless network architecture using a multi-radio AP with fast passive scan mode largely improves the performance of wireless LANs in terms of latency time during handoff and provides traffic load balance among APs in the network. The STAs in the proposed system perform a handoff that is faster and smoother than in the traditional and relative works. Furthermore, because the handoff process is controlled by the AP instead of the STA, the network is able to provide traffic

load balance among neighbor APs, thus allowing the proposed scheme to reduce the number of dropped packets due to traffic overload. The simulation results show a large reduction in dropped packets.

Moreover, the novel WLAN infrastructure based positioning system is presented. In this system, the AP uses the second transceiver scans nearby STAs in the transmission range and sends advanced information to their associated APs, which analyze and search a database to estimate the location of the STA. The TDOA technique is processed simultaneously to improve the accuracy of the location estimation and to automatically generate and update the database. The initial results show that wireless networks are able to better estimate the location of a STA without disrupting the Internet connection.

The disadvantages of the proposed method are that the APs must be equipped with two radios, and users might need to update the firmware for their WLAN cards. However, the seamless handoff scheme provided by the proposed mechanism largely compensates for these disadvantages by improving the support of real-time services and the distribution of traffic load inside the WLAN. Furthermore, a high accuracy wireless positioning system that does not interrupt the Internet connection will be useful for future WLANs. Such systems are capable of supporting real-time services and can be enhanced to support higher data rate applications.

In addition, the cost of the proposed network is surveyed and compared to the conventional and related works. The total cost of a small wireless network (3 APs and 20 STAs) shows it costs more than the conventional scheme but less than other related works.

5.2 Future Works

Future works will focus on using the location of the STA to improve wireless network performance in terms of seamless mobility and traffic load balance among neighbor APs. Research on multi-radio access points for higher data rates in wireless networks should be considered to improve quality of service (QoS) and real-time service support. Nonlinear combination with neural networks might be considered instead of using fuzzy logic in the handoff decision process to provide an effective handoff trigger. Moreover, studies on techniques to improve the wireless positioning systems based on the WLAN infrastructure are needed, and the system should be evaluated in real experiments.

Appendix A

Fuzzy Logic Principles

Fundamentals

In 1965, Professor Lotfi A. Zadeh of University of California, Berkeley laid the foundation for fuzzy logic [65] [66] [67] as it is known today. He recognized that the true-or-false nature of Boolean logic does not account for the many shades of gray found in real-world problems. Zadeh expanded the idea of a classical set to what he termed as a fuzzy set. Boolean logic is bivalent, with only two values, zero (false) or one (true), that are mutually exclusive. On the other hand, fuzzy logic is multi-valued, dealing in degrees of membership or truth within the set. Thus, values within a set can be either partially true or partially false at the same time.

For any set S, its characteristic function $f_S(x)$ describes whether an element x is an element of set S, where $f_S(x)=1$ if true and $f_S(x)=0$ if false.

In Boolean logic, this can be expressed as:

$$f_S(x) = \begin{cases} 1, & if\ x \in S \\ 0, & if\ x \notin S \end{cases} \qquad \textbf{(A-1)}$$

Although sets can overlap in Boolean logic, the transition at the border of the set is instantaneous. At the border of the set, element x either is or is not a member of the set (see Figure A-1). As x approaches this border, small changes in x can cause significantly different reactions in the system as x changes from set 1 to set 2.

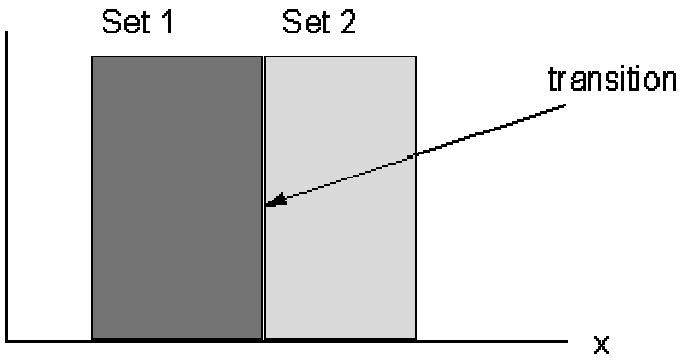

Figure A-1. Conventional Boolean Sets.

In fuzzy logic, $\mu_S(x)$ describes the membership function of S, or the degree to which x is a member of set S; this is known as the degree of truth.

$$\mu_S(x) = \begin{cases} 1, & if\ x\ is\ totally \in S \\ 0, & if\ x\ is\ not \notin S \\ 0 < \mu_S(x) < 1, & if\ x\ is\ partially \in S \end{cases} \qquad \textbf{(A-2)}$$

With fuzzy logic, this transition at the border of sets is gradual, thus allowing partial membership in both sets (see Figure A-2). Small changes in x cause a more gradual change in system performance.

Fuzzy systems offer advantages over classical systems in control design, including a higher degree of user friendliness, self-diagnostic capabilities, and a higher degree of adaptability. Rigor and respectability is desired in control, but there are many realistic problems that cannot be rigorously defined. According to Zadeh [65] [66] [67], fuzzy algorithms for control policy will gain increasing though perhaps grudging acceptance, because conventional non-fuzzy

algorithms cannot, in general, cope with the complexity and ill-defined nature of large scale systems. Control theory must be less preoccupied with mathematical rigor and precision and more concerned with the development of qualitative or approximate solutions to real-world problems.

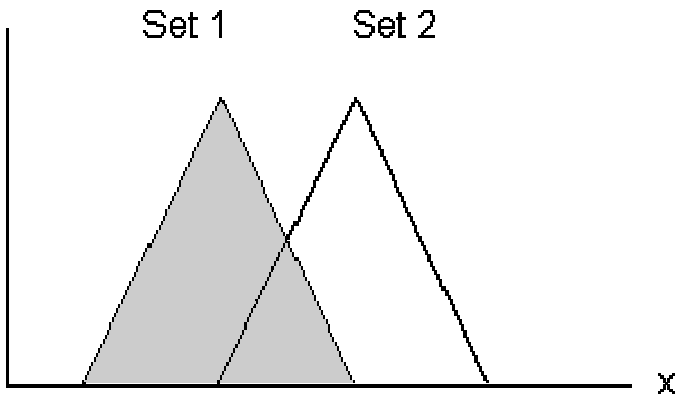

Figure A-2. Fuzzy Sets.

Stability theory for classical control systems is limited in the sense that it requires linearization and assumptions of the problem at hand. It is very difficult to determine if those assumptions hold; thus, there is no comfortable assurance in the stability of the control model. Fuzzy systems are course control systems that exploit tolerance for imprecision. Although stability theory for fuzzy systems is not as well-developed as it is for classical systems, it is very effective when it comes to linear systems; fuzzy systems deal with nonlinearity. Conventional classical control techniques for high performance systems, such as proportional integral derivative (PID) control, are widely used. However, the performance of PID controllers depends heavily on the operating parameters of the system. Linearization of the mathematical model is required, and the system's behavior must be thoroughly understood. Often, it is very difficult to implement this mathematical model.

Fuzzy logic employs linguistic terms, as described by experienced users, that assist in the generation of a precise control surface using appropriate rules and membership functions for the variables. Its use in engineering applications has been very successful in Japan and in Europe. However, conservative North American attitudes have regarded the methodology cautiously. Recently, there has been some acceptance and implementation of fuzzy logic in control applications.

The Process

The process of a fuzzy logic system is incorporated into a fuzzy inferencing unit (FIU). It is comprised of three steps that process the system inputs to the appropriate system outputs: fuzzification, rule evaluation, and defuzzification. The FIU is illustrated in Figure A-3. Each step of the FIU is described in the following sections.

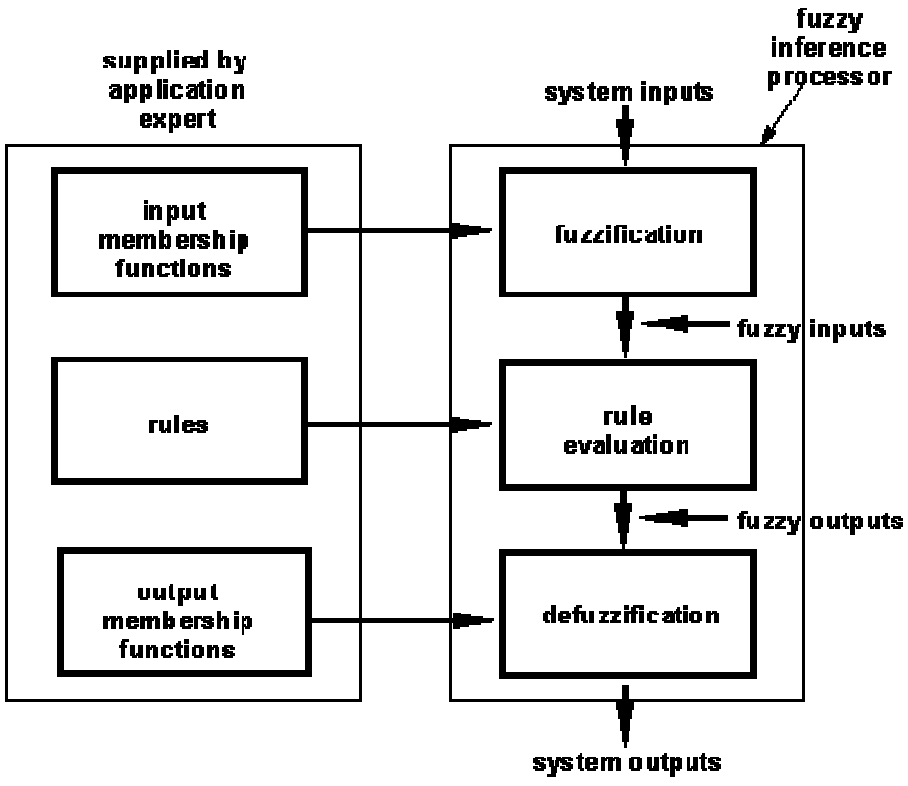

Figure A-3. Fuzzy Inferencing Unit.

Fuzzification

Fuzzification is the first step in the fuzzy inferencing process. This involves domain transformation in which where crisp inputs are transformed into fuzzy inputs. Crisp inputs are exact inputs measured by sensors and passed into the control system for processing, such as temperature, pressure, rpm, etc. Each crisp input that must be processed by the FIU has its own group of membership functions or sets to which they are transformed. This group of membership functions exists within a universe of discourse that holds all relevant values that the crisp input can possess. Figure A-4 shows the structure of membership functions within a universe of discourse for a crisp input, where

- **degree of membership**: degree to which a crisp value is compatible to a membership function, from 0 to 1; also known as the truth value or fuzzy input
- **membership function (MF)**: defines a fuzzy set by mapping crisp values from its domain to the set's associated degree of membership
- **crisp inputs**: distinct or exact inputs to a certain system variable, usually measured parameters external from the control system, e.g. 6V
- **label**: descriptive name used to identify a membership function
- **scope**: the width of the membership function or range of concepts, usually numbers, over which a membership function is mapped
- **universe of discourse**: range of all possible values, or concepts, applicable to a system variable

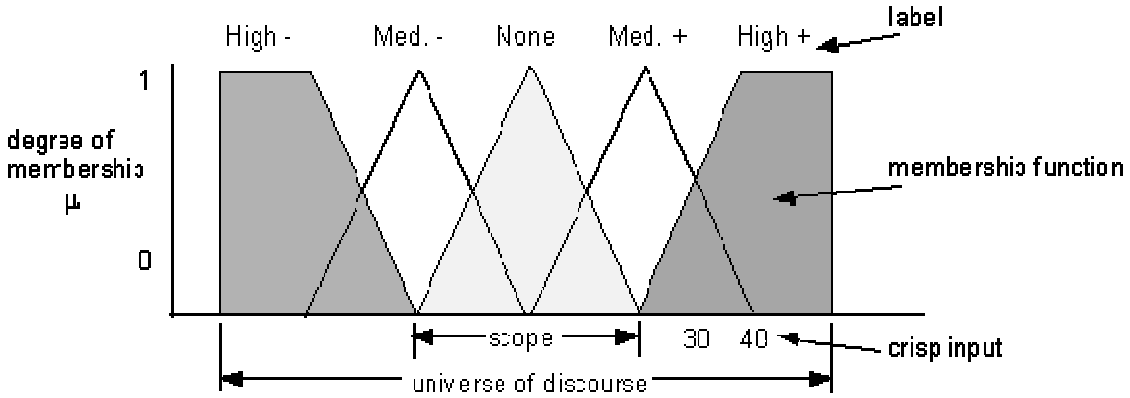

Figure A-4. Membership Function Structure.

When designing the number of membership functions for an input variable, labels must be initially determined for the membership functions. The number of labels corresponding to the number of regions that the universe should be divided, such that each label describes a region of behavior. A scope must be assigned to each membership function that numerically identifies the range of input values that correspond to a label.

The shape of the membership function should be representative of the variable. However, this shape is also restricted by the computing resources available. Complicated shapes require more complex descriptive equations or large lookup tables. For 8-bit MCUs, trapezoidal shapes and singletons are generally used. Figure A-5 shows examples of possible shapes for membership functions.

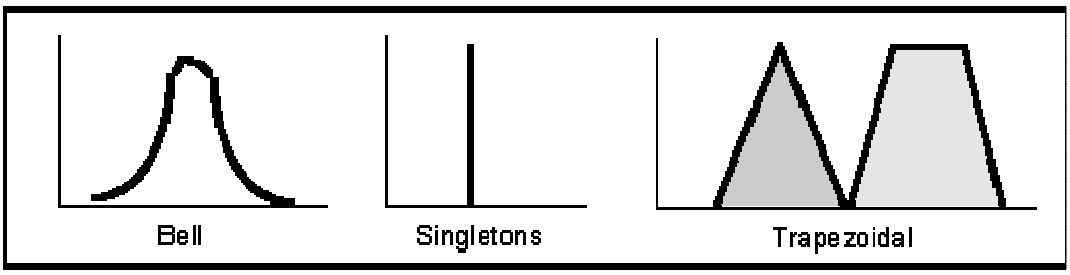

Figure A-5. Membership Function Shapes.

The singletons and trapezoidal shapes can be represented by a point-slope format. Singletons require one byte for descriptions; trapezoids, four bytes, two point locations on the variable axis, and two slopes or grade values. The point locations require only the *x* coordinate, because the *y* coordinate is defined as zero for point 1 and one for point 2 (Figure A-6).

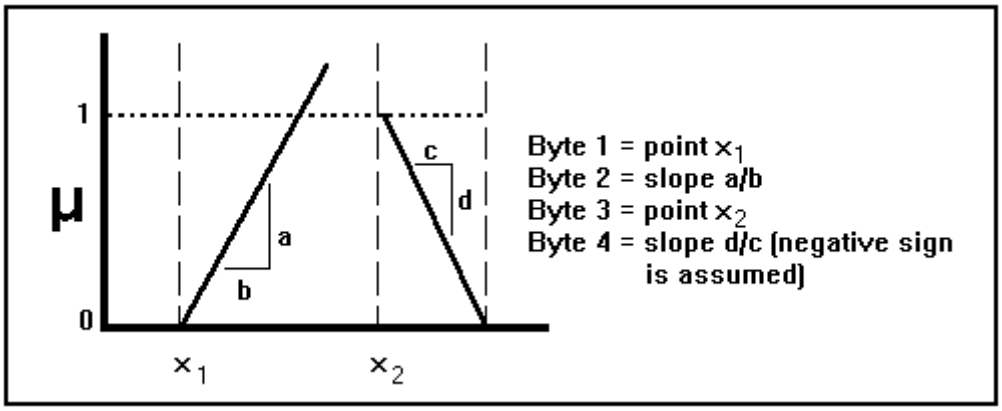

Figure A-6. Point-Slope Representation.

Considering the number of membership functions that exist within the universe of discourse, one must remember that:

i) too few membership functions for a given application will cause slow response of the system and failure to provide sufficient output control in order to recover from a small input change. This may also cause oscillation in the system.

ii) too many membership functions may cause rapid firing of different rule consequents for small changes in input, resulting in large output changes, which may cause instability in the system.

The industry standard consists of 3 to 9 membership functions. These membership functions should overlap. No overlap reduces a system based on Boolean logic. Every input point on the universe of discourse should belong to the scope of at least one but no more than two membership functions. No two

membership functions should have the same point of maximum truth (Eq. A-3). When two membership functions overlap, the sum of truths or grades for any point within the overlap should be less than or equal to one. Overlap should not cross the point of maximal truth of either membership function. In 1992, Marsh from Motorola [36] has proposed two indices to quantitatively describe the overlap of membership functions: overlap ratio and overlap robustness. Figure A-7 illustrates their meaning.

$$Overlap\ Ratio = \frac{overlap\ scope}{adjacent\ MF\ scope} \qquad \textbf{(A-3)}$$

$$Overlap\ Robustness = \frac{area\ of\ summed\ overlap}{\max.\ area\ of\ summed\ overlap} = \frac{\int_L^U (\mu_1 + \mu_2)dx}{2(U-L)} \qquad \textbf{(A-4)}$$

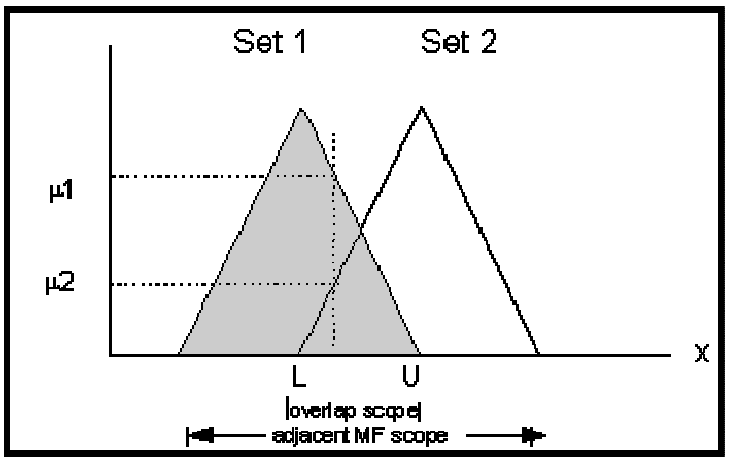

Figure A-7. Overlap Indices

The industry standard is that the overlap ratio should be in the range of 0.2 to 0.6 (ideally 0.33). The value of the overlap robustness is usually greater than the overlap ratio, falling in the range 0.3 to 0.7 (ideally 0.5). High overlap ratio or robustness enables the fuzzy logic controller to cope with more ambiguity, giving it a greater degree of control.

The fuzzification process maps each crisp input in the universe of discourse. Its intersection with each membership function is transposed onto the μ axis as illustrated in Figure A-7. These μ values are the degrees of truth for each crisp input and are associated with each label as fuzzy inputs. These fuzzy inputs then pass to the next step, rule evaluation.

Rule Evaluation, Min./Max. Inference

Rule evaluation consists of a series of IF-Zadeh Operator-THEN rules. A decision structure to determine the rules requires familiarity with the system and its desired operation. For this dissertation, the rule involves obtaining information on signal strength and traffic load conditions from neighbor APs. There is a strict syntax that is structured as:

IF antecedent 1 ZADEH OPERATOR antecedent 2.....

THEN consequent 1 ZADEH OPERATOR consequent 2.....

The antecedent consists of an input variable IS label and is equal to its associated fuzzy input or truth value $\mu(x)$. The consequent consists of output variable *IS* label, and its value depends on the Zadeh Operator, which determines the type of inferencing used. There are three Zadeh Operators: AND, OR, and NOT. The label of the consequent is associated with its output membership function. The Zadeh Operator is limited on two membership functions, as discussed in the fuzzification process. Zadeh Operators are similar to Boolean Operators such that

AND represents the intersection or minimum between the two sets, expressed as

$$\mu_{A\cap B} = \min[\mu_A(x), \mu_B(x)] \qquad \textbf{(A-5)}$$

OR represents the union or maximum between the two sets, expressed as

$$\mu_{A\cup B} = \max[\mu_A(x), \mu_B(x)] \quad \textbf{(A-6)}$$

and NOT represents the opposite of the set, expressed as

$$\overline{\mu_A} = [1 - \mu_A(x)] \quad \textbf{(A-7)}$$

Given the design software used for this thesis, the Zadeh Operators are limited to the use of AND only; this is referred to as minimum inferencing. The rule strength is determined by taking the minimum fuzzy input of antecedent 1 (AND) antecedent 2 (min. inferencing). This minimum result is equal to the consequent rule strength. If there are any consequents that are the same, then the maximum rule strength between similar consequents is taken, referred to as maximum inferencing. This infers that the truest rule is taken. These rule strength values are referred to as fuzzy outputs.

Defuzzification

Defuzzification involves the process of transposing fuzzy outputs to crisp outputs. There are a variety of methods to achieve this, but this discussion is limited to the process used in the thesis design.

A method of averaging known as the center of gravity (COG) method is used to calculate the centroids of sets. The output membership functions to which the fuzzy outputs are transposed are restricted to singletons. This limits the degree of calculation intensity in the microcontroller. The fuzzy outputs are transposed to their membership functions, similarly to fuzzification. With COG, the singleton values of outputs are calculated using a weighted average, illustrated in Figure A-8. The crisp output passes out of the FIU for processing elsewhere in the program of the controller.

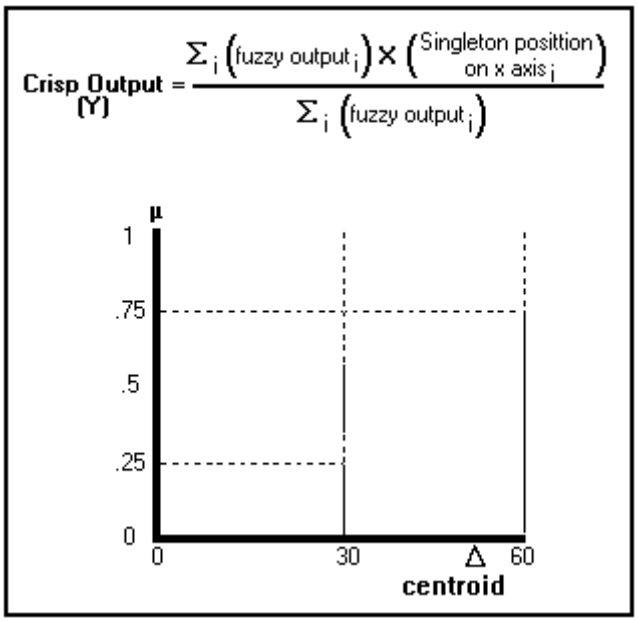

Figure A-8. COG of Singletons.

Several applications of fuzzy algorithms for the handoff process have been reported in the literature. In this dissertation, fuzzy classifiers were used as a handoff enhancement process. Simulation results are reported and compared against the common RSSI with hysteresis algorithm.

The number of handoffs resulting from applying the fuzzy algorithms is comparable to that obtained with the RSSI algorithm, though exhibiting a smaller number of handoffs for large propagation variance environments. Additionally, the advantage of using fuzzy classifier schemes is that the cell shape and radius are kept closer to the original designed area, thus avoiding cell coverage go far inside the area of other cells. This advantage can be of great significance because the cochannel and adjacent channel interference can be considerably reduced in situations of high traffic load.

Appendix B

Hyperbolic Equation Solving Algorithms

Once the time difference of arrival (TDOA) estimates have been obtained, they are converted into range difference measurements that can be subsequently converted into nonlinear hyperbolic equations. Solving these non-linear equations is a challenging operation. Several algorithms have been proposed for different complexities and accuracies. This appendix will first discuss the mathematical model that is used by these algorithms, followed by a survey of the algorithms that can be used for solving hyperbolic equations.

Mathematical Model for Hyperbolic TDOA Equations

A general model for the two-dimensional (2D) positioning location (PL) estimation of a source using M base stations is developed (see Figure B-1). Referring all TDOAs to the first base station, which is assumed to control the call and is the first to receive the transmitted signal, let index $i = 2,\ldots,M$, unless otherwise specified; (x, y) be the source location; and $(Xi; Yi)$ be the known location of the ith receiver. The squared range distance between the source and the ith receiver is given as

$$R_i = \sqrt{(X_i - x)^2 + (Y_i - y)^2} = \sqrt{X_i^2 + Y_i^2 - 2X_i x - 2Y_i y + x^2 + y^2} \quad \textbf{(B-1)}$$

The range difference between base stations with respect to the base station where the signal first arrives is obtained by

$$R_{i,1} = c\, d_{i,1} = R_i - R_1 = \sqrt{(X_i - x)^2 + (Y_i - y)^2} - \sqrt{(X_1 - x)^2 + (Y_1 - y)^2} \quad \textbf{(B-2)}$$

where c is the signal propagation speed; $R_{i,1}$ is the range difference distance between the first base station and the ith base station; R_1 is the distance between the first base station and the source; and $d_{i,1}$ is the estimated TDOA between the first base station and the ith base station. This defines the set of nonlinear hyperbolic equations whose solution gives the 2D coordinates of the source.

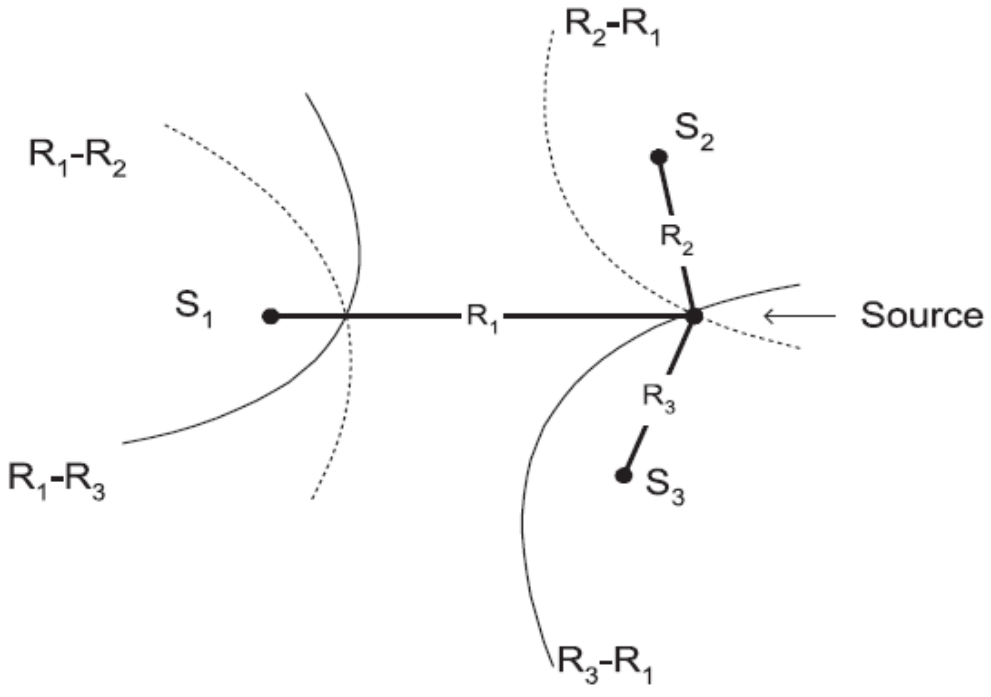

Figure B-1. 2D Hyperbolic Position Location Solution.

Solving the nonlinear equations (Eq. B-2) is difficult. Consequently, this set of equations is commonly linearized. One way of linearizing these equations is

through the use of Taylor-series expansion, retaining the first two terms [68, 69]. An alternative method, presented in [70, 71, 72, 73], is to first transform the set of nonlinear equations (Eq. B-2) into another set of equations as follows:

$$R_i^2 = \left(R_{i,1} + R_1\right)^2 \qquad \textbf{(B-3)}$$

Eq. B-1 can now be rewritten as

$$R_{i,1}^2 + 2R_{i,1}R_1 + R_1^2 = X_i^2 + Y_i^2 - 2X_i x - 2Y_i y + x^2 + y^2 \qquad \textbf{(B-4)}$$

Subtracting Eq. B-1 at $i = 1$ from Eq. B-4 results in

$$R_{i,1}^2 + 2R_{i,1}R_1 = X_i^2 + Y_i^2 - 2X_{i,1} x - 2Y_{i,1} y + x^2 + y^2 \qquad \textbf{(B-5)}$$

where $X_{i,1}$ and $Y_{i,1}$ are equal to $(X_i - X_1)$ and $(Y_i - Y_1)$, respectively. The set of Eq. B-5 are now linear, with the source location (x, y) and the range of the first receiver to the source R_1 as the unknown variables.

Algorithms for Linearly Placed Base Stations

When base stations are placed in a linear fashion, the estimation of the PL is simplified. Since base stations in a practical cellular-type system are usually non-linear, these algorithms are not of much significance for wireless E-911. This section presents a brief discussion of four algorithms proposed in the literature for such cases.

For receivers arranged in a line, Carter's beam forming method provides an exact solution for the source range and bearing [74]. However, it requires an extensive search over a set of possible source locations, which can become computationally intensive. Hahn's method [75, 76] estimates the source range and bearing from the weighted sum of ranges and bearings obtained from the TDOAs of every possible combination; this method is sensitive to the choice of weights, can be complicated, and is only valid for distant sources. Abel and Smith provide an explicit solution that can achieve the 24 Cramer-Rao lower

bound (CRLB) in the small error region [77]. The CRLB defines the optimum performance for an algorithm that solves Eq. B-2 [43] and evaluates how close any particular position location technique comes to approaching the theoretical minimum mean squared error [64, 78, 79]. Chan's method, which works for arbitrarily placed receivers, can also be used for linearly placed receivers with minor modifications [64]. A detailed discussion of this method will follow later in this section.

Algorithms for Arbitrarily Placed Base Stations

When base stations are arbitrarily placed, which is a typical scenario in the infrastructure of a cellular/WLAN system, position x becomes more complex. Apart from complexity, another issue is the consistency of the system of equations. If the set of nonlinear hyperbolic equations equals the number of unknown coordinates of the source, then the system is consistent, and a unique solution can be determined from either closed form formulas or iterative algorithms.

For example, determining the position of a mobile station in a 2D system using three base stations, which gives us two TDOA measurements at base stations #2 and #3 relative to base station #1, we have a consistent system, since there are two equations to solve for two unknowns. However, if the system is inconsistent, i.e., there are redundant range difference measurements, then the problem of solving for the position location of the source becomes more difficult, because no unique solution exists. This may happen if we try to use more than three base stations to obtain redundant TDOA measurements for a 2D solution. Although this may not happen very often because of the limit cover area of the WLAN, this may occur in some situations such as

microcellular environments. Hence, it is an important issue that an algorithm can optimally solve inconsistent systems of equations.

Other issues include computational complexity of the algorithms, their ability to provide exact solutions, the risk of convergence to a local minimum for iterative algorithms if the starting point is bad, and the requirement of some *a priori* information for the algorithms to work.

The following sections survey seven algorithms found in the literature that are able to deal with situations when the receivers are arbitrarily placed. These algorithms have been examined in light of the issues mentioned above. There are three algorithms found to be particularly feasible for wireless LAN based positioning systems; they are explained in more mathematical detail later.

Friedlander's Method: Friedlander's method utilizes least squares (LS) and weighted least squares (WLS) error criteria to solve for the position location estimate [70]. It has been shown in [80] that the LS solution provides the maximum likelihood (ML) estimate, if the range difference errors are uncorrelated and Gaussian distributed with zero mean and equal variances. If the variances are equal, then the WLS is the ML estimate. However, a problem exists, because the variances are either not known *a priori* or are difficult to estimate. Friedlander's simulation results show that the LS and WLS solutions were identical using four base stations. For more than four base stations, the WLS PL solution outperformed the LS PL solution. This method assumes that R_1 is independent of x and y in Eq. B-5 and thus is able to eliminate R_1 from those equations. This method reduces the computational complexity as compared to other solutions but is suboptimal, because it eliminates a fundamental relationship.

Spherical-Intersection Method: The spherical-intersection (SX) method [71, 81] is another commonly used approach. It assumes that *R1* is known and solves x and y in terms of R_1 from Eq. B-5. The LS solution of Eq. B-1 is then used to find R_1 and thus x and y. Since R_1 is assumed to be constant in the first step, the degree of freedom to minimize the second norm of the error vector φ used in the solution is reduced [64]. The solution obtained is therefore suboptimal as demonstrated in [72, 73].

Spherical-Interpolation Method: Another approach called the spherical-interpolation (SI) method [72, 73, 81], first solves x and y in terms of R_1, then inserts the intermediate result back into Eq. B-5 to generate equations in the unknown R_1 only. Substituting the computed R_1 values that minimize the LS equation error to the intermediate result produces the final result. One drawback to the SI method is its inability to produce a solution if the number of unknowns is equal to the number of equations based on the TDOA estimates, which may occur in certain situations. The SI method was shown in [72] to provide an order of magnitude greater noise immunity than the SX method. Although the SI method performs better than the SX method, it assumes the x, y and R_1 variables in Eq. B-5 to be independent and eliminates R_1 from those equations. Consequently, the solution is suboptimal, because this relationship is ignored. The method proposed by Friedlander and the SI method have been shown in [70] to be mathematically equivalent.

Divide-and-Conquer Method: A divide and conquer (DAC) method, proposed by Abel [82], consists of dividing the TDOA measurements into groups, each having a size equal to the number of unknowns. The solution of the unknowns is calculated for each group and then appropriately combined to provide a final solution. Although this method can achieve optimum

performance, the solution uses stochastic approximation and requires that the Fisher information be sufficiently large. The Fisher information matrix (FIM) is the inverse of the Cramer-Rao Matrix Bound (CRMB) [76]. The estimator provides optimum performance for small errors, thus implying a low-noise threshold in which the method deviates from the CRLB. This method requires an equal number of range difference measurements in each group; as a result, the TDOA estimates from the remaining sensors cannot be used to improve accuracy.

Taylor-Series Method: Another method to obtain the precise estimate at the reasonable noise levels is the Taylor-series method [68, 69]. The Taylor-series method linearizes the set of Eq. B-2 by Taylor-series expansion, then uses an iterative method to solve the system of linear equations. The iterative method begins with an initial guess and improves the estimate at each iteration by determining the local linear LS solution. The Taylor-series can provide accurate results and is robust; it can also make use of redundant measurements to improve the PL solution. However, it requires a good initial guess and can be computationally intensive. For most situations, linearization of the nonlinear equations does not introduce undue errors in the position location estimate. However, linearization can introduce significant errors when determining a PL solution in poor geometric dilution of precision (GDOP) situations. GDOP describes a situation in which a relatively small ranging error can result in a large position location error, because the mobile is located on a portion of the hyperbola far away from both receivers. Bancroft [83] shows that eliminating the second order terms can lead to significant errors in this situation. The effect of linearization of hyperbolic equations on the position location solution is also explored by Nicholson in [84, 85].

Fang's Method: For arbitrarily placed base stations and a consistent system of equations in which the number of equations equals the number of unknown source coordinates to be solved, Fang [86] provides an exact solution to the Eq. B-5. However, his solution does not make use of redundant measurements made at additional receivers to improve position location accuracy. Furthermore, his method experiences an ambiguity problem due to the inherent squaring operation. These ambiguities can be resolved using *a priori* information or symmetry properties. Unlike the algorithms mentioned previously, this method provides a closed form exact solution and is computationally less intensive than the Taylor-series method.

Chan's Method: Chan [64] proposes a non-iterative solution to the hyperbolic position estimation problem that is capable of achieving optimum performance for arbitrarily placed sensors. The solution is in closed form and valid for both distant and close sources. When TDOA estimation errors are small, this method is an approximation to the ML estimator. Chan's method performs significantly better than the SI method and has a higher noise threshold than the DAC method before the performance deviates from the CRLB. Furthermore, it provides an explicit solution form that is not available in the Taylor-series method. It is also better than Fang's method, since it can take advantage of redundant measurements, like the Taylor-series method. However, it needs *a priori* information to resolve an ambiguity in its calculations like the Fang's method.

In the light of the above discussion, it appears that the Taylor-series method, Fang's method, and Chan's method can be practically used for solving hyperbolic equations. Among these, Fang's and Chan's methods provide a closed form exact solution that is not available with the Taylor-series method

and are computationally less intensive. The Taylor-series method also carries the risk of converging to a local minimum if given a bad starting point. On the other hand, the Taylor-series method and Chan's method can make use of redundant measurements, if available. The mathematical procedures for these three algorithms follow.

Mathematical Procedure for the Taylor-Series Method

The iterative Taylor-series method begins with an initial guess and improves the estimate at each iteration by determining the local linear LS solution. With a set of TDOA estimates, the method starts with an initial guess (x_0; y_0) and computes the deviations of the position location estimation as follows:

$$\begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} = \left(G_t^T Q^{-1} G_t\right)^{-1} G_t^T Q^{-1} h_t \qquad \textbf{(B-6)}$$

where

$$h_t = \begin{bmatrix} R_{2,1} - (R_2 - R_1) \\ R_{3,1} - (R_3 - R_1) \\ \vdots \\ R_{M,1} - (R_M - R_1) \end{bmatrix}$$

$$G_t = \begin{bmatrix} [(X_1 - x)/R_1] - [(X_2 - x)/R_2] & [(Y_1 - x)/R_1] - [(Y_2 - x)/R_2] \\ [(X_1 - x)/R_1] - [(X_3 - x)/R_3] & [(Y_1 - x)/R_1] - [(Y_3 - x)/R_3] \\ \vdots & \vdots \\ [(X_1 - x)/R_1] - [(X_M - x)/R_M] & [(Y_1 - x)/R_1] - [(Y_M - x)/R_M] \end{bmatrix}$$

Q is the covariance matrix of the estimated TDOAs. Values R_i for i = 1, 2,…,M are computed from Eq. B-1 with $x = x_0$ and $y = y_0$. In the next iteration, x_0 and y_0 are set to $x_0+\Delta x$ and $y_0+\Delta y$, respectively. The entire process repeats until Δx and Δy are sufficiently small, resulting in the estimated PL of the source (x, y). The Taylor-series method can provide accurate results; however, it requires a close initial (x_0, y_0) to guarantee convergence and can be computationally intensive.

Mathematical Procedure for Fang's Method

For a 2D hyperbolic PL system using three base stations to estimate the source location (x, y), Fang establishes a coordinate system so that the first base station (BS) is located at (0, 0); the second BS at (x_2, 0); and the third BS at (x_3, y_3). For the first BS (i = 1, $X1$ = $Y1$ = 0) and the second BS (i = 2, Y_2 = 0), the relationships are simplified as

$$R_1 = \sqrt{(X_1 - x)^2 + (Y_1 - y)^2} = \sqrt{x^2 + y^2}$$
$$X_{i,1} = X_i - X_1 = X_i$$
$$Y_{i,1} = Y_i - Y_1 = Y_i$$

Using these relationships, the Eq. B-5 can be rewritten as

$$\begin{aligned} 2R_{2,1}R_1 &= R_{2,1}^2 - X_i^2 + 2X_{i,1}x \\ 2R_{3,1}R_1 &= R_{3,1}^2 - \left(X_3^2 + Y_3^2\right) + 2X_{3,1}x + 2Y_{3,1}y \end{aligned} \qquad \textbf{(B-7)}$$

Using Eq. B-7, the equation can be simplified as

$$y = g * x + h \qquad \textbf{(B-8)}$$

where

$$g = \{R_{3,1} - (X_2 / R_{2,1}) - X_3\} / Y_3$$
$$h = \{X_3^2 + Y_3^2 - R_{3,1}^2 + R_{3,1} * R_{2,1}(1 - (X_2/R_{2,1})^2)\}/2Y_3$$

Substituting Eq. B-8 into the first Eq. B-7 results in

$$d * x^2 + e * x + f = 0 \qquad \textbf{(B-9)}$$

where

$$d = -\{(1 - (X_2 / R_{2,1})^2) + g^2\}$$
$$e = X_2 * \{(1 - (X_2 / R_{2,1})^2)\} - 2g * h$$
$$f = (R_{2,1}^2 / 4) * \{(1 - (X_2 / R_{2,1})^2)\}^2 - h^2$$

Solving the quadratic Eq. B-9, we get two values for x. Using *a priori* information, one of the values is chosen to determine y from Eq. B-8.

However, this ambiguity is not a problem in WLAN systems. This study finds through simulations that one of the roots of Eq. B-9, always results in x values that give mobile position estimates that are well beyond the cell coverage area. Hence, for position location in cellular/WLAN systems, we only need to evaluate the following root from Eq. B-9:

$$x = \frac{-e - \sqrt{e^2 - 4df}}{2d} \qquad \textbf{(B-10)}$$

As stated earlier, putting this value of x in Eq. B-8 will give us the other coordinate of the mobile's position estimate.

Mathematical Procedure for Chan's Method

Following Chan's method [64], for a three base station system (M=3), producing two TDOAs, x and y can be solved in terms of R_1 from Eq. B-5. The solution is in the form of

$$\begin{bmatrix} x \\ y \end{bmatrix} = -\begin{bmatrix} X_{2,1} & Y_{2,1} \\ X_{3,1} & Y_{3,1} \end{bmatrix}^{-1} \times \left\{ \begin{bmatrix} R_{2,1} \\ R_{3,1} \end{bmatrix} R_1 + \frac{1}{2} \begin{bmatrix} R_{2,1}^2 - K_2 + K_1 \\ R_{3,1}^2 - K_3 + K_1 \end{bmatrix} \right\} \qquad \textbf{(B-11)}$$

where

$$K_1 = X_1^2 + Y_1^2$$
$$K_2 = X_2^2 + Y_2^2$$
$$K_3 = X_3^2 + Y_3^2$$

When Eq. B-11 is inserted into Eq. B-1, with i = 1, a quadratic equation in terms of $R1$ is produced. Substituting the positive root back into Eq. B-11 results in the final solution. There may exist two positive roots from the quadratic

equation that can produce two different solutions, resulting in an ambiguity. This problem has to be resolved by using *a priori* information.

As shown for Fang's algorithm, simulations in this work have shown that one of the roots of the quadratic equation in *R1* almost always provides negative values for *R1*, which is not possible. In some rare cases when that root does give positive numbers, the numbers are too large and are well above the cell radius, which is not possible. Hence, when the quadratic equation in *R1* is obtained in by

$$aR_1^2 + bR_1 + c = 0 \qquad \textbf{(B-12)}$$

only the following root should be considered for cellular PL.

$$R_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \qquad \textbf{(B-13)}$$

It is interesting to note that the ambiguities in Fang's and Chan's algorithms are essentially the same. If we make wrong choices in both algorithms for a given case, the same results are given by both algorithms.

In [64], Chan and Ho present a version of their algorithm that can take advantage of redundant measurements (four or more sensors for a 2D system). The simulation results in [64] show that this method clearly outperforms or performs at least as well as other algorithms in all cases. Chang and Ho give another version of their algorithm for the case when the receivers are arranged in a linear fashion and show that it is mathematically equivalent to Carter's beam forming method [74].

When Chan's method is compared with the other two algorithms considered, it might be the best choice for solving hyperbolic equations. It is an exact solution that is better than the Taylor-series method, which is iterative and has

the risk of convergence to local minima. When compared with Fang's method, it can take advantage of redundant measurements, if available, whereas Fang's method cannot. Hence, the Chan's method is the best available option for this dissertation to solve hyperbolic equations for wireless positioning systems.

References

[1] A. Balachandran et al., "Characterizing User Behaviour and Network Performance in a Public Wireless LAN" Proc. ACM SIGMETRIC, pp.195-205, June 2002.

[2] M. Hazas, J. Scott and J. Krumm, "Location-Aware Computing Comes of Age", IEEE Computer, Vol. 37, no. 2, pp. 95-97, Feb 2004.

[3] J. Hightower and G. Borriello, "Location Systems for Ubiquitous Computing", IEEE Computer, Vol. 34, pp. 57-66, 2001.

[4] ESRI, "GIS Technology and Applications for the Fire Service", ESRI White Paper, Mar 2006.

[5] M. Youssef et al., "WLAN Location Determination via Clustering and Probability Distributions", Proc. IEEE PerCom2003, Mar 2003.

[6] M. Kanaan and K. Pahlavan, "CN-TOAG: A New Algorithm for Indoor Geolocation", Proc. IEEE PIMRC'04, Vol.3, pp.1906-1910, Sep 2004.

[7] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai, "IEEE 802.11 Wireless Local Area Network", IEEE Communications Magazine, Vol.35, Issue.9 pages 116-126, 1997

[8] B. Bing, "High-Speed Wireless ATM and LANs", Artech House, 2000.

[9] IEEE 802.11 WG. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Standard 802.11, 1999.

[10] O. Tickoo and B. Sikdar, "On the Impact of IEEE 802.11 MAC on Traffic Characteristics", IEEE Journal on Selected Areas in Communication, Vol.21, No.2, pp.189-203, Feb 2003.

[11] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function", IEEE Journal on Selected Areas in Communications, Vol.18, pp.535-547, March 2000.

[12] M. Ghassemian and A. H. Aghvami, "Comparing different Handoff Schemes in IP based Micro-Mobility Protocols", Proceedings of Information Society Technologies Conference, Nov. 2002.

[13] N. D. Tripathi et al., "Radio Resource Management in Cellular Systems", Kluwer Academic Publishers, 2002.

[14] D. Wong and T. J. Lim, "Soft Handoffs in CDMA Mobile Systems", IEEE Trans. on Personal Communications, vol.4, No.6, pp.6-17, Dec 1997.

[15] V. Hector and K. Gunnar, "Techniques to reduce IEEE 802.11b MAC layer handover time", Technical Report, Royal Institute of Technology, April 2003.

[16] M. R. Jeong, F. Watanabe, T. Kawahara, "Fast Active Scan for Measurement and Handoff", Contribution to IEEE802, 11 May 2003.

[17] IEEE P802.11F/D: Inter-Access-Point Protocol (IAPP). IEEE 802.11f Draft Standard, Jan 2003.

[18] P. Chatzimisios, V. Vitsas and A. C. Boucouvalas, "Throughput and Delay Analysis of IEEE 802.11 Protocol", Tech Report, Bournemouth University, UK 2002.

[19] H. Harada and R. Prasad, "Simulation and Software radio for mobile communication", Artech House 2002.

[20] "MATLAB and SIMULINK", http://www.mathworks.com

[21] M. Hata, "Empirical formula for propagation loss in land mobile radio services", IEEE Trans. Veh. Technol., vol. 29, pp. 317–325, Aug. 1980.

[22] K. W. Kolodziej and J. Hjelm, "Local Positioning Systems: LBS Applications and Services", CRC, May 2006.

[23] H. S. Cobb, "GPS Pseudolites: Theory, Design, and Applications." A Ph.D dissertation, Stanford University, 1997.

[24] Z. Biacs, G. Marshall, M. Meoglein, and W. Riley, "The Qualcomm/SnapTrack Wireless-Assisted GPS Hybrid Positioning System and Results from Initial Commercial Deployments", Proc. IOS GPS, pp. 378-384, 2002.

[25] BWCS, "The Last Known Location of E-OTD", BWCS White Paper, Oct 2002.

[26] J. A. Tauber, "Indoor Location Systems for Pervasive Computing", MIT Report, Aug 2002.

[27] N. Hashimoto et al., "Assets Location Management Solution Based on the Combination of SmartLocator and RFID", NEC Technical Journal, Vol. 1, pp. 92-96, May 2006.

[28] R. Want, A. Hopper, V. Falco, and J. Gibbons, "The Active Badge Location System", ACM Trans. On Information Systems, Vol.10, no.1, pp. 91-102, Jan 1992.

[29] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, "The Anatomy of a Context-Aware Application", Proc. ACM/IEEE MobiCom'99, pp.59-68, Aug 1999.

[30] P. Bahl et al, "RADAR: An In-Building RF-Based User Location and Tracing System", Proc. Infocom2000, pp.775-784, Mar 2000.

[31] L. F. M. Moraes, B. A. A. Nunes, "Calibration-Free WLAN Location System Based on Dynamic Mapping of Signal Strength", Proc. ACM MobiWAC'06, pp.92-99, Oct 2006.

[32] Y. Hong, M. Shin and H. Kim "Consideration of FMIPv6 in 802.11 networks" IEEE 802.11 Internet draft, June 2003.

[33] M. Shin, A. Mishra and W. Arbaugh, "Improving the Latency of 802.11 Hand-offs using Neighbor Graphs", Proc. ACM Mobisys 2004, pp.70-83, June 2004.

[34] A. Mishra et al., "Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network", Proc. IEEE INFOCOM, Vol.1, pp.351-361, March 2004.

[35] S. Pack, H. Jung, T. Kwon and Y. Choi, "A Selective Neighbor Caching Scheme for Fast Handoff in IEEE 802.11 Wireless Networks", Proc. IEEE ICC, Vol.5, pp.3599-3603, May 2005.

[36] S. Shin, A. Rawat, and H. Schelzrinne, "Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs" Proc. ACM MobiWac, pp.19-26, October 2004.

[37] S. Pack and Y. Choi, "Fast Inter-AP Handoff using Predictive-Authentication Scheme in Public Wireless LAN", Proceedings of IEEE International Conference on Networking, pp. 15-26, August 2002.

[38] P. Bahl, A. Adya, J. Padhye, A. Wolman, "Reconsidering Wireless Systems with Multiple Radios", Proc. ACM Sigcomm Computer Comunications Review, Vol. 34, No. 5, pp.39-46, Oct 2004.

[39] V. Brik, A. Mishra, S. Banerjee, "Eliminating Handoff Latencies in 802.11 WLANs using Multiple Radios: Application, Experience, and Evaluation", Proc. ACM IMC 2005, pp. 299-304, Oct 2005.

[40] T. Manodham, L. Loyola, G. Atoche, M. Hayasaka and T. Miki, "A Seamless Handoff Scheme with new AP Module for Wireless LANs Support VoIP", in IEEE International Symposium on Applications and the Internet, SAINT 2006, pp. 253-258, January 2006.

[41] T. Manodham and T. Miki, "A Novel AP for Improving the Performance of Wireless LANs Supporting VoIP", Journal of Networks, Vol. 1, Issue 4, pp. 41-48, Aug 2006.

[42] S. Kim, C. Kang and K. Kim, "An adaptive handover decision algorithm based on the estimating mobility from signal strength measurements", Proc. IEEE VTC-Fall, Vol.2, pp.1004-1008, Sept 2004.

[43] T. S. Rappaport, "Wireless Communications: Principles and Practice (2nd Edition)", Prentice Hall PTR, Upper Saddle River, New Jersey, Dec 2001.

[44] Y. Kinoshita et al, "Advanced Handoff Control Using Fuzzy Inference for Indoor Radio System", Proc. IEEE VTC'92, Vol.2, pp. 649-653, May 1992.M. Hazas, J. Scott and J. Krumm, "Location-Aware Computing Comes of Age", IEEE Computer, Vol.37, no.2 pp.95-97, Feb 2004.

[45] S. Wu and B. Razavi, "A 900-MHz/1.8-GHz CMOS receiver for dual-band applications," IEEE J. Solid-State Circuits, vol. 33, pp. 2178-2185, December 1998.

[46] J. Tham et al., "A 2.7V 900-MHz dual-band transceiver IC for digital wireless communication," IEEE J. Solid-State Circuits, vol. 34, pp. 286-291, March 1999.

[47] J. Imbornone, J. Mourant, and T. Tewksbury, "Fully differential dual-band image reject receiver in SiGe BiCMOS," in IEEE RFIC Symp. Dig., pp. 147-150, June 2000.

[48] A. A. Abidi, "Direct-conversion radio transceivers for digital communication," IEEE J. Solid-State Circuits, vol. 30, pp. 1399-1410, December 1995.

[49] V. Erven, "Modular RF Antenna and Filter System for Dual Radio WLAN Access Points," United States Patent, No. US-6961596, November 2005.

[50] M. Zannoth et al., "A Highly Integrated Dual-Band Multimode Wireless LAN Transceiver," IEEE J. Solid-State Circuits, vol. 39, pp. 1191-1195, July 2004.

[51] Engim, Inc., EN-3001 Intelligent Wideband WLAN Technology, http://www.engim.com

[52] OPNET Modeler version 10.5 with wireless module, WLAN MAC process model. http//www.opnet.com.

[53] Daniel Collins, "Carrier Grade Voice over IP, 2nd Ed", MGraw-Hill, September 2002.

[54] A. Smailagic and D. Kogan, "Location Sensing and Privacy in a Context-Aware Computing Environment", IEEE Wireless Communications, Vol.9, no.5, pp.10-17, Oct 2002.

[55] Ekahau, Inc., "Ekahau Positioning Engine 4.0", http://www.ekahau.com/

[56] R. Yamasaki et al., "TDOA Location System for IEEE 802.11b WLAN", Proc. IEEE WCNC'05, pp.2338-2343, March 2005.

[57] T. Manodham, L. Loyola and T. Miki, "A Novel Wireless Positioning System for Seamless Internet Connectivity based on the WLAN Infrastructure", Springer Journal on Wireless Personal Communications, Dec 2007.

[58] A. H. Sayed, "Fundamentals of Adaptive Filtering", John Wiley & Sons, Jun 2003.

[59] A. Alloum et al., "Parameters Nonlinear Identification for Vehicle Model", Proc. IEE International Conference on Control Application, Hartford, Ct, Oct 1997.

[60] R. Kalman, "A new approach to linear filtering and prediction problems", Trans. ASME, J. Basic Eng. 82D, pp. 35-45, 1960.

[61] I. Guvenc et al., "Enhancements to RSS based indoor Tracking Systems Using Kalman Filters", Proc. International Signal Processing Conference and Global Signal Processing Expo, 2003.

[62] J. C. Eidson, "Measurement, Control and Communication Using IEEE 1588", Springer, Apr 2006.

[63] X. Li and K. Pahlavan, "Super-resolution TOA estimation with diversity for indoor geolocation", IEEE Trans. On Wireless Communications, Vol. 3, pp. 224-234, Jan 2004.

[64] Y. T. Chan and K. C. Ho, "A Simple and Efficient Estimator for Hyperbolic Location", IEEE Transactions on Signal Processing, vol. 42, no. 8, pp. 1905-1915, August 1994.

[65] L.A. Zadeh, Fuzzy Sets, Information and Control, 1965

[66] L.A. Zadeh, Outline of A New Approach to the Analysis of of Complex Systems and Decision Processes, 1973

[67] L.A. Zadeh, "Fuzzy algorithms," Info. & Ctl., Vol. 12, pp. 94-102, 1968.

[68] W. H. Foy, "Position-Location Solutions by Taylor-Series Estimation", IEEE Transactions on Aerospace and Electronic Systems, vol. AES-12, pp. 187-194, March 1976.

[69] D. J. Torrieri, "Statistical Theory of Passive Location Systems", IEEE Transactions on Aerospace and Electronic Systems, vol. AES-20, no. 2, pp. 183-198, March 1984.

[70] B. Friedlander, "A Passive Localization Algorithm and Its Accuracy Analysis", IEEE Journal of Oceanic Engineering, vol. OE-12, no. 1, pp. 234-244, January 1987.

[71] H. C. Schau and A. Z. Robinson, "Passive Source Localization Employing Intersecting Spherical Surfaces from Time-of-Arrival Differences", IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. ASSP-35, no. 8, pp. 1223-1225, August 1987.

[72] J. O. Smith and J. S. Abel, "The Spherical Interpolation Method for Source Localization", IEEE Journal of Oceanic Engineering, vol. OE-12, no. 1, pp. 246-252, January 1987.

[73] J. S. Abel and J. O. Smith, "The Spherical Interpolation Method for Closed-Form Passive Localization Using Range Difference Measurements", in Proc. ICASSP-87, pp. 471-474, Dallas, TX, 1987.

[74] G. C. Carter, "Time Delay Estimation for Passive Sonar Signal Processing", IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. ASSP-29, no. 3, pp. 463-470, June 1981.

[75] W. R. Hahn and S. A. Tretter, "Optimum Processing for Delay-Vector Estimation in Passive Signal Analysis", IEEE Transactions on Information Theory, vol. IT-19, no. 5, pp. 608-614, September 1973.

[76] W. R. Hahn, "Optimum Signal Processing for Passive Sonar Range and Bearing Estimation", Journal of Acoustical Society of America, vol. 58, pp. 201-207, July 1975.

[77] J. S. Abel and J. O. Smith, "Source Range and Depth Estimation from Multipath Range Difference Measurements", IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 37, no. 8, pp. 1157-1165, August 1989.

[78] P. Stoica and A. Nehorai, "MUSIC, Maximum Likelihood, & Cramer-Rao Bound", Proc. IEEE, vol. 57, no. 8, pp. 1408-1418, August 1969.

[79] T. M. Cover and J. A. Thomas, Elements of Information Theory, Wiley, New York, 1991.

[80] H. Stark and J. W. Woods, Probability, Random Processes and Estimation Theory for Engineers, Prentice-Hall, Inc., 2nd edition, 1994.

[81] J. O. Smith and J. S. Abel, "Closed-Form Least-Squares Source Location Estimation from Range-Difference Measurements", IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. ASSP-35, no. 12, pp. 1661-1669, December 1987.

[82] J. S. Abel, "A Divide and Conquer Approach to Least-Squares Estimation", IEEE Transactions on Aerospace and Electronic Systems, vol. 26, pp. 423-427, March 1990.

[83] S. Bancroft, "An Algebric Solution of the GPS Equations", IEEE Transactions on Aerospace and Electronic Systems, vol. AES-21, pp. 56-59, January 1985.

[84] D. L. Nicholson, "Multipath Sensitivity of a Linearized Algorithm Used in Time-Difference-of-Arrival Location Systems", Digest of International Electrical and Electronics Conference and Exposition, 1973, Paper No. 73253.

[85] D. L. Nicholson, "Multipath and Ducting Tolerant Location Techniques for Automatic Vehicle Location Systems", in IEEE Vehicular Technology Conference 1976, pp. 151-154, March 1976.

[86] B. T. Fang, "Simple Solutions for Hyperbolic and Related Fixes", IEEE Transactions on Aerospace and Electronic Systems, vol. 26, no. 5, pp. 748-753, September 1990.

[87] IEEE, "Draft 5 Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," IEEE Draft 802.11f/D5, January 2003.

[88] A. Mishra, M. Shin and W. Arbaugh "An empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process", Technical Report, University of Maryland Department of Computer Science, September 2002.

[89] A. Mishra, M. Shin and W. Arbaugh, "Improving the Latency of 802.11 Hand-offs using Neighbor Graphs", Contribution to IEEE 802, May 2003.

[90] M. Shin, A. Mishra, W. Arbaugh, I. Lee and K. Jang, "Improving the latency of the Probe Phase during 802.11 Handoff", Doc. IEEE 802.11-03/417r2, May 2003.

[91] N. D. Tripathi, J. H. Reed and H. F. Vanlandingham, "Radio Resource Management in Cellular Systems", Kluwer Academic Publishers, June 2001.

[92] Y. Suh and C. Jun, "Efficient Wireless LAN MAC Protocols for Ad-hoc Networks", IEICE Trans. Commun., Vol.E84-B, pp.595-604, March 2001.

[93] S. Pack and Y .Choi, "Fast Handoff Scheme based on Mobility Prediction in Public Wireless LAN Systems", IEE Proceedings Communications, Vol.151, pp.489-495, October 2004.

[94] K. Sato, M. Katsumoto, and T. Miki, "Source mobility support multicast (SMM)", IPSJ Journal, Vol. 45, pp.412-424, 2004.

[95] R. Koodli, "Fast Handovers for Mobile IPv6", Internet Draft draft-ietf-mobileip-fast-mipv6-08.txt, Internet Engineering Task Force (IETF), October 2003.

[96] T. S. Rappaport, "Wireless Communications", Prentice Hall PTR, 2002.

[97] C. S. et al., "3G Wireless Networks", McGraw-Hill Telecom, 2002.

[98] M. S. Gast, "802.11 wireless networks, the definitive guide", O'Reilly, USA, April 2002.

[99] Y. Bejerano, S. Han and L. Li, "Fairness and Load Balancing in Wireless LANs Using Association Control", Proc. ACM MobiCom'04, pp.315-329, September 2004.

[100] I. Shin and C. Lee, "A QoS Guaranteed Fast Handoff Algorithm for Wireless Local Area Network Environments", IEICE Trans. Commun., Vol.E87-B, no.9, pp.2529-2536, Sep 2004.

[101] H. Chaouchi and G. Pujolle, "A New Handover Control in the Current and Future Wireless Networks", IEICE Trans. Commun., Vol.E87-B, no.9, pp.2537-2547, Sep 2004.

[102] Y. Sakai et al., "Mismatch of Packet Recovery Mechanisms for Bit Error and Handover in Wireless TCP", IEICE Trans. Commun., Vol.E87-B, no.9, pp.2626-2633, Sep 2004.

[103] D. Pandya et al, "Indoor Location Estimation Using Multiple Wireless Technologies", Proc. IEEE PIMRC2003, Sep 2003

[104] T. Roos et al., "A Probabilistic Approach to WLAN User Location," Int'l Journal of Wireless Information Networks, vol.9, pp.155-164, Jul. 2002.

[105] K. Kaemarungsi et al., "Modeling of Indoor Positioning Systems Based on Location Fingerprinting," in Proc. IEEE Infocom2004, May 2004.

[106] G. J.M. Janssen, and R. Prasad, "Propagation Measurements in an Indoor Radio Environment at 2.4 GHz, 4.75 GHz and 11.5 GHz," Proc. IEEE VTC, 1992, pp. 617–620, May 1992.

[107] Y. Chen and H. Kobayashi, "Signal Strength Based Indoor Geolocation," Proc. IEEE ICC2002, pp. 436-439, Apr 2002.

[108] A. M. Ladd et al, "Robotics-Based Location Sensing using Wireless Ethernet," Proc. MOBICOM2002, pp. 227-238, Sep 2002.

[109] McGraw Hill and Sybil P. Parker "McGraw Hill Dictionary of Scientific and Technical Terms, 6th Edition", McGraw Hill, Oct 2002.

[110] J. Schiller and A. Voisard, "Location-Based Services", Morgan Kaufmann, Apr 2004.

[111] M. Burton, "Channel overlap calculations for 802.11b networks," white paper, 2002, Cirond.

Acronyms

ACK	acknowledgment
AGC	automatic gain control
A-GPS	assisted global positioning system
AID	association identifier
AOA	angle of arrival
AP	access point
ATIM	announcement traffic indication message
ATM	Asynchronous Transfer Mode
B3G	Beyond 3G
BCC	binary convolutional code
BPSK	binary phase shift keying
BSS	basic service set
BSSID	basic service set identification
CCA	clear channel assessment
CCK	complementary code keying
CDMA	code division multiple access
CFP	contention-free period
CID	connection identifier
COO	cell of origin
CP	contention period
CRC	cyclic redundancy code

CS	carrier sense
CSMA/CA	carrier sense multiple access with collision avoidance
CTS	clear to send
CW	contention window
DA	destination address
DBPSK	differential binary phase shift keying
DCF	distributed coordination function
DCLA	direct current level adjustment
DFIR	diffuse infrared
DIFS	distributed (coordination function) interframe space
DLL	data link layer
DLOS	direct line-of-sight
DPSK	differential phase shift keying
DQPSK	differential quadrature phase shift keying
DS	distribution system
DSS	distribution system service
DSSS	direct sequence spread spectrum
DTIM	delivery traffic indication message
EIFS	extended interframe space
EIRP	equivalent isotropically radiated power
E-OTD	enhanced observed time difference of arrival
ESS	extended service set
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FCS	frame check sequence
FER	frame error ratio
FHR	frequent handoff region
FHSS	frequency-hopping spread spectrum

FIFO	first in first out
GFSK	gaussian frequency shift keying
GPRS	General Packet Radio Service
GPS	Global Positioning system
GSM	Global System for Mobile communications
HIPERLAN	high performance radio LANs
HR/DSSS	high rate direct sequence spread spectrum
IAPP	inter-access point protocol
IBSS	independent basic service set
ICI	interchip interference
IDU	interface data unit
IEEE	Institute of Electrical and Electronics Engineers
IFS	interframe space
IR	infrared
ISM	industrial, scientific, and medical
IV	initialization vector
LAN	local area network
LBS	location-based services
LLC	logical link control
LOS	line-of-sight
MAC	medium access control
MIB	management information base
MIMO	multiple-input multiple-output
MMPDU	MAC management protocol data unit
MPDU	MAC protocol data unit
MSDU	MAC service data unit
N/A	not applicable
NAV	network allocation vector

NGN	next generation network
OFDM	orthogonal frequency domain multiplexing
PC	point coordinator
PCF	point coordination function
PDU	protocol data unit
PHY	physical, physical layer
PIFS	point (coordination function) interframe space
PLCP	physical layer convergence protocol
PMD	physical medium dependent
PNC	proactive neighbor caching
PPDU	PLCP protocol data unit
PPM	pulse position modulation
PSDU	PLCP service data unit
QAM	quadrature amplitude modulation
QoS	quality of service
QPSK	quadrature phase shift keying
RA	receiver address
RF	radio frequency
RFID	radio frequency ID
RSADSI	RSA data security, Inc
RSS	received signal strength
RSSI	received signal strength index
RTS	request to send
RX	receive or receiver
SA	source address
SAP	service access point
SDU	service data unit
SFD	start frame delimiter

SIFS	short interframe space
SNR	signal to noise ratio
SS	station service
SSAP	source service access point
SSID	service set identifier
STA	mobile station
TA	transmitter address
TBTT	target beacon transmission time
TCP	transmission control protocol
TDOA	time difference of arrival
TIM	traffic indication map
TOA	time of arrival
TSF	timing synchronization function
TU	time unit
TX	transmit or transmitter
UDP	user datagram protocol
UMTS	universal mobile telecommunications system
VoD	video on demand
VoIP	voice over IP
W3C	World Wide Web Consortium
WAN	wide area network
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access
WEP	wired equivalent privacy
WG	working group
Wi-Fi	wireless fidelity
WiMAX	worldwide interoperability for microwave access
WLAN	wireless local area network

WPA	Wi-Fi Protected Access
WPS	wireless positioning system
WWW	World Wide Web

Publications

List of publications related to the dissertation

(1) Journal Papers

1. T. Manodham and T. Miki, "A Novel AP for Improving the Performance of Wireless LANs Supporting VoIP", Journal of Networks, Vol. 1, Issue 4, pp. 41-48, Aug 2006.

2. T. Manodham, L. Loyola and T. Miki, "A Novel Wireless Positioning System for Seamless Internet Connectivity based on the WLAN Infrastructure", International Journal on Wireless Personal Communications, Springer (in press).

3. T. Manodham, L. Loyola and T. Miki, "A Seamless Handoff Scheme with Access Point Load Balance for Real-Time Services Support in 802.11 Wireless LANs", IEICE Transactions on Communications (in press).

(2) International Conference Papers

4. T. Manodham, M. Hayasaka, S. Sugawara, M. Terada and T. Miki, "Novel Handover Scheme for Wireless LANs", Proceedings of the International Workshop on Modern Science and Technology, IWMST 2004, pp. 247-251, Hokkaido Japan, September 2004.

5. T. Manodham, L. Loyola, G. Atoche, M. Hayasaka and T. Miki, "A Novel Handover Scheme for Reducing Latency in WLANs", Proceedings of the

Vehicular Technology Conference, VTC2005 Fall, pp. 1141-1144, Texas USA, September 2005.

6. T. Manodham, L. Loyola, G. Atoche, M. Hayasaka and T. Miki, "A SMOOTH HANDOFF SCHEME FOR REAL-TIME SERVICES IN WIRELESS LANS", Proceedings of the Global Mobile Congress, GMC 2005, pp. 95-100, Chongqing China, October 2005.

7. T. Manodham, L. Loyola, G. Atoche, M. Hayasaka and T. Miki, "A Seamless Handoff Scheme with new AP Module for Wireless LANs Support VoIP", Proceedings of the International Symposium on Applications and the Internet, SAINT 2006, pp. 253-258, Arizona – USA, January 2006.

8. T. Manodham, M. Hayasaka and T. Miki, "A Novel Handover Scheme for Improving the Performance of WLANs based on IEEE802.11", Proceedings of the Asia Pacific Communication Conference, APCC 2006, 3B2, Busan Korea, August 2006.

(3) Domestic Conference Papers

9. T. Manodham and T. Miki, "Techniques to Reduce Handover Time on Wireless LANs", Proceedings of the 2004 IEICE General Conference, SB-9-7, Tokyo Japan, March 2004.

10. T. Manodham and T. Miki, "A Novel AP Module for Seamless Handoff in WLANs", Proceedings of the International Symposium on Photonics and Advanced Networks, ISPAN 2006, pp. 121, Tokyo Japan, January 2006.

11. T. Manodham, M. Hayasaka and T. Miki, "Wireless Positioning System Based on 802.11 WLAN Infrastructure using a Novel Access Point", Proceedings of the 2006 IEICE Society Conference, B-5-129, Kanazawa Japan, September 2006.

Author Biography

Thavisak Manodham was born in Houphan province, Laos P.D.R. on May 5, 1974. In 1996, he received his Bachelors of Electrical Engineering, specializing in Communications and Computers, with honors from the King Mongkut's Institute of Technology North Bangkok (KMITNB), Bangkok, Thailand. From 1996 to 2001, he worked with the Enterprise of Telecommunications Laos (ETL) as an administrator of Internet and Network Systems; then he worked for IT Project Planning as a senior researcher. He received his Masters of Information Technology from the University of Electro-Communications, Tokyo, Japan in 2004. He became a Ph.D. candidate of Information Technology at the Department of Electronic Engineering, University of Electro-Communications, Tokyo, Japan in April 2004.

Focusing on the performance of wireless local area networks, Manodham's research on wireless network technology examines roaming technology for wireless local area networks, and wireless positioning systems based on the WLAN infrastructure. His research interests include the medium access control and networking issues related to wireless communication systems and new wireless network architecture for advanced wireless network systems such as Wi-Fi and WiMAX.