2011

Loss Diagnosis and Indoor Position Location System based on IEEE 802.11 WLANs

Tian Zhou

Loss Diagnosis and Indoor Position Location System based on IEEE 802.11 WLANs

(Spine title: Loss Diagnosis and Indoor Localization using 802.11 WLANs)

(Thesis format: Monograph Article)

by

Tian ZHOU

Graduate Program
in
Engineering Science
Electrical and Computer Engineering

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Engineering Science

School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

Certificate of Examination

THE UNIVERSITY OF WESTERN ONTARIO
SCHOOL OF GRADUATE AND POSTDOCTORAL STUDIES
CERTIFICATE OF EXAMINATION

Chief Advisor:	**Examining Board:**
Dr. Xianbin Wang	Dr. Jean-Yves Chouinard
	Dr. Raveendra K. Rao
	Dr. Jayshri Sabarinathan

The thesis by
Tian ZHOU
entitled:
Loss Diagnosis and Indoor Position Location System based on IEEE 802.11 WLANs
is accepted in partial fulfillment of the
requirements for the degree of
Master of Engineering Science

Date: ____________________

Chair of Examining Board
Dr. Shaun Salisbury

Abstract

Wireless local area networks (WLANs) have been widely deployed to provide short range broadband communications. Due to the fast evolvement of IEEE 802.11 based WLAN standards and various relevant applications, many research efforts have been focused on the optimization of WLAN data rate, power and channel utilization efficiency. On the other hand, many emerging applications based on WLANs have been introduced. Indoor position location (IPL) system is one of such applications which turns IEEE 802.11 from a wireless communications infrastructure into a position location network. This thesis mainly focuses on data transmission rate enhancement techniques and the development of IEEE 802.11 WLAN based IPL system with improved locationing accuracy.

In IEEE 802.11 systems, rate adaptation algorithms (RAAs) are employed to improve transmission efficiency by choosing an appropriate modulation and coding scheme according to point-to-point channel conditions. However, due to the resource-sharing nature of WLANs, co-channel interferences and frame collisions cannot be avoided, which further complicates the wireless environment and makes the RAA design a more challenging task. As WLAN performance depends on many dynamic factors such as multipath fading and co-channel interferences, differentiating the cause of performance degradation such as frame losses, which is known as loss diagnosis techniques, is essential for performance enhancements of existing rate adaptation schemes. In this thesis, we propose a fast and reliable collision detection scheme for frame loss diagnosis in IEEE 802.11 WLANs. Collisions are detected by tracking changes of the signal-to-interference-and-noise-ratio (SINR) in IEEE 802.11 WLANs with a nonparametric order-based cumulative sum (CUSUM) algorithm for rapid loss diagnosis. Numerical simulations are conducted to evaluate the effectiveness of the proposed collision detection scheme.

The other aspect of this thesis is the investigation of an IEEE 802.11 WLAN based IPL system. WLAN based IPL systems have received increasing attentions due to their variety of potential applications. Instead of relying on dedicated locationing networks and devices, IEEE 802.11 WLAN based IPL systems utilize widely deployed IEEE 802.11 WLAN infrastructures and standardized wireless stations to determine the position of a target station in indoor environments.

In this thesis, a WLAN protocol-based distance measurement technique is investigated, which takes advantages of existing IEEE 802.11 data/ACK frame exchange sequences. In the proposed distance measurement technique, neither dedicated hardware nor hardware modifications is required. Thus it can be easily integrated into off-the-shelf commercial, inexpensive WLAN stations for IPL system implementation. Field test results confirm the efficacy of the proposed protocol-based distance measurement technique. Furthermore, a preliminary IPL system based on the proposed method is also developed to evaluate the feasibility of the proposed technique in realistic indoor wireless environments.

Acknowledgements

This research would not have been possible without the support of many people. I am heartily thankful to those people who helped me and inspired me during my research.

I could not express enough thanks to my advisor Dr. Xianbin Wang for his continuous guidance, support and wisdom throughout my education. It has been a true fortune and privilege to work with him.

I am grateful to Dr. Serguei Primak, Dr. Raveendra Rao and Dr. Hanif Ladak for those courses through which I learned a lot for improving my research in theoretical analysis, understanding of communication systems, and simulation works.

I am indebted to Dr. Weikun Hou and Dr. Viet-Ha Pham for their thorough proofreading of my manuscript and their valuable suggestions. Their instructions and guidance will benefit me for my future study and work all the time.

I wish to thank all my colleagues in our research group who have helped me over the last two years,

My deepest gratitude goes to my family for their support and encouragement during this journey.

Finally, I would like to dedicate this work to my girlfriend for her advices on my research and also for all her encouragements when I got frustrated.

Table of Contents

List of Tables

List of Figures

Acronyms

AARF	*Adaptive Auto Rate Fallback*
ACK	*Acknowledgement*
AP	*Access Point*
ARF	*Auto Rate Fallback*
BEB	*Binary Exponential Backoff*
CP	*Cyclic Prefix*
CRC	*Cyclic Redundancy Check*
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*
CTS	*Clear to Send*
CUSUM	*Cumulative Sum*
CW	*Contention Window*
DC	*Direct Current*
DCF	*Distributed Coordination Function*
DDP	*Dominant Direct Path*
DIFS	*DCF Inter-Frame Spacing*
DME	*Distance Measurement Error*
DP	*Direct Path*
FDP	*First Detected Peak*
GPS	*Global Positioning System*
ICMP	*Internet Control Message Protocol*
IFFT	*Inverse Fast Fourier Transform*
IFS	*Inter-Frame Spacing*
IP	*Internet Protocol*
IPL	*Indoor Position Location*
ISM	*Industrial, Scientific And Medical*
LOS	*Line-of-Sight*
MAC	*Media Access Control*
MMSE	*Minimum Mean Square Error*

MPDU	*MAC Protocal Data Unit*
MSE	*Mean Square Error*
NAV	*Network Allocation Vector*
NDDP	*Non-Dominant Direct Path*
NIC	*Network Interface Card*
NUDP	*Non Undetected Direct Path*
OFDM	*Orthogonal Frequency Division Multiplexing*
OS	*Operating System*
OTT	*One-way Trip Time*
P/S	*Parallel-to-Serial*
PCF	*Point Coordination Function*
PDF	*Probability Density Function*
PHY	*Physical*
PLCP	*Physical Layer Convergence Procedure*
PPDU	*PLCP Protocal Data Unit*
PSDU	*PLCP Service Data Unit*
QoS	*Quality of Service*
RAA	*Rate Adaptation Algorithm*
RSS	*Received Signal Strength*
RSSI	*Received Signal Strength Indicator*
RTS	*Ready-to-Send*
RTT	*Round Trip Time*
S/P	*Serial-to-Parallel*
SIFS	*Short IFS*
SINR	*Signal to Interference and Noise Ratio*
TOA	*Time of Arrival*
TSF	*Timing Synchronization Function*
UDP	*Undetected Direct Path*
U-NII	*Unlicensed National Information Infrastructure*
WLAN	*Wireless Local Area Network*
ZF	*Zero Forcing*

Chapter 1
Introduction

1.1 Background and Motivation

IEEE 802.11 wireless local area networks (WLANs) have become an essential access technique for flexible and economical broadband communications in both public venues and residential areas. As applications of IEEE 802.11 are getting more diverse, such as voice or video over IP are emerging in IEEE 802.11 WLANs, quality-of-service (QoS) requirements of IEEE 802.11 WLANs have been strictly bounded by multimedia communications in terms of frame losses. However, frame losses in IEEE 802.11 WLANs are inevitable due to vulnerability of hostile wireless channels, fast diagnosing the cause of a frame loss is a key component for efficient rate adaptation in real-time.

IEEE 802.11 networks generally experience two kinds of frame losses: the channel fading dominated and the frame collisions dominated. To reduce frame losses, most IEEE 802.11 wireless stations and access points (APs) have employed certain strategies, known as rate adaptation algorithms (RAAs), to adjust transmission parameters, such as transmission rate and power. However, without the capability of diagnosing the cause of frame losses, RAAs unduly decrease rates in response to both channel fading induced and collision induced frame losses. In this sense, such schemes cannot work effectively in collision dominated environments or in the presence of losses from channel fading together with collisions. Furthermore, decreasing transmission rate in the presence of collisions results in a longer transmission time, which may increase interferences and collisions, thereby reducing the transmission efficiency.

Motivated by the need of identifying collisions for frame loss diagnosis, a nonparametric order-based cumulative sum (CUSUM) algorithm based on the physical (PHY) layer signal-to-interference-and-noise ratio (SINR) is proposed in this thesis. Unlike other frame based loss diagnosis schemes which imply the occurrence of collisions according to frame losses statistics, the PHY layer SINR is a direct metric that represents the extent to which the received signal power exceeds the sum of noise plus interference at the receiver. Furthermore, recent studies have proven SINR to be the most appropriate metric for evaluating the quality of a wireless link [41]. Benefiting from the proposed algorithm, SINR is tracked at the PHY layer OFDM symbol level so that collisions can be detected with short delay and low false alarm probability, thereby providing a fast and reliable loss diagnosis to enhance current IEEE 802.11 rate adaptation mechanisms.

While transmission efficiency improvements have received extensive research attentions, WLAN location-based services have emerged due to the rapid increase in the adoption rate of IEEE 802.11 WLANs coupled with the availability of high quality infrastructures. Unlike solutions requiring a dedicated, independent infrastructure, researches on IEEE 802.11 WLAN localization techniques have facilitated the emergence of indoor position location (IPL) systems completely based on IEEE 802.11 infrastructures.

Although existing localization technologies, e.g., global positioning system (GPS), have numerous applications in outdoor areas, they do not perform properly in indoor areas [32]. Taking advantages of existing IEEE 802.11 WLAN infrastructures, IPL systems are aimed to determine the position of a wireless station without dedicated networks or devices. Moreover, IPL systems also play an important role in WLAN power and transmission adaptations [33], wireless ad-hoc network routing [22] [25] and wireless network securities [46].

This thesis presents a technique that mainly focuses on the distance measurement, which is one of the key steps for IPL system implementations. The goal of this research is to estimate the distance between two WLAN stations precisely using low-cost, commercial

WLAN stations without hardware modifications or additional hardware equipments. The proposed distance measurement technique is based on standard-compatible frame exchange sequences between two IEEE 802.11 stations, so that the cost and complexity of implementation can be reduced drastically.

1.2 Thesis Contributions

The main contributions of this thesis are summarized as follows:

- A collision detection algorithm for IEEE 802.11 WLANs is proposed to perform loss diagnosis based on PHY layer SINR measurements. Since SINR is a direct metric that indicates collisions, the algorithm is designed for fast collision detections with low false alarm probability, so that it can be further integrated into existing RAAs for loss diagnosis.

- A protocol-based distance measurement technique for IPL systems is presented. The presented approach utilizes the existing IEEE 802.11 network infrastructures and standard compatible frame exchange sequences (i.e. data/acknowledgement (ACK)) to measure the distance between two 802.11 wireless stations without additional hardware or hardware modifications.

- Field tests have been conducted to evaluate the presented protocol-based indoor distance measurement method using wireless stations with commercial IEEE 802.11 WLAN network interface cards (NICs) in realistic indoor scenarios. Furthermore, a preliminary IPL system is also implemented to prove availability of the proposed method in realistic environments.

1.3 Thesis Organization

The rest of the thesis is organized as follows:

In Chapter 2, the background knowledge of IEEE 802.11 standard is introduced. The standard specified OFDM-based PHY layer and media access control (MAC) layer are described in detail, including an introduction of the 802.11a/g transceiver structure and the CSMA/CA based distributed coordination function (DCF). Following this, existing RAAs for optimizing IEEE 802.11 MAC system performance are reviewed. An analysis of impairments of those RAAs demonstrates the necessity of collision detection schemes for enhancing RAA performances.

In Chapter 3, a collision detection algorithm based on PHY layer SINR is proposed to detect the occurrence of collisions during frame transmissions. Related works on loss diagnosis in IEEE 802.11 are first reviewed. Following this, the decision directed SINR estimation used in our collision detection scheme is introduced. With the estimated SINR, a nonparametric order-based cumulative sum (CUSUM) algorithm is employed to track SINR changes in real time for collision detections. Finally, simulation setups and results are presented to evaluate the efficacy of the proposed algorithm.

In Chapter 4, a protocol-based distance measurement method for IPL systems using IEEE 802.11 WLANs is presented. Several 802.11 WLANs based distance measurement approaches are reviewed first. Theoretical difficulties and practical implementation issues of protocol-based distance measurement method using commercial IEEE 802.11 WLAN NICs are discussed, followed by the monitor station aided round trip time (RTT) measurement for distance determination.

In Chapter 5, field tests are introduced to evaluate the protocol-based distance measurement technique based on IEEE 802.11 WLANs in realistic indoor environments. Configurations and test procedures are presented in detail. Following this, test results validate the efficacy of the proposed technique for IPL system implementations. Finally, conclusions are drawn and future works are discussed in Chapter 6.

Chapter 2

Introduction to IEEE 802.11 Wireless LANs

IEEE 802.11 denotes a set of WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee. It closely follows the open systems interconnection (OSI) reference model, which is a layered abstract description for communications and computer network protocol designs. The relationship between the IEEE 802.11 specified system model and the OSI reference model is shown in Figure 2.1. Services and protocols specified in the IEEE 802.11 are mapped to the data link layer and PHY layer of the seven-layer OSI networking reference model. IEEE 802.11 further splits the data link layer into two sublayers named logical link control (LLC) layer and MAC layer. The LLC layer hides different structures among IEEE 802 family members, thus making them transparent to upper layer applications. The MAC layer determines procedures to access the medium for data transmissions by performing corresponding configurations to the PHY layer. The PHY layer is the interface between the wireless medium and the MAC layer, which is dedicated to frame transmissions and receptions over the shared wireless medium between two or more stations. In the following, the IEEE 802.11 PHY and MAC layer will be introduced in detail in Section 2.1 and 2.2, respectively.

2.1 Physical Layer in IEEE 802.11

Three different PHY layer specifications for single input single output IEEE 802.11 WLAN systems, namely IEEE 802.11a [1], 802.11b [2], and 802.11g [4], are mainly deployed to

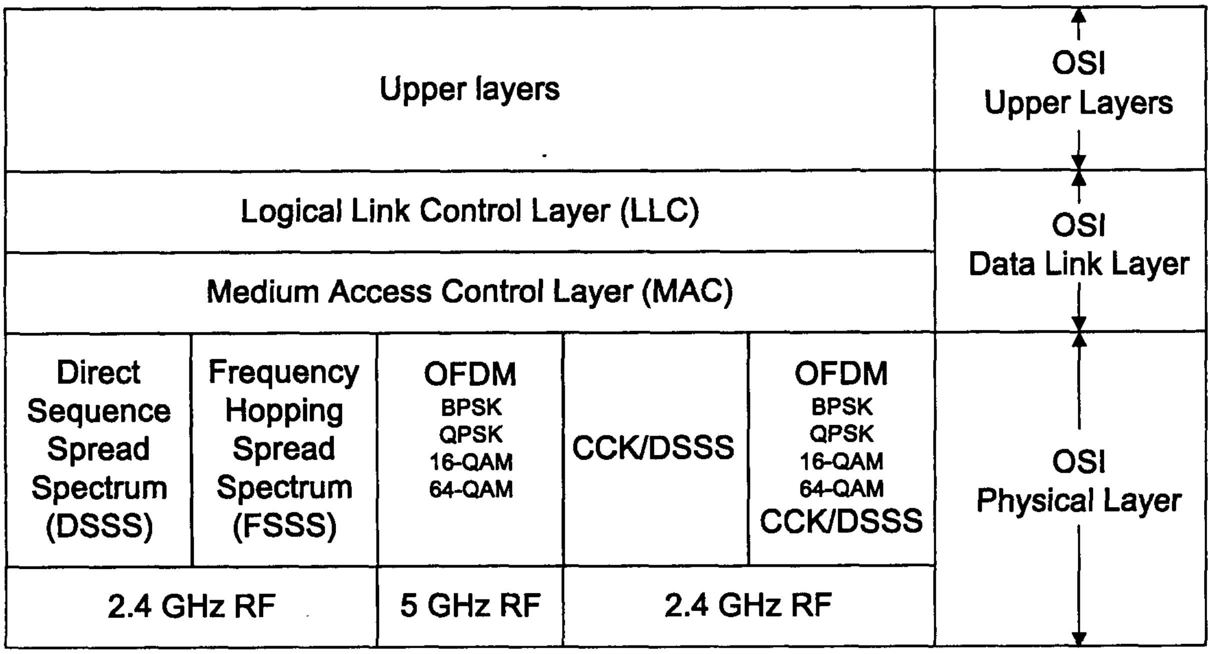

Upper layers
OSI Upper Layers
Logical Link Control Layer (LLC)
Medium Access Control Layer (MAC)
OSI Data Link Layer
Direct Sequence Spread Spectrum (DSSS)
Frequency Hopping Spread Spectrum (FSSS)
OFDM BPSK QPSK 16-QAM 64-QAM
CCK/DSSS
OFDM BPSK QPSK 16-QAM 64-QAM CCK/DSSS
OSI Physical Layer
2.4 GHz RF
5 GHz RF
2.4 GHz RF

Figure 2.1: The mapping from IEEE 802.11 model to OSI reference model.

provide short range broadband wireless communications.

The original 802.11 PHY specification [5] is based on direct sequence spread spectrum (DSSS) with 1 Mbps and 2 Mbps data rates in the 2.4GHz industrial scientific and medical (ISM) band. Later on, 802.11b PHY with additional rates of 5.5Mbps and 11Mbps was specified. To provide higher data rates (e.g., 5.5 Mbps and 11 Mbps), a complementary code keying (CCK) modulation scheme is employed in IEEE 802.11b. CCK is a variation on M-ary orthogonal keying modulation that uses I/Q modulation architecture with complex symbol structures. 802.11a PHY is standardized to utilize 5GHz unlicensed national information infrastructure (UNII) spectrum and provide higher data rates (6 to 54 Mbps) based on the orthogonal frequency division multiplexing (OFDM) technique. 802.11g PHY is designed to operates in 2.4 GHz ISM frequency band and supports all data rates in 802.11a PHY while retains the backward compatibility of IEEE 802.11b PHY.

The details of OFDM based PHY of IEEE 802.11 is introduced in the next section.

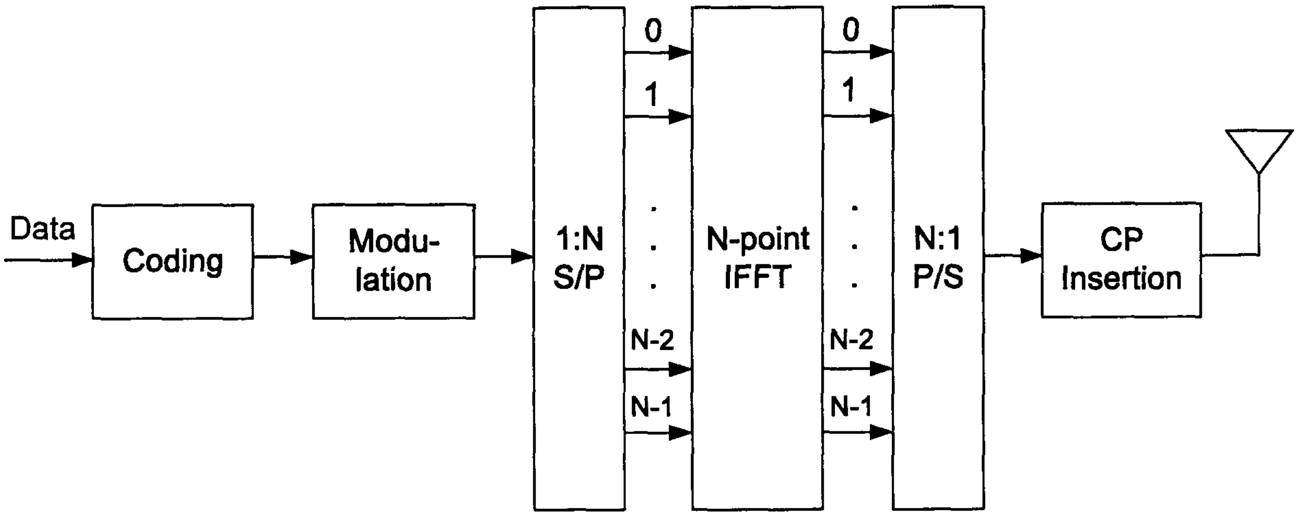


Figure 2.2: An OFDM transmitter structure.

2.1.1 OFDM Transceiver Structure in IEEE 802.11

OFDM is a wideband digital communication modulation technique in which high-rate data is transmitted in parallel via multiple closely-spaced narrowband orthogonal subcarriers. It has been adopted as a part of PHY layer specifications in IEEE 802.11a and IEEE 802.11g. In this section, typical OFDM transmitter and receiver structures are introduced.

Figure 2.2 depicts an OFDM transmitter structure. As it is shown, incoming data bits are encoded and then modulated as complex samples in the coding and modulation blocks respectively. Following these two blocks, the serial sample sequence is passed through a serial-to-parallel (S/P) converter.

To convert the paralleled frequency domain samples into time domain signals, an N-point IFFT is employed. Each sample at the kth IFFT bin is denoted as $X(k)$, where $0 \leq k \leq N-1$. Figure 2.3 illustrates an example of five subcarriers of one OFDM symbol, where the spectral peak of each subcarrier is located at nulls of all other subcarriers, thereby ensuring the orthogonality among subcarriers during the transmission.

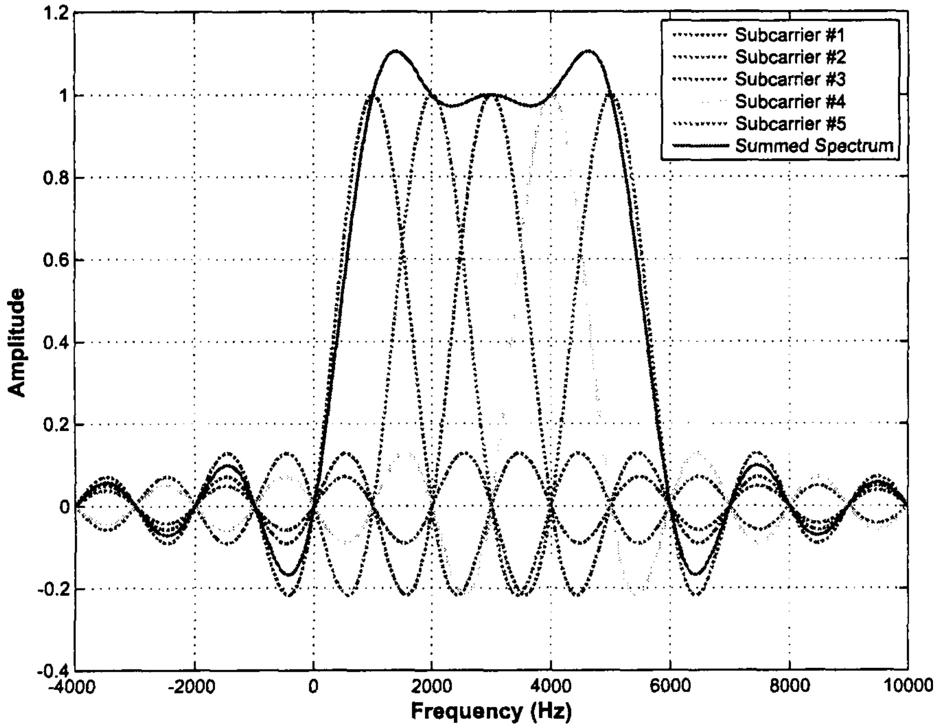


Figure 2.3: Five orthogonal OFDM subcarriers in the frequency domain.

The time domain OFDM data sample $s(m)$ after the IFFT block is expressed as

$$s(m) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X(k)\, e^{j\frac{2\pi k}{N}m}, \; 0 \leq m \leq N-1. \tag{2.1}$$

The data sample $s(m)$ is then passed through a parallel-to-serial (P/S) converter, forming a complex-valued OFDM data symbol. Prior to transmissions, each OFDM data symbol is prefixed with the last N_{cp} samples of itself, known as the cyclic prefix (CP) as shown in Figure 2.4. The insertion of CP extends the length of the original OFDM data symbol, allowing signals affected by multipath from previous symbol to degrade before the reception of the current symbol. The cyclic prefixed OFDM sample, $s'(m)$, can be expressed as

$$s'(m) = [s(N-N_{cp}), \cdots, s(N-1), s(0), \cdots, s(N-1)]. \tag{2.2}$$

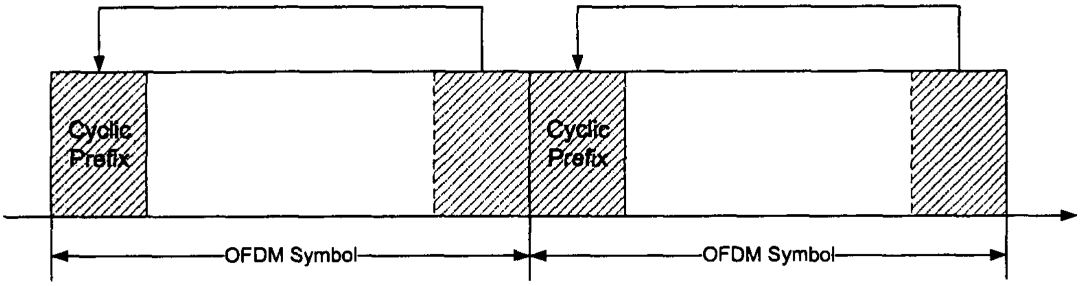


Figure 2.4: An example of CP insertion of OFDM symbols.

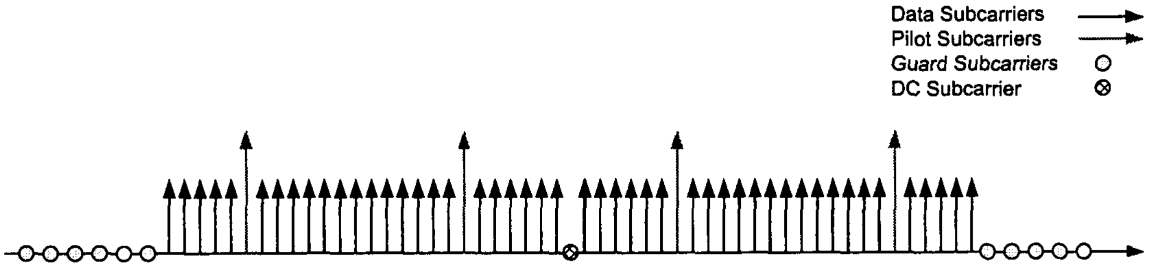


Figure 2.5: IFFT operation in OFDM based PHY of IEEE 802.11.

Table 2.1: OFDM based IEEE 802.11 a/g PHY modulation and coding schemes

Data Rates (Mbps)	Code Rate	Modulation	Bits per Subcarrier	Data Bits per OFDM Symbol
6	1/2	BPSK	1	24
9	3/4	BPSK	1	36
12	1/2	QPSK	2	48
18	3/4	QPSK	2	72
24	1/2	16-QAM	4	96
36	3/4	16-QAM	4	144
48	2/3	64-QAM	6	192
54	3/4	64-QAM	6	216

In IEEE 802.11 a/g, various modulation and coding schemes are supported by the OFDM based PHY layer to achieve different transmission rates. The availability of multiple transmission rates at the PHY layer enables IEEE 802.11 a/g to adaptively adjust modulation and coding schemes for transmissions according to channel conditions as well as QoS requirements. Detailed modulation and coding schemes supported by OFDM based PHY of IEEE 802.11 a/g are illustrated in Table 2.1.

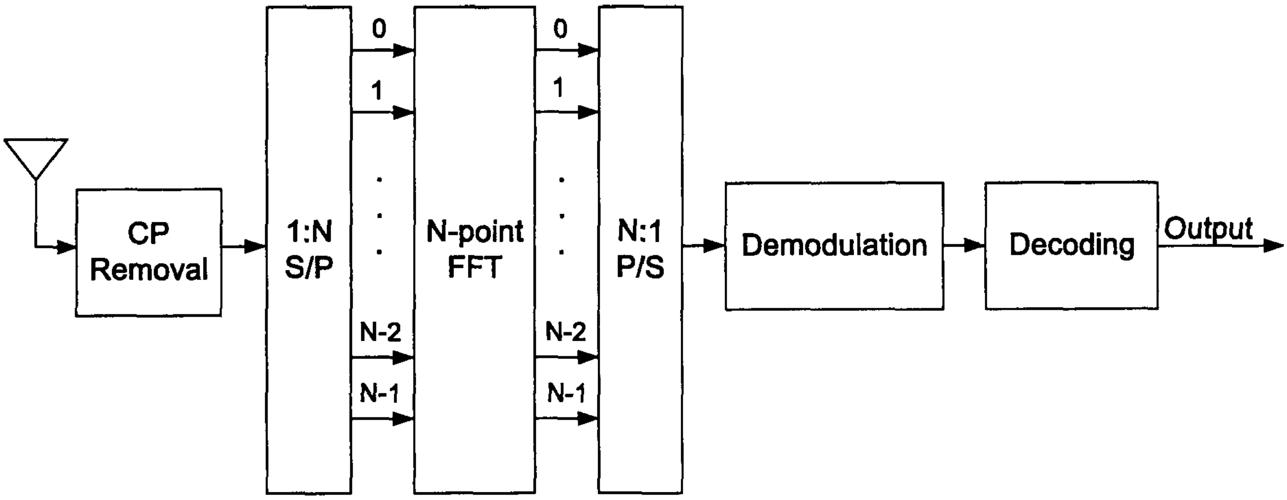


Figure 2.6: An OFDM receiver structure.

For each OFDM symbol in the PHY of IEEE 802.11 a/g, 64 subcarriers are employed. Among the 64 subcarriers, 48 are used for data transmission, 4 subcarriers are dedicated for pilots to make the coherent detection robust against frequency offsets and phase noise. The remaining 12 subcarriers serve as spectral guards to mitigate interferences between OFDM symbols in adjacent frequency bands except for the direct current (DC) subcarrier which is set to null to remove the DC offset. The subcarrier arrangement of one OFDM symbol in IEEE 802.11 a/g is depicted in Figure 2.5.

Fig. 2.6 illustrates the receiver structure of an OFDM system. After the receiving antenna, the sampled time domain signal $r(m)$ without CP is S/P converted and sent to FFT block. The frequency domain signal $R(k)$ over the kth subcarrier after FFT demodulation is given by

$$R(k) = \sum_{m=0}^{N-1} r(m) e^{-j\frac{2\pi k}{N}m}, \quad 0 \leq k \leq N-1. \tag{2.3}$$

Following this, $R(k)$ is P/S converted and the serial signal is then sent to the demodulation and decoding blocks for further processing.

A summary of PHY layer parameters of OFDM based IEEE 802.11 is presented in Table 2.2.

2.2 Media Access Control Layer in IEEE 802.11

In this section, MAC layer in IEEE 802.11 is introduced in detail. The IEEE 802.11 MAC specification defines two major coordination functions responsible for wireless media accesses, the point coordination function (PCF) and the distributed coordination function (DCF). The PCF is based on a centralized polling scheme, which requires stations to be polled even when they do not have data for transmission. In contrast to the PCF, the DCF provides a mechanism whereby stations in the network only access the channel upon data transmissions. The DCF is a mandatory channel access function and the primary MAC scheme in IEEE 802.11 WLANs [5].

To prevent collisions caused by simultaneous transmissions, DCF employs the contention-based carrier sense multiple access with collision avoidance (CSMA/CA) protocol for channel accesses. In DCF, two types of carrier sensing scheme are supported, the physical carrier sensing and the virtual carrier sensing.

The physical carrier sensing is where stations compare the energy presenting on the channel with a threshold to determine whether the medium is busy. Before transmitting a frame, the transmitter waits until the channel is idle for a duration equal to the DCF interframe space (DIFS) period. To further reduce transmission collisions, the transmitter randomly selects a backoff duration ranging from zero to the contention window (CW) size in

Table 2.2: PHY layer parameters in OFDM-based IEEE 802.11

Parameter	Value
Number of data subcarriers (N_{sc})	48
FFT size (N)	64
Number of pilot per subcarrier	4
OFDM symbol duration (T_s)	4 μs
CP length (μ)	0.8 μs (16 samples)
Subcarrier bandwidth	312.5 kHz
Channel bandwidth (B)	20 MHz

units of time slots (T_{slot}) before the transmission. If the channel is still idle after the backoff period expires, the station starts transmission immediately. The CW size initially starts at the minimum contention window size (CW_{min}) and grows exponentially after every frame retransmission until the maximum window size CW_{max} is reached. The backoff duration gives more priority (less backoff duration) to frames incurring fewer retransmissions than frames that have been retransmitted multiple times. Once a backoff duration is selected, the backoff counter is decremented every idle slot until the counter value reaches zero. When the backoff counter value reaches zero, a frame can be retransmitted or a new frame can be transmitted. If the channel becomes busy before the backoff counter value reaches zero, the backoff counter value is frozen and the counter is restarted after the channel becomes idle for at least a DIFS period.

Upon a frame reception, the CSMA/CA scheme requires the receiver to transmit an acknowledgement (ACK) frame after waiting for a short interframe space (SIFS) period indicating that the transmitted data frame was received intact. SIFS is the smallest frame space specified in IEEE 802.11 MAC. Since other stations require the channel to be idle for at least a DIFS period in order to commence frame transmission, SIFS is designed to give priority to communicating stations. Once a frame is transmitted, the transmitter expects an ACK frame within a time period equal to SIFS plus the ACK timeout period, *ACK_timeout*. The last transmitted frame is considered to be a frame loss if no ACK is received at the transmitter after *ACK_timeout* expired.

However, the hidden station problem in IEEE 802.11 WLANs poses a prominent challenge for the above mentioned CSMA/CA physical carrier sensing method. A hidden station is a potential interference sender in the transmission range of the receiver which cannot be detected by the sender. Figure 2.7 shows an example of a typical scenario where the hidden station problem occurs. In Figure 2.7, station B and station C are located at the far edge of the transmission range of station A, therefore both station B and C are able to sense the

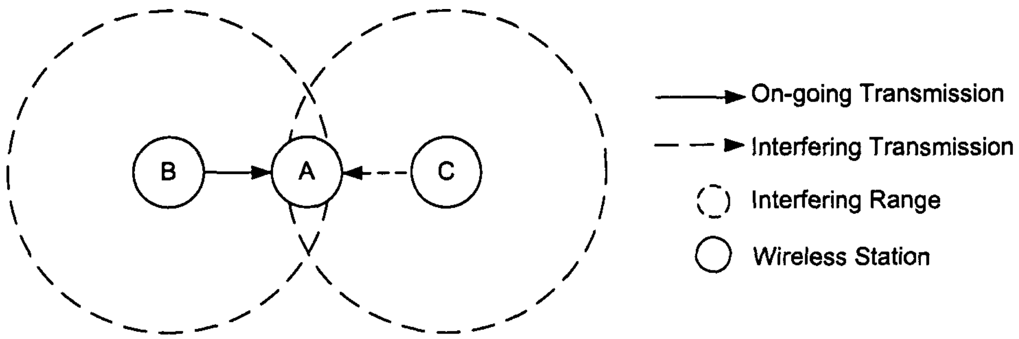


Figure 2.7: The hidden station problem in CSMA/CA.

presence of station A by physical carrier sensing of CSMA/CA. However, station B and C are not able to sense the presence of each other, thus these two stations are considered to be hidden from each other in this wireless network. When station B and C start their transmissions to station A simultaneously, collisions may occur at the intending receiver station A, causing severe transmission frame losses and performance degradation of the overall wireless network [53].

To solve the hidden station problem, the IEEE 802.11 specified an optional virtual carrier sensing mechanism, which allows two communicating stations to use request-to-send (RTS) and clear-to-send (CTS) frames respectively to notify other stations of their ongoing transmissions in conjunction with the CSMA/CA scheme. This mechanism is triggered as long as the MAC protocol data unit (MPDU) size (including the MAC payload, header and cyclic redundancy check (CRC)) exceeds a threshold (*RTS_threshold*). To start the RTS/CTS frame exchange, the intending transmitter sends an RTS frame to the intended receiver before actual data transmission to request permissions from intended receiver for transmissions. After the RTS frame reception, the intended receiver sends a CTS frame to the intending transmitter to allow the following data transmission from the intending transmitter. The RTS and CTS frame exchange in the wireless network allows stations in the transmission range of the intending transmitter and intended receiver to set their network allocation vector (NAV) to the value corresponding to the time which the communicating pair requires for data exchanges. NAV maintains a prediction of the medium busy time based on the duration value set by the RTS frame. With the NAV set, other stations in the range of the communicating pair withhold frame transmissions until the transmission terminates or their NAV expires.

To further clarify the above introduced procedures, a simplified flow chart of data frame transmission using CSMA/CA scheme is presented in Figure 2.8. Once a data frame is ready for transmission, the transmitter senses the channel with the physical carrier sensing technique. If the wireless channel is sensed busy, the transmitter performs random backoff and re-senses the channel after the backoff timer expires. Otherwise the transmitter starts to deliver the data frame if channel is sensed idle. In the case that the RTS/CTS handshake is enabled, an additional RTS frame is transmitted to the intended receiver as an indication of transmission request before actual data transmissions. The transmitter only starts the transmission upon the reception of the corresponding CTS frame from the intended receiver. If the hidden station problem occurs, only the RTS frame is affected by collisions resulted from transmissions from other interfering stations and may not be received properly at the intended receiver. Since the transmitter has to withhold the transmission until the CTS frame is received, when the transmitted RTS frame is lost, the transmitter will not perform further data frame transmissions, so that potential collisions to data frames at the intended receiver can be avoided.

The values of the previously mentioned MAC layer parameters of OFDM based IEEE 802.11 standards are summarized in Table 2.3.

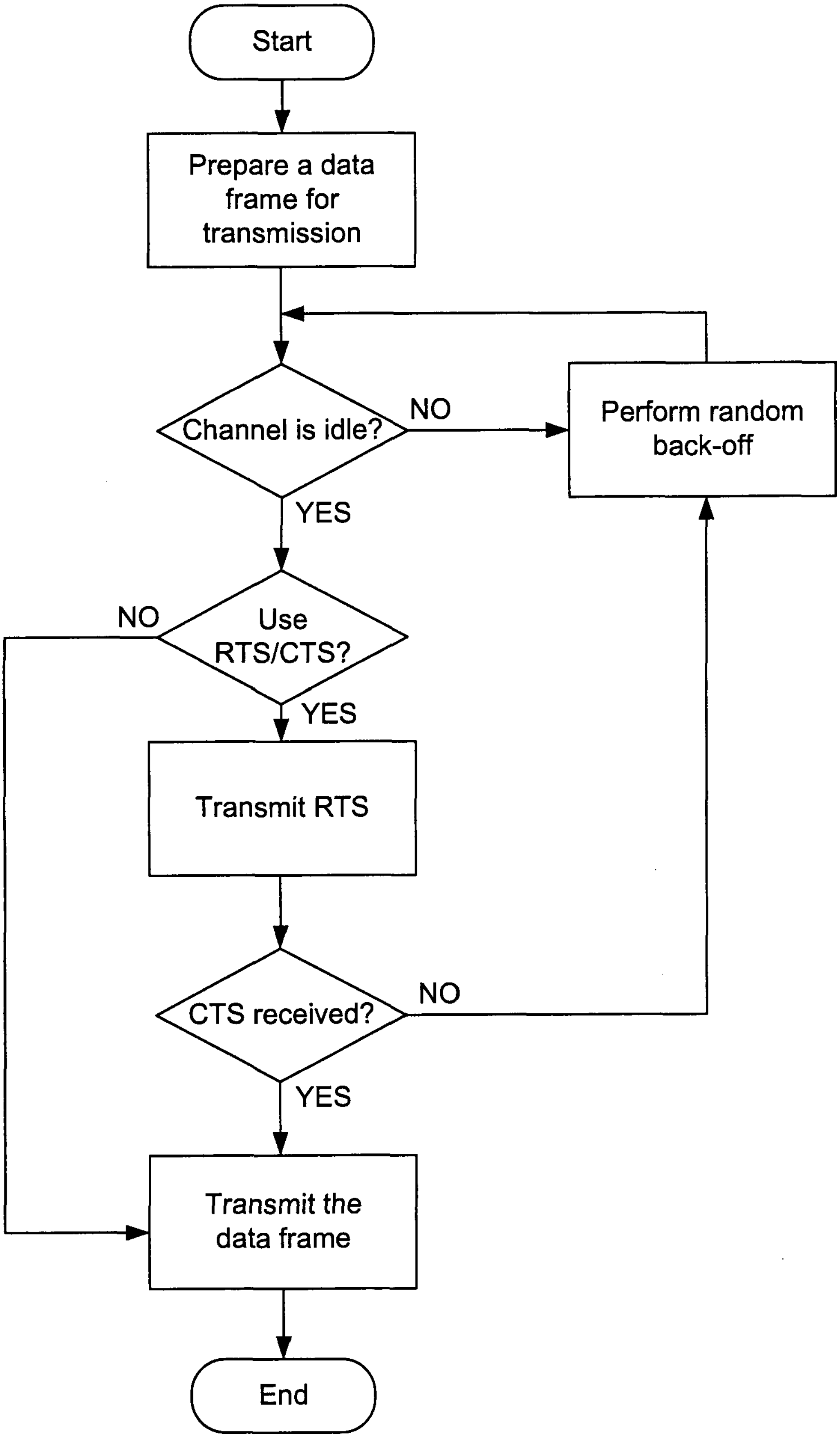


Figure 2.8: Flow chart of the CSMA/CA scheme.

Table 2.3: MAC layer parameter values of OFDM based IEEE 802.11

MAC Parameters	Values
DIFS	34 μs (IEEE 802.11a), 28 μs (IEEE 802.11g)
SIFS	16 μs (IEEE 802.11a), 10 μs (IEEE 802.11g)
T_{slot}	9 μs
CW_{min}	15
CW_{max}	1023
$ACK\_timeout$	$T_{ack} + T_{slot}$
$RTS\_threshold$	0-2304 Bytes
t_{symbol}	4 μs
L_{ack}	14 Bytes
$t_{preamble}$	16 μs

2.3 Review of Rate Adaptation Algorithms in IEEE 802.11

Although the MAC layer CSMA/CA based DCF provides a simple and fully distributed channel access mechanism for IEEE 802.11 WLANs, additional adaptation schemes are required to deal with the fundamental challenges for wireless communications, including transmissions on a shared medium and lossy wireless channel conditions, by adjusting transmission parameters [12] [15]. RAAs are such schemes designed for IEEE 802.11 wireless stations to select the best transmission rate under different channel conditions. The key challenge in RAA designs is that RAAs should be responsive to rapidly fluctuating wireless channels and accurately estimate channel conditions to determine the most suitable data transmission rate.

Various RAAs have been explored for IEEE 802.11 WLANs for proper data transmission scheme adaptations, the auto rate fallback (ARF) [23], for example, is one of the earliest RAAs commercially adopted by Lucent Wave-II wireless LAN adapters for IEEE 802.11 WLANs. ARF considers all frame losses as an indicator of channel conditions and adjusts transmission rates based on a constant threshold of consecutive successful transmissions. However, the constant threshold for rate adjustments causes two problems [26]. First, ARF cannot adapt effectively if channel conditions change quickly since it does not decrease the transmission until several consecutive failures have been accumulated. Second, after a fixed number of consecutive successful transmission, ARF attempts to increase transmission rate, which leads to periodical rate fluctuations. Other RAAs have also been proposed to enhance the performance of IEEE 802.11 WLANs. Adaptive auto rate fallback (AARF) [26] is proposed to tackle problems in ARF by adaptively adjusting the threshold for rate adaptations based on whether frame losses occur at a newly increased rate. A periodical transmission statistics based RAA, SampleRate [13], is adopted by Atheros chips in the MadWiFi project [28]. SampleRate randomly samples one of those rates whose lossless transmission time is less than the average transmission time of the rate in use every 10 frames. Using the rate with the smallest average transmission time, SampleRate seeks to achieve a better long-term average throughput.

The effectiveness of the above RAAs has been extensively evaluated under various wireless channel conditions when there is only one or sparse wireless stations in the network. However, in multiple-user environments where collisions present, several studies report that the performance of the above introduced RAAs degrades drastically or even misleads to wrong rate adaptation decisions because of the inability of diagnosing the causes of frame losses [15] [24] [55]. This is because rate decreasing upon frame losses does not increase the chance of successful transmissions in collision dominated environments. In fact, a lower data rate transmission covers a wider geographical range and occupies a longer transmission duration, which leads to more interferences and a higher collision probability. Consequently, congestions in the wireless network may be exacerbated [15].

Although the optional RTS/CTS handshake mechanism provided by IEEE 802.11 standards is designed to further reduce the probability of collisions, studies and field measurements have discovered that most wireless traffics in IEEE 802.11 WLANs are transmitted without RTS/CTS due to the significant amount of overhead introduced by the additional handshake procedure [42] [56]. Therefore, collisions are likely to occur in the environment with high wireless station density and it is of necessity to enable RAAs to detect collision induced frame losses so that the RTS/CTS mechanism can be adaptively enabled/disabled to limit the occurrence of collisions and filter only non-collision losses into the consideration for rate adjustments while maintaining low transmission overhead.

In order to provide a fast and reliable loss differentiation mechanism to assist current RAAs, a collision detection algorithm based on PHY layer signal-to-interference-and-noise ratio (SINR) rather than frame based transmission statistics is presented in next chapter.

2.4 Summary

In this chapter, the basic knowledge of IEEE 802.11 WLANs is introduced. In Section 2.1, the PHY layer of IEEE 802.11 WLANs is presented and the OFDM based IEEE 802.11 a/g transceiver structure as well as transmission and reception procedures are presented in detail. Following this, the IEEE 802.11 MAC layer is introduced in Section 2.2 focusing on the CSMA/CA based DCF and analysis of hidden station problems. Existing RAAs for system performance optimizations of IEEE 802.11 MAC are reviewed in Section 2.3, including the analysis of impairments of RAA designs and the necessity of collision detections in multi-user environments for RAA performance enhancement.

Chapter 3

Fast Collision Detections in IEEE 802.11 with Physical Layer SINR Monitoring

In IEEE 802.11 network, system performances are affected by various factors such as pathloss, multipath fading and co-channel interference. In order to accommodate such complicated and dynamic channel conditions, RAAs are commonly employed by IEEE 802.11 stations to adjust transmission parameters accordingly. However, as analyzed in Section 2.3 in Chapter 2, traditional RAAs adjust modulation and coding schemes primarily according to received signal strength or frame loss statistics, while the cause of performance degradation is not identified. Due to the open nature of wireless medium, frame loss may be caused by different factors such as multipath fading between the two point-to-point communicating stations, or co-channel interference induced by transmission collisions. Consequently, traditional RAAs without frame loss diagnosis may fail to work effectively in IEEE 802.11 networks, especially in the station-crowded environment with heavy traffic load and high transmission collision rate. To further enhance the system performance, different adaptation strategies are needed based on different causes of performance degradations. Therefore, a fast collision detection scheme that monitors the ongoing transmissions and diagnoses the cause of performance degradations is essential to effectively adjust the transmission parameters for system performance improvements.

Though there are a few efforts made in this area, fast and reliable collision detection schemes used to diagnose frame losses and maintain system QoS requirements to assist IEEE

802.11 RAAs during transmission are not well investigated.

In this chapter, a collision detection algorithm based on PHY layer SINR is proposed to detect the occurrence of collisions during frame transmissions. The proposed algorithm is designed to provide an additional ability of loss diagnosis for existing RAAs to handle different kinds of frame losses. By using SINR measurements from PHY layer, the algorithm can quickly detect collisions in symbol basis, thereby enhancing the speed and effectiveness of rate adaptations.

The rest of this chapter is organized as follows. Existing collision detection mechanisms for loss diagnosis in IEEE 802.11 WLANs are reviewed first. Following this, the decision directed SINR estimation used in our collision detection scheme is introduced. With the estimated SINR, a nonparametric order-based cumulative sum (CUSUM) algorithm is employed to track SINR changes in real time to detect collisions. Instead of using SINR values directly, this sequential nonparametric CUSUM algorithm use the order statistics of the SINR measurements to detect SINR changes. Therefore, no *a priori* distribution of SINR under interference or fading scenarios is required, which enhances the robustness of the proposed collision detection scheme in practical applications. Finally, simulation setups and results are presented to evaluate the efficacy of the proposed algorithm.

3.1 Research Motivations

In IEEE 802.11 WLANs, frame loss is one of the key criterions for network performance evaluations. There are multiple factors resulting in frame losses, such as pathloss, multipath fading and co-channel interference. Different responses therefore should be taken based on the cause of frame losses by adjusting transmission parameters accordingly to enhance system performance. For example, if a frame loss is caused by channel fading, PHY layer transmission parameters such as modulation coding schemes and transmit power should be adjusted for more robust frame deliveries. On the other hand, if frame losses are related to collisions, which result in severe co-channel interferences, the length of contention window should be doubled as suggested by the binary exponential backoff (BEB) scheme in IEEE 802.11 and colliding stations should back off and re-compete for another channel access to reduce the collision probability. In addition, the optional RTS/CTS handshake mechanism can be enabled to further reduce the probability of collisions in the wireless network.

Although various schemes have been explored for IEEE 802.11 WLANs to achieve adaptive transmissions, the development of collision detection schemes for frame loss diagnosis in IEEE 802.11 RAAs is still challenging. The difficulty is that existing WLAN NICs provide only binary feedbacks on frame transmissions and receptions. In other words, the driver and other upper layer software applications are only aware whether the last frame transmission or reception is successful or not, however the cause of the frame loss is not reported. As more and more applications, such as voice or video over IP are emerging in IEEE 802.11 WLANs, system requirements to the QoS become more challenging. Therefore, it is extremely important to diagnose the cause of a frame loss in real-time and adapt transmission accordingly to guarantee the QoS.

3.2 Related Works

Several studies have been focused on collision detections to improve the effectiveness of RAAs in device-intensive environments where frame losses are likely caused by a combination of collisions and channel fadings.

Loss-differentiating-ARF (LD-ARF) for IEEE 802.11 WLANs [34] is one notable algorithm proposed to introduce the ability of differentiating frame losses between channel fadings and collisions. The loss diagnosis in the scheme is performed by combining ARF with a loss-differentiating MAC [35]. Once the cause of frame loss is identified at the receiver, a specially designed "negative ACK" frame is employed to notify the sender of the cause of frame losses. However, this collision detection algorithm is based on the assumption that both the frame header and body are destroyed in collisions. Furthermore, this approach is not standard compatible because additional modifications to the frame structure are required.

Different from LD-ARF that requires modifications to the standard, other schemes, such as collision-aware rate adaptation (CARA) [24] and robust rate adaptation algorithm (RRAA) [52] have been proposed to address the collision detection problem in standard compatible manner by utilizing the optional RTS/CTS handshake mechanism. CARA enables RTS/CTS for data frame retransmissions to probe the channel when the previously transmitted data frame is lost. Once the retransmission of data frame with RTS enabled also fails, the loss of previous data frame is considered to be collision induced. To mitigate the overhead caused by using RTS/CTS frames, CARA suggests another collision detection mechanism in which a transmitting station switches its adapter to sense the channel immediately upon a transmission completion. If its transmission gets lost and the channel is sensed busy, the loss is attributed to collision without the need of enabling RTS/CTS handshakes. However, the busy channel sensed by the source station does not necessarily result in a collision at the destination station. Similarly to CARA, RRAA also relies on the use of RTS/CTS in loss diagnosis after a frame loss and further avoids collisions. RRAA presents an adaptive RTS (A-RTS) strategy to reduce possible collision losses. It implicitly assumes that a frame loss without RTS results from collisions. When a frame preceded by RTS is lost, or a frame without RTS succeeds, RRAA determines that channel fading causes the frame loss rather than collisions.

The philosophy employed by these algorithms is to conduct active tests or experiments by retransmitting or sending frames such as RTS to indicate the existence of a collision. However, these approaches require multiple transmissions and observations in frame basis to identify the cause of frame losses, thereby taking a long time to converge to adjust transmission parameters.

3.3 Decision Directed SINR Estimation

As the detection of frame losses relies on frame basis parity bit checking of the whole frame, such process will reduce the responsiveness of RAAs to varying channel conditions. To speed up the collision detection process, in this section, the PHY layer SINR is employed as a link quality indicator to detect the occurrence of collisions. SINR represents the extent to which the desired received signal power exceeds the sum of noise plus interference and has been considered to be the most appropriate metric for quantifying the link quality by recent studies [41] [49]. The definition of SINR is expressed as below

$$\mathrm{SINR} = \frac{S}{I + N_0}, \tag{3.1}$$

where S is the received power from desired signals, I is the co-channel interference power caused by collisions during frame receptions and N_0 is the AWGN introduced by the background thermal noise.

To present the proposed SINR based collision detection algorithm, an OFDM transmitter structure is introduced first. Figure 3.1(a) shows the block diagram of an IEEE 802.11 OFDM transmitter. Source data bits are first encoded and mapped to complex symbols $X(k), 0 \leq k \leq N-1$ over each subcarrier after the serial-to-parallel conversion. By transforming these complex symbols from frequency domain to time domain using IFFT, the corresponding baseband OFDM signal $s(m)$ can be expressed as

$$s(m) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X(k)\, e^{j\frac{2\pi k}{N}m},\ 0 \leq m \leq N-1. \tag{3.2}$$

Before the transmission of each OFDM symbol, CP is appended by copying the last part of useful data to the beginning.

Figure 3.1(b) depicts the corresponding IEEE 802.11 receiver supplemented with the proposed collision detection scheme. As shown in the figure, after the CP removal, the received baseband signal $r(m)$ is demodulated by FFT. The frequency domain signal over each subcarrier is given by

$$\begin{aligned} R(k) &= \sum_{m=0}^{N-1} r(m)\, e^{-j\frac{2\pi k}{N}m} \\ &= H(k)X(k) + N(k), \quad 0 \leq k \leq N-1, \end{aligned} \tag{3.3}$$

where $X(k)$ is the transmitted symbol and $N(k)$ is the AWGN with variance N_0 on the kth subcarrier, $H(k)$ is the corresponding complex channel gain.

As indicated in (3.3), each subcarrier experiences a flat fading channel with a complex channel gain $H(k)$, $k = 0, \cdots, N-1$ and simple one tap equalizer is normally employed to equalize the signal $R(k)$ as follows

$$X_{eq}(k) = G(k)R(k), \quad 0 \leq k \leq N-1, \tag{3.4}$$

where $X_{\mathrm{eq}}(k)$ is the equalized signal and $G(k)$ is the corresponding equalizer gain with $G(k) = \frac{H^*(k)}{\|H(k)\|^2}$ for zero forcing (ZF) equalizer or $G(k) = \frac{H^*(k)}{(\|H(k)\|^2 + N_0)}$ for minimum mean squared error (MMSE) equalizer. Perfect channel state information is assumed in the above equalization procedure.

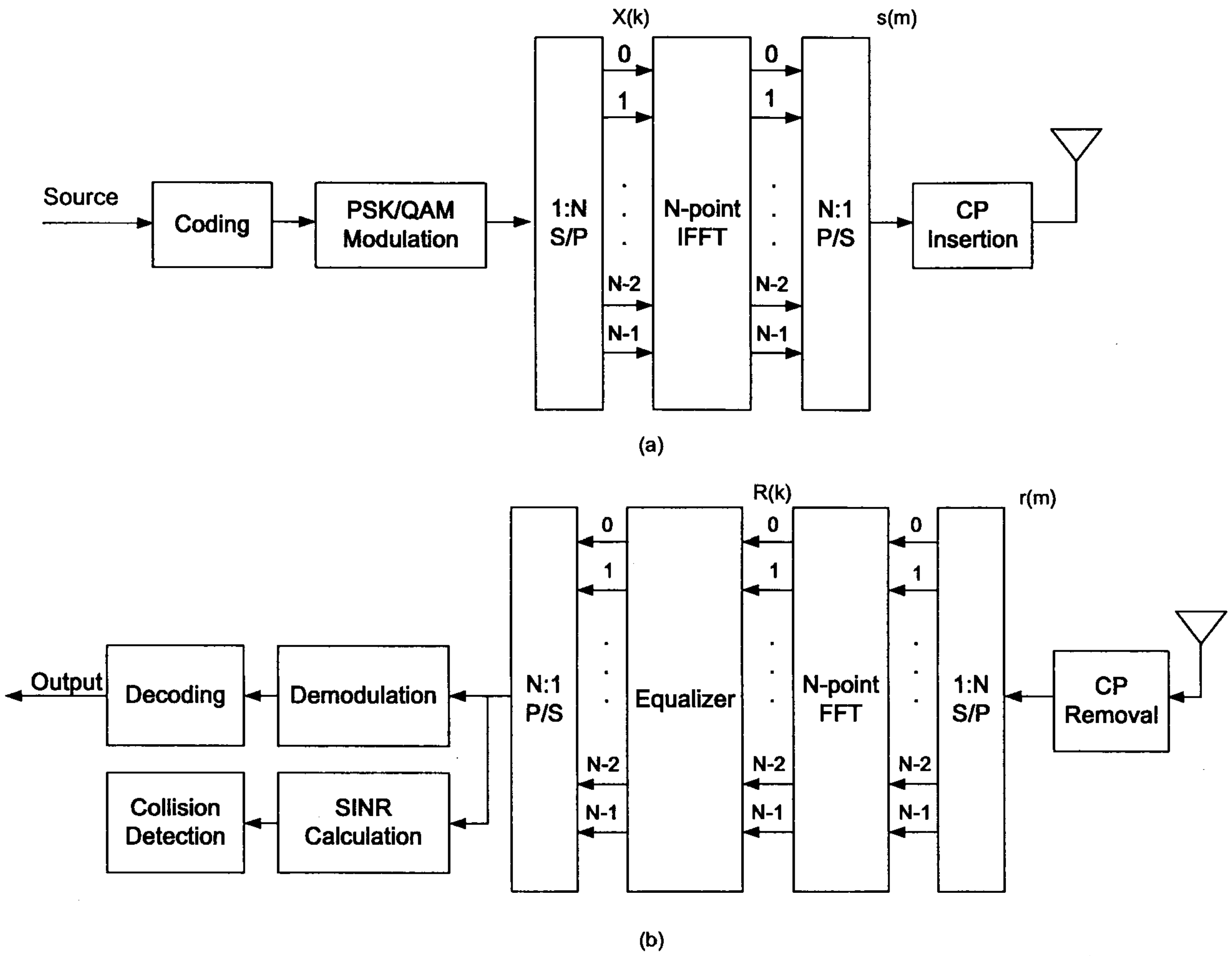


Figure 3.1: The transmitter and receiver block diagram for the OFDM based IEEE 802.11 PHY supplemented with the proposed collision detection component.

Once the symbol is detected, the signal power can be estimated by averaging the detected symbol across subcarriers. Meanwhile, the noise variance can be estimated by averaging the squared difference between the equalized signal $X_{\mathrm{eq}}(k)$ and the detected signal. The signal and interference plus noise power can be estimated as

$$\begin{cases} \hat{\mathrm{S}} = \frac{1}{N} \sum\limits_{k=0}^{N-1} \|\psi(X_{\mathrm{eq}}(k))\|^2 \\ \widehat{\mathrm{IN}}_0 = \frac{1}{N} \sum\limits_{k=0}^{N-1} \|X_{\mathrm{eq}}(k) - \psi(X_{\mathrm{eq}}(k))\|^2 \end{cases}, \tag{3.5}$$

where function $\psi(\cdot)$ maps the input equalized signal to the closest discrete constellation point, $\hat{\mathrm{S}}$ and $\widehat{\mathrm{IN}}_0$ represents the estimated signal power and the noise plus interference power resepectively.

Based on (3.5), the SINR measurement γ can be developed as

$$\gamma = \frac{\sum\limits_{k=0}^{N-1} \|\psi(X_{\mathrm{eq}}(k))\|^2}{\sum\limits_{k=0}^{N-1} \|X_{\mathrm{eq}}(k) - \psi(X_{\mathrm{eq}}(k))\|^2}. \tag{3.6}$$

Compared with other wireless channel quality indicators, such as BER or PER which updates on frame level and requires a long period to converge, the above SINR measurements update on symbol basis. Consequently, it can fast track channel variations and detect the collision, which enables more intelligent and rapid rate adaptations.

3.4 Collision Detection Based on SINR Changes

SINR in (3.1) is a direct wireless link quality indicator, which varies according to channel fadings as well as collisions induced co-channel interference. However, noise, channel fading and co-channel interference have different impacts on SINR measurements. To be more specific, the desired signal power S in (3.1) is attenuated by pathloss and channel fading, which changes slowly during the coherence time; while the interference term I in (3.1) can abruptly change due to collisions presented during transmissions. Due to the different characteristics of fading and interference exhibited in SINR measurements, channel variations and collisions can be differentiated by tracking the change presented in the samples of SINR estimate.

In the following, a fast collision detection algorithm is proposed by detecting abrupt changes in SINR measurements caused by collisions using nonparametric CUSUM algorithm [38]. The proposed algorithm requires no knowledge about the SINR distribution functions which need to be obtained by a long time observation, thereby making it robust under various multipath channels in real-time processing.

3.4.1 Hypothesis Test of SINR Changes

In this section, SINR based collision detection algorithm is introduced in detail. Denote $\mathbf{\Gamma}_{\text{est}}(n)$ as a vector of p SINR estimates calculated by (3.6) at the nth received OFDM symbol. The p SINR estimates can be obtained from either simultaneous receptions by p antenna branches, or p specific subcarriers in one OFDM symbol with known formats, e.g., pilot subcarriers and typically $1 \leq p \leq 4$ in the IEEE 802.11 system.

For the nth OFDM symbol in the received frame, we have

$$\mathbf{\Gamma}_{\text{est}}(n) = [\gamma_{\text{est}_1}(n), \gamma_{\text{est}_2}(n), \cdots, \gamma_{\text{est}_p}(n)]^T. \tag{3.7}$$

In the case of no collision, the SINR vector $\mathbf{\Gamma}_{\text{est}}(n)$ fluctuates according to channel fading with a fixed or slow rate. The mean value $\boldsymbol{\mu}_{\text{est}}$ of each SINR estimates in $\mathbf{\Gamma}_{\text{est}}(n)$ will not change significantly within the channel coherence time. It can be obtained through training or calibration procedures when no collision occurs, or by averaging the SINR measurements across a number of OFDM symbols:

$$\hat{\mu}_{\text{est}}(n) = \frac{1}{m} \sum_{l=n-m+1}^{n} \Gamma_{\text{est}}(l), \tag{3.8}$$

where m is the number of consecutive OFDM symbols used in averaging and its value depends on the channel coherence time normalized by the symbol period.

The channel coherence time T_C can be approximately calculated as [39]

$$T_C \approx \frac{9}{16\pi f_d}, \tag{3.9}$$

where $f_{\text{d}} = f_{\text{c}} \times \frac{v}{c}$ [44] is the maximum Doppler shift, f_{c} is the carrier frequency, v represents the relative velocity between two communicating stations and c denotes the propagation speed of electromagnetic waves in the air. For typical IEEE 802.11 WLAN scenarios where wireless stations are generally stationary or carried by pedestrians, a maximum relative movement velocity of 2 m/s is assumed, which results in a maximum Doppler shift of 16 Hz for the 2.4 GHz IEEE 802.11 WLANs. Consequently, given that the symbol period of one OFDM symbol is 4 μs, the channel coherence time is approximately equivalent to the duration of 2300 OFDM symbols. This proves that in the case of no collisions, the SINR vector fluctuates with a slow rate according to channel fadings.

To better illustrate the properties of SINR vector $\Gamma_{\text{est}}(n)$, define a vector $\Gamma(n)$ by removing the estimated SINR mean vector $\hat{\mu}_{\text{est}}(n)$ from $\Gamma_{\text{est}}(n)$ as follows

$$\begin{aligned} \Gamma(n) &= \Gamma_{\text{est}}(n) - \hat{\mu}_{\text{est}} \\ &= [\gamma_1(n), \gamma_2(n), \cdots, \gamma_{\text{p}}(n)]^T. \end{aligned} \tag{3.10}$$

Therefore, $\mathbf{\Gamma}(n)$ is a vector with zero mean (i.e. $\boldsymbol{\mu} = [\mu_1, \mu_2, \cdots, \mu_{\mathrm{p}}]^T$ and $\boldsymbol{\mu} = \mathbf{0}$) when no collision occurs. By simply removing the mean value inherent in the observed SINR vector, the sample vector is shifted to zero.

When collision presents, there is an abrupt change in the mean value of the SINR due to co-channel interference introduced by collisions. The mean values of $\mathbf{\Gamma}(n)$ will constantly shift away from zero. Thus, the detection of collisions can be converted into a binary hypothesis test on the change of the mean value of $\mathbf{\Gamma}(n)$, i.e.,

$$\begin{aligned} &\mathcal{H}_0 : \boldsymbol{\mu} = [\mu_1, \mu_2, \cdots, \mu_{\mathrm{p}}]^T = \mathbf{0}, \quad \text{when no collision occurs,} \\ &\mathcal{H}_1 : \boldsymbol{\mu} = [\mu_1, \mu_2, \cdots, \mu_{\mathrm{p}}]^T \neq \mathbf{0}, \quad \text{when collision occurs.} \end{aligned} \tag{3.11}$$

The null hypothesis $\mathcal{H}_0$ in (3.11) can be further decomposed into two sub-hypotheses $\mathcal{H}_0^{(1)}$ and $\mathcal{H}_0^{(2)}$ as follows for better understanding:

$$\mathcal{H}_0^{(1)} : \mu_1 = \mu_2 = \cdots = \mu_{\mathrm{p}} \tag{3.12}$$

and

$$\mathcal{H}_0^{(2)} : \sum_{j=1}^{p} \mu_{\mathrm{j}} = 0. \tag{3.13}$$

Hypothesis $\mathcal{H}_0^{(1)}$ assumes the mean values of SINR measurements $\mu_{\mathrm{i}}(n)$ from different antennas or different pilot subcarriers are the same. When collision occurs, $\mu_{\mathrm{i}}(n)$ from different branches may shift with different magnitudes, which causes a violation of $\mathcal{H}_0^{(1)}$, thus the collision can be detected. However, in the particular collision case that all the mean values of SINR measurements shift with the same magnitude, $\mathcal{H}_0^{(1)}$ is not violated and the collision cannot be detected. Therefore, $\mathcal{H}_0^{(2)}$ is required to fully constrain SINR variations to successfully detect a collision. More specifically, when a violation of $\mathcal{H}_0$ happens, the closer it is to $\mathcal{H}_0^{(1)}$, the farther it is from $\mathcal{H}_0^{(2)}$, and vice versa. Consequently, a combination of both $\mathcal{H}_0^{(1)}$ and $\mathcal{H}_0^{(2)}$ should be considered in the collision detection procedure using CUSUM algorithm [38].

Though the combination of $\mathcal{H}_0^{(1)}$ and $\mathcal{H}_0^{(2)}$ is complete condition for (3.11) for collision detection, it is computational inefficient to test these two sub-hypotheses (3.12) and (3.13) at the same time.

To cope with this problem, the received signal strength (RSS) is also taken into consideration for the proposed collision detection algorithm. The RSS represents the total signal strength measured upon reception, which is a combined strength of signal, interference and noise. Recall (3.1), while the strength of desired signal decreases due to additional co-channel interference during collisions, the RSS increases since it is a summation of total received signal strength. Therefore, when collision occurs, the mean value of SINR and RSS will shift towards different directions, thus the limitation of (3.12) is avoided and the hypothesis test in (3.11) can be further simplified by adding rss(n) into (3.10) as follows

$$\mathbf{\Gamma}^*(n) = [\gamma_1(n), \gamma_2(n), \cdots, \gamma_{\mathrm{p}}(n), \gamma_{\mathrm{rss}}(n)]^T, \tag{3.14}$$

where $\gamma_{\mathrm{rss}}(n) = \mathrm{rss}_{\mathrm{est}}(n) - \overline{\mathrm{rss}}(n)$, $\mathrm{rss}_{\mathrm{est}}(n)$ is the estimated RSS at nth received OFDM symbol and $\overline{\mathrm{rss}}(n)$ is obtained through the procedure similar in (3.8).

Consequently $\mathcal{H}_0$ in (3.11) is turned into

$$\mathcal{H}_0^* : \mu_1 = \mu_2 = \cdots = \mu_{\mathrm{p}} = \mu_{\mathrm{rss}}. \tag{3.15}$$

Based on (3.15), $\mathcal{H}_0^*$ can be utilized to detect changes with either different magnitudes or the same magnitude presented in the SINR vector $\mathbf{\Gamma}(n)$. Furthermore, (3.15) solves the problem that (3.11) does not work for single antenna system where $p = 1$. Therefore, detecting the presence of collisions can be achieved by simply testing this sole hypothesis $\mathcal{H}_0^*$.

3.4.2 Collision Detection Using the Nonparametric Order-based CUSUM Algorithm

As previously discussed, the collision detection can be formulated as a binary hypothesis testing $\mathcal{H}_0^*$. The method employed here for testing the hypothesis $\mathcal{H}_0^*$ is to track changes of SINR measurement permutations at the nth OFDM symbol as well as the local reference $\gamma_{\text{ref}}(n)$. Changes on the permutations can directly indicate violations of $\mathcal{H}_0^*$, which indicate the presence of collisions.

In order to represent the permutation of SINR measurements at the nth OFDM symbol, an order vector $\mathbf{O}(n)$ for $\mathbf{\Gamma}^*(n)$ is defined as follows

$$\mathbf{O}(n) = [O_1(n), O_2(n), \cdots, O_{\text{p}}(n), O_{\text{p}+1}(n)]^T, \tag{3.16}$$

where each component of $\mathbf{O}(n)$ is the index of the corresponding element in $\mathbf{\Gamma}^*(n)$ after an ascending permutation such that

$$\gamma_{O_1(n)}(n) \leq \gamma_{O_2(n)}(n) \leq \cdots \leq \gamma_{O_{\text{p}+1}(n)}(n). \tag{3.17}$$

The possible value of each component $O_{\text{i}}(n)$ of the order vector $\mathbf{O}(n)$ is within the range $[1, p+1]$. In other words, the first component $O_1(n)$ in the order vector $\mathbf{O}(n)$ is the index of the smallest element among $\mathbf{\Gamma}^*(n)$, and the last component $O_{\text{p}+1}(n)$ is the index of the largest one in $\mathbf{\Gamma}^*(n)$.

Although any single component or combinations of multiple components in the order vector $\mathbf{O}(n)$ can be used to detect changes in permutations for collision detections [38], without loss of generality, the proposed scheme presented in the following section is based on the first component $O_1(n)$, i.e., the smallest element in $\mathbf{\Gamma}^*(n)$.

We further define the indicator vector as $\boldsymbol{\xi}_1(n) = \{\xi_{1,\mathrm{j}}(n),\ j = 1, 2, \cdots, p, p+1\}$, where each component in this vector is the indicator function $\xi_{1,\mathrm{j}}(n)$ as given below

$$\xi_{1,\mathrm{j}}(n) = \begin{cases} 1 & \text{if } O_1(n) = j, \\ 0 & \text{otherwise,} \end{cases} \qquad 1 \le j \le p+1. \tag{3.18}$$

From (3.18), when the jth element is the smallest element among the $p+1$ components in $\mathbf{\Gamma}^*(n)$ at the nth symbol, $\xi_{1,\mathrm{j}}(n) = 1$; otherwise it is zero.

Below we give an example to demonstrate the relationship of the order vector, indicator vector with SINR measurement vector $\mathbf{\Gamma}^*(n)$. Suppose the measured SINR vector $\mathbf{\Gamma}^*(n)$ at the nth OFDM symbol is $[4, 8, 7, 1]^T$, the corresponding order vector therefore is $\mathbf{O}(n) = [2, 4, 3, 1]$ and the indicator vector is $\boldsymbol{\xi}_1(n) = [0, 0, 0, 1]^T$ showing that the fourth component in the vector $\mathbf{\Gamma}^*(n) = [4, 8, 7, 1]^T$ is the smallest among $\mathbf{\Gamma}^*(n)$.

Define $\mathbf{g}_1(n)$ as the expectation of the indicator vector $\boldsymbol{\xi}_1(n)$, where each element of $\mathbf{g}_1(n)$ is given by

$$g_{1,\mathrm{j}}(i) = E(\xi_{1,\mathrm{j}}(n)), \quad j = 1, 2, \cdots, p, p+1. \tag{3.19}$$

The expectation of the indicator vector above gives the frequency of the smallest value appearing over each index, which is the probability distribution of $O_1(n)$, i.e. $p(O_1(n)) = \{g_{1,\mathrm{j}}, \mathrm{j} = 1, 2, \cdots, p+1\}$. When collision occurs, the mean of SINR vector $\boldsymbol{\mu}$ will change.

The order vector $\mathbf{O}(n)$ features two important advantages [38] which the SINR based collision detection algorithm can benefit from. First, the distribution function of $\mathbf{O}(n)$ under the hypothesis $\mathcal{H}_0^*$ is a uniform distribution function regardless of the distribution of SINR estimates as long as the distribution functions of p branches are independent and identical to each other. Based on this feature, it is unnecessary to model the analytical distribution of SINR, which is difficult to construct in realistic scenarios. Especially with the presence of collisions, this nonparametric feature enables the proposed collision detection algorithm to operate under various channel conditions without prior knowledge of SINR distributions. Second, the distribution function of $\mathbf{O}(n)$ is sensitive to violations of either $\mathcal{H}_0^{(1)}$ or $\mathcal{H}_0^{(2)}$ or both, which corresponds to the occurrence of collisions, thereby shortening the collision detection delay.

To track changes in the SINR measurement permutations, we define the nonparametric order-based CUSUM procedure as follows [11] [48]. Define $C(n)$ as a recursive function that indicates the changes in permutations of the mean vector:

$$\begin{aligned} C(n) &= [(\mathbf{S}^{(1)}(n-1) - \mathbf{S}^{(2)}(n-1)) + (\xi_1(n) - \mathbf{g}_1)]^T \\ &\times \ \mathrm{diag}((S_1^{(2)}(n-1) + g_{1,1})^{-1}, \cdots, (S_{p+1}^{(2)}(n-1) + g_{1,p+1})^{-1}) \\ &\times \ [(\mathbf{S}^{(1)}(n-1) - \mathbf{S}^{(2)}(n-1)) + (\xi_1(n) - \mathbf{g}_1)], \end{aligned} \tag{3.20}$$

where $\mathbf{g}_1 = [g_{1,1}, g_{1,2}, \cdots, g_{1,\mathrm{p}+1}]^T$. $\mathbf{S}^{(1)}(n)$ and $\mathbf{S}^{(2)}(n)$ are two accumulation vectors initialized to zero at the beginning of the CUSUM procedure and will be discussed later.

$C(n)$ is used to update the cumulative sum $\mathbf{S}^{(1)}(n)$ and $\mathbf{S}^{(2)}(n)$ or reset them to zero according to the tuning factor k. The tuning factor k is used to repeatedly reset the CUSUM procedure when there is no evidence of violation of $\mathcal{H}_0^*$, i.e., no presence of collisions during the communication, such that the procedure can react to a real abrupt SINR change promptly.

When $C(n) < k$, no changes in permutations of the mean vector are assumed, which indicates no collisions occurred. Then $\mathbf{S}^{(1)}(n)$ and $\mathbf{S}^{(2)}(n)$ are reset to zero as follows

$$\begin{cases} \mathbf{S}^{(1)}(n) & = \mathbf{0} \\ \mathbf{S}^{(2)}(n) & = \mathbf{0}\,. \end{cases} \tag{3.21}$$

When $C(n) \geq k$, the permutation of mean vector has been changed, then $\mathbf{S}^{(1)}(n)$ and $\mathbf{S}^{(2)}(n)$ are updated according to the accumulation functions given below

$$\begin{cases} \mathbf{S}^{(1)}(n) = (\mathbf{S}^{(1)}(n-1) + \xi_1(n))(C(n)-k)/C(n) \\ \mathbf{S}^{(2)}(n) = (\mathbf{S}^{(2)}(n-1) + \mathbf{g}_1)(C(n)-k)/C(n). \end{cases} \tag{3.22}$$

The CUSUM result $y(n)$ used for threshold comparison is given by:

$$\begin{aligned} y(n) &= (\mathbf{S}^{(1)}(n) - \mathbf{S}^{(2)}(n))^T \mathrm{diag}(1/S_1^{(2)}(n), \cdots, 1/S_{\mathrm{p}+1}^{(2)}(n)) \\ &\times (\mathbf{S}^{(1)}(n) - \mathbf{S}^{(2)}(n)). \end{aligned} \tag{3.23}$$

By applying the nonparametric order-based CUSUM procedure described in (3.21)-(3.23) and comparing $y(n)$ given in (3.23) with a pre-defined threshold y_{T}, collisions can be detected.

To better illustrate the algorithm, the procedure of collision detections using the nonparametric order-based CUSUM algorithm is summarized in Table 3.1.

Table 3.1: Nonparametric order-based CUSUM procedure

Nonparametric order-based CUSUM	
1)	Set accumulation vectors $\mathbf{S}^{(1)}(n)$ and $\mathbf{S}^{(2)}(n)$ to $\mathbf{0}$ in initialization in (3.21).
2)	Calculate the order vector $\mathbf{O}(n)$ and the corresponding indicator $\xi_1(n)$ at the nth received OFDM symbol following (3.16)-(3.18).
3)	Update accumulation vectors $\mathbf{S}^{(1)}(n)$ and $\mathbf{S}^{(2)}(n)$ based on calculation results given in Step 2) using (3.22).
4)	Update recursive function $C(n)$ based on results given in Step 3) using (3.20). If $C(n) < k$, go to Step 1) to reset the two accumulation vectors; Otherwise, continue.
5)	Calculate CUSUM result $y(n)$ in (3.23) and compare it with a pre-defined threshold y_{T}. If $y(n) < y_{\mathrm{T}}$, go to Step 2) and continue the procedure; Otherwise, signal an alarm indicating a collision is detected, stop.

3.5 Simulation Results

In this section, the nonparametric property of the order-based CUSUM algorithm is first evaluated. After that, simulation results are presented to evaluate the performance of the proposed collision detection scheme.

To evaluate the nonparametric property of the order-based CUSUM algorithm, multivariate numbers $\upsilon(n) = [v_1(n), v_2(n), v_3(n)]$ are randomly generated from several independent distributions, namely Normal distribution, Gamma distribution and Chi-square distribution. In this simulation, two cases are considered, where each element $v_{\mathrm{i}}(n)$ $i \in [1, 3]$ is generated from identical and non-identical distributions for demonstrating the relationship between distribution of $v_{\mathrm{i}}(n)$ and the performance of the order-based CUSUM algorithm in terms of average detection delay, false alarm probability and miss detection probability.

The mean value of $\upsilon(n)$ is normalized to zero in the beginning. At a pre-defined moment, the mean value of $\upsilon(n)$ changes to υ_{C} to evaluate the performance of the order-based CUSUM algorithm.

Table 3.2 presents the evaluation results. In this table, the Mix distribution refers

Table 3.2: Evaluation of order-based CUSUM algorithm

$\upsilon_{\mathrm{C}} = [-2, -1, -3.5]$			
Distribution	Average Detection Delay	False Alarm Prob.	Miss Detection Prob.
Normal	16.1002	4×10^{-4}	0
Gamma	15.8667	4×10^{-4}	0
Chi-Square	16.0568	8×10^{-4}	0
Mix	16.0744	6×10^{-4}	0
$\upsilon_{\mathrm{C}} = [2, 1, 3.5]$			
Distribution	Average Detection Delay	False Alarm Prob.	Miss Detection Prob.
Normal	24.6992	1×10^{-3}	0
Gamma	24.3379	1×10^{-3}	0
Chi-Square	24.351	8×10^{-4}	0
Mix	24.5403	6×10^{-4}	0
$\upsilon_{\mathrm{C}} = [2, 0, -3.5]$			
Distribution	Average Detection Delay	False Alarm Prob.	Miss Detection Prob.
Normal	10.2734	4×10^{-4}	0
Gamma	10.3305	4×10^{-4}	0
Chi-Square	10.034	1×10^{-3}	0
Mix	10.3017	1×10^{-3}	0

to the case that $v_{\rm i}(n)$ is generated from different distribution compared with $v_{\rm j}(n)$, where $i \neq j$. Three kind of mean value changes $\upsilon_{\rm C}$ are considered in this simulation, namely down shifting, up shifting and mixed shifting. It can be observed from the table that for a given change scenario, the performance of the algorithm in terms of average detection delay, probability of false alarm and probability of miss detection are approximately the same for all four considered distributions. This proves that the order-based CUSUM algorithm is capable to detect the occurrence of changes in $\upsilon(n)$ without *a priori* knowledge of the distribution of $v_{\rm i}$.

The proposed scheme detects the occurrence of collisions during point-to-point wireless transmissions by monitoring SINR changes. In realistic scenarios, the statistical distribution of SINR under interferences or fadings is difficult to predict. Therefore, the nonparametric property enhances the robustness of the proposed collision detection scheme in practical applications.

In the next simulation for evaluating the ability of collision detection, a pair of IEEE 802.11a OFDM transmitter and receiver are employed to simulate the desired point-to-point transmissions. Another IEEE 802.11a station is introduced as a hidden transmitter that interferes the desired point-to-point communication channel during transmissions. As a result, collisions are introduced. The transmitter and receiver in the point-to-point communication supports all mandatory and optional data rates in IEEE 802.11a, while the hidden transmitter uses a fixed data rate during transmission.

Figure 3.2 illustrates a typical variation of SINR measured at the receiver when a collision occurs. The interference power is set to be the same as the desired signal power for better demonstration. The dash curve in blue color represents the SINR measurement without the presence of interferences from the hidden station. The red continuous curve, on the other hand, represents the case that the hidden station starts its transmissions from the 150th symbol. It can be observed from the figure that although the dynamic range of

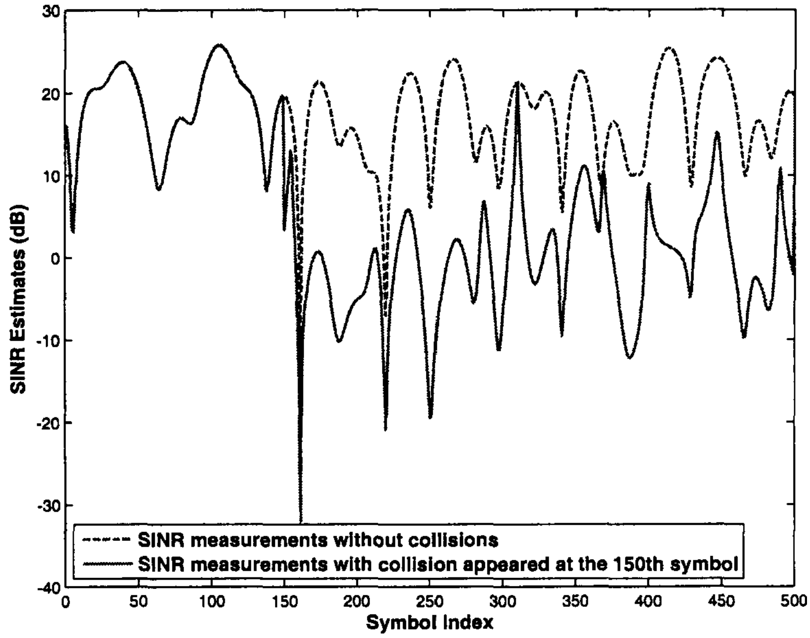


Figure 3.2: SINR measurements at the receiver side with a collision beginning with the 150th OFDM symbol.

the estimated SINR is large due to multipath fadings of the point-to-point wireless channel, the mean value of SINR measurements vary slowly in the absence of collisions. On the other hand, the occurrence of collision causes an abrupt change in the mean values of SINR measurements. This kind of abrupt changes enable the nonparametric order-based CUSUM algorithm to detect collisions.

Figure 3.3 shows the corresponding results of the proposed collision detection scheme by tracking the SINR estimates shown in the Figure 3.2. The black vertical line on the left indicates the occurrence of collisions starts from the 150th OFDM symbol during the desired transmission. The blue curve shows the calculated CUSUM results for SINR measurements. It can be observed from this figure that even though the SINR variation caused by multipath fadings is large (deep fades will cause apparent SINR change during the transmission), the proposed algorithm is able to constantly reset its CUSUM results when no collision occurs. On the other hand, the collision is detected with a detection delay of 14 OFDM symbols

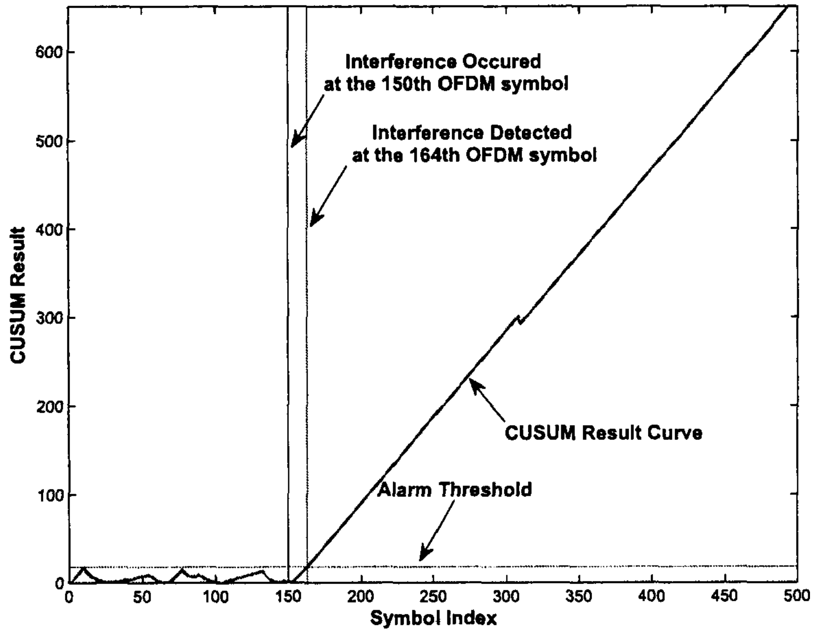


Figure 3.3: The result of CUSUM algorithm applied on the SINR measurements shown in Figure 3.2. The collision is detected at the 164th symbol.

after the presence of collisions. According to the standard, a typical data frame in IEEE 802.11 has a length of 1500 bytes, which means at least 56 OFDM symbols are needed using the highest modulation and coding scheme supported by IEEE 802.11. Lower modulation and coding schemes require a larger number of OFDM symbols for data frame transmission. Therefore, the detection delay of the proposed scheme is significantly shorter than the length of one typical IEEE 802.11 data frame and collisions can be detected within just one frame period. Compared with frame loss based collision detection schemes, our proposed scheme provides a close-to-real-time metric, thus shorten the decision delay of RAA schemes.

Figure 3.4 and 3.5 demonstrate the impact of selections of CUSUM tuning factor k and collision detection threshold y_T to the performance of the proposed collision detection algorithm in terms of average detection delay (in number of OFDM symbols) and probability of false alarm. In these two figures, the SNR of the point-to-point channel is fixed at 10 dB and the interference to signal ratio is fixed at 0.2. Figure 3.4 shows that larger

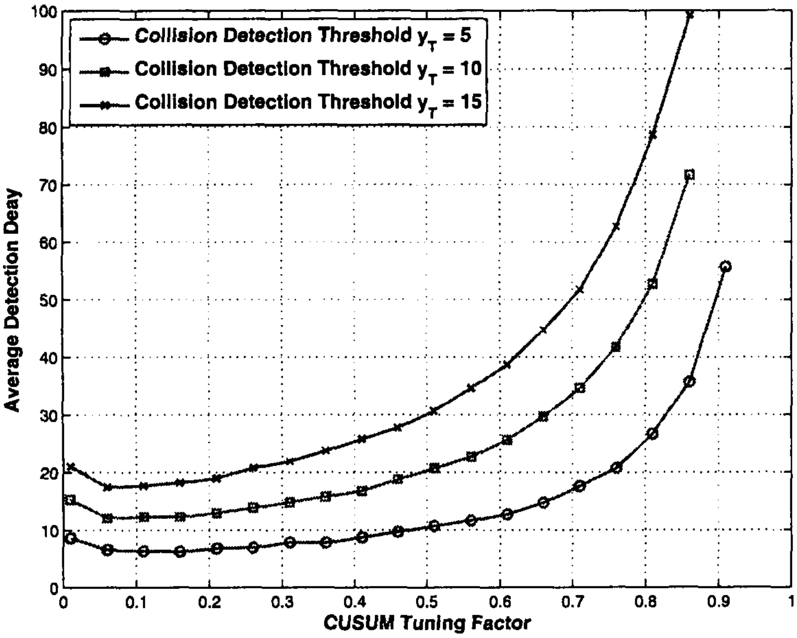


Figure 3.4: The collision detection delay under different combinations of CUSUM tuning factor and collision detection delay when the modulation scheme of signal is QPSK, SNR is fixed at 10 dB.

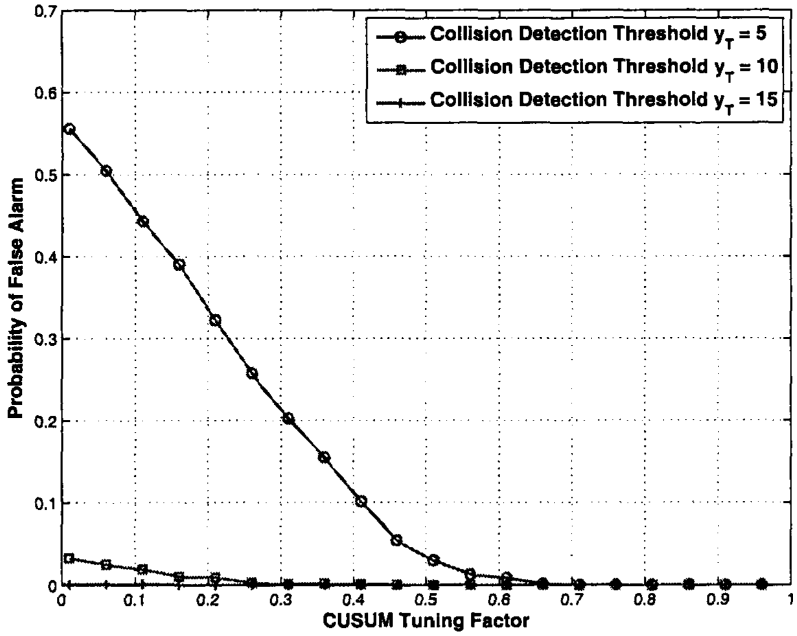


Figure 3.5: The probability of false alarm under different combinations of CUSUM tuning factor and collision detection delay when the modulation scheme of signal is QPSK, SNR is fixed at 10 dB.

collision detection threshold and larger CUMSUM tuning factor result in longer detection delay, while Figure 3.5 demonstrates that the probability of false alarm decreases with larger collision detection threshold and CUMSUM tuning factor. It can be observed that when CUSUM tuning factor is small, the probability of false alarm is sensitive to the choice of collision detection threshold. This is because smaller CUSUM tuning factor results in higher sensitivity to the presence of abrupt changes in SINR measurements. In this case, the CUSUM result given in (3.23) may constantly accumulate with the fluctuations of multipath fading channel and therefore result in higher false alarm probability.

Figure 3.6 and 3.7 investigate the effects of different modulation schemes employed in the signal to the collision detection performance in terms of detection delay. All the four IEEE 802.11 supported modulation schemes are considered in this simulation. To better demonstrate the result, in these simulations, the CUSUM tuning factor and detection threshold are fixed at 0.2 and 15, respectively, according to the results previously presented in Figure 3.4 and Figure 3.5. It can be observed from Figure 3.4 and Figure 3.5 that all the four modulation schemes follow the same downward trend in terms of average collision detection delay when signal SNR and interference to signal power ratio increases. It can also be observed from these results that for higher order modulation schemes, the average detection delay increases. However, this performance degradation is less than 10 OFDM symbols for the worst case where SNR is 0 dB and interference to signal power ratio is 0.1. For the result presented in Figure 3.6, the corresponding false alarm rate is less than 5×10^{-4} and the average detection delay is less than 40 OFDM symbols for all combination of different modulation schemes and SNR values. This proves that the proposed collision detection algorithm is robust against point-to-point channel variations. For the result presented in Figure 3.7, the corresponding false alarm rate is also less than 5×10^{-4} and the average detection delay is less than 30 OFDM symbols for all combination of different modulation schemes and interference to signal power ratios. Furthermore, all the four modulation schemes con-

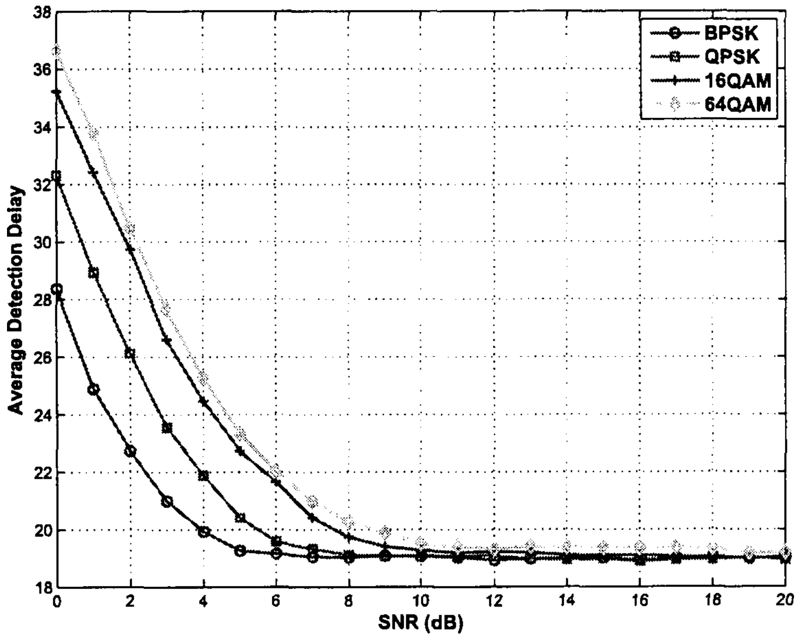


Figure 3.6: The collision detection delay for different modulation schemes versus various SNR when the interference to signal power ratio is fixed at 0.2, $k = 0.2$ and $y_T = 15$.

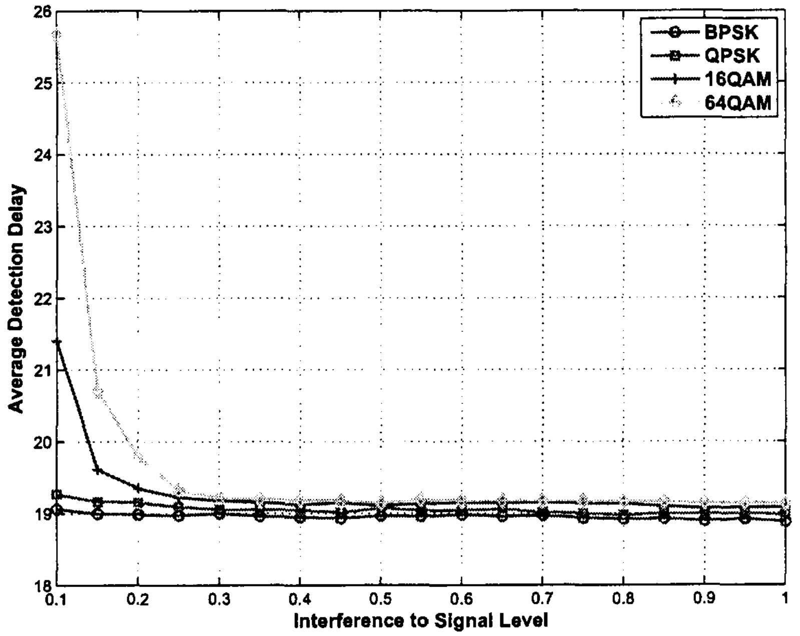


Figure 3.7: The collision detection delay for different modulation schemes versus various interference to signal power ratio when the SNR is fixed at 10 dB, $k = 0.2$ and $y_T = 15$.

verge at a stable detection delay of approximate 20 OFDM symbols when the interference to signal power is greater than 0.2. This proves that the proposed collision detection algorithm is sensitive to collisions even when the interfering power is not too strong. This is particularly useful since the non-overlapping wireless channels in IEEE 802.11 is limited and it is a typical case that several APs are geometrically septated with short distance to each other and operating at the same or neighboring channels. In such scenarios, the co-channel interferences and collisions may not strong enough to break the intending transmission, yet they introduce additional frame losses to the intending transmission which cannot be simply resolved by adjusting transmission modulation and coding schemes. With the help of the proposed collision detection scheme, weak interferences and collisions can also be detected such that AP can switch its operating channel to enhance the stability of transmissions.

Figure 3.8 shows the evaluation of the performance of the proposed collision detection algorithm in terms of collision detection delay, considering different levels of desired signal strength and different interference to signal power ratio. According to results presented in Figure 3.4 and 3.5, the CUSUM tuning factor and collision detection threshold is chosen to be 0.2 and 15, respectively. A Rayleigh fading channel with maximum Doppler frequency of 20 Hz is used in the simulation. Based on this configuration, the maximum relative velocity of movements between two point-to-point communicating stations is approximately 2 m/s. This is a typical scenario for IEEE 802.11 WLAN, in which wireless stations are generally stationary or carried by pedestrians.

In Figure 3.8, detection delays under different signal strength levels (SNR = [0 dB, 5 dB, 10 dB, 15 dB]) are shown in four separate curves respectively. For each curve with a fixed signal strength, the detection delay decreases as the interference power level increases. It is also observed that with the fixed interference power level, detection delay decrease with the increase of SNR. This is as expected because higher interference level results in larger changes in the mean values of SINR measurements, lower noise level results in smaller

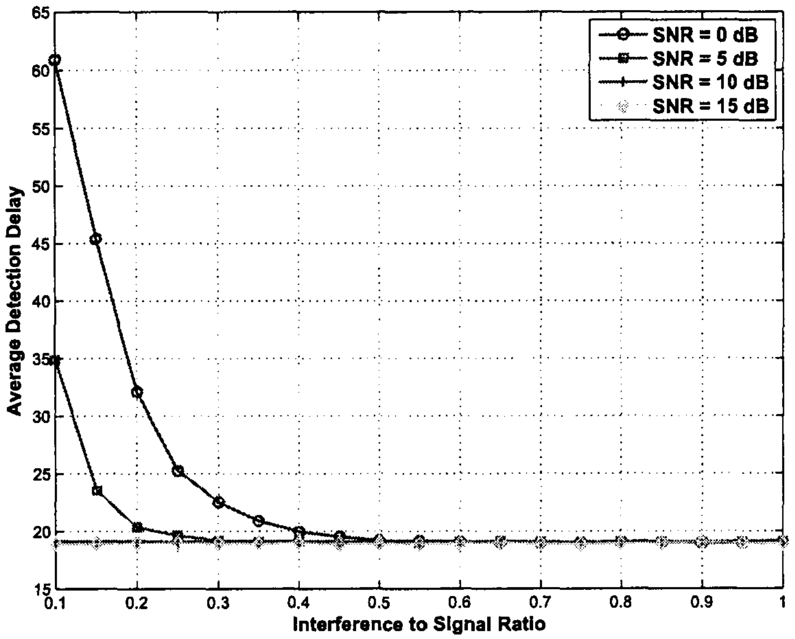


Figure 3.8: The collision detection delay under different interference power level in Rayleigh fading channel with a maximum 20Hz Doppler frequency when the modulation scheme of signal is QPSK, $k = 0.2$ and $y_T = 15$.

variations in the SINR measurements, both of which make the collision detection algorithm more responsive to the presence of collisions. Furthermore, the detection delay becomes stable at about 20 OFDM symbols when the interference to signal power ratio is higher than 0.4, which confirms the responsiveness to the presence of interferences. Compared with a typical IEEE 802.11 data frame which consists at least 56 OFDM symbols, this detection delay is significantly shorter, enabling the ability to detect the collision during a single frame transmission. The false alarm probability for all SNR cases is less than 5×10^{-4}, proving the reliability of the proposed collision detection algorithm under varying channel conditions.

3.6 Summary

In this chapter, we proposed a fast and reliable collision detection algorithm for IEEE 802.11 systems using SINR measurements obtained from the PHY layer. It is an appealing scheme because of its fast response to channel conditions. To detect the abrupt SINR change caused by collisions a nonparametric order-based CUSUM procedure is employed. This sequential change detection scheme is able to distinguish collisions from conventional channel variations based on the order statistics of SINR measurements. With this order-based CUSUM procedure, no *a priori* SINR distribution is required. Furthermore, the proposed collision detection scheme is based on decision directed SINR measurements which utilizes existing demodulated symbols and thereby can be easily integrated into current RAAS to further enhance IEEE 802.11 WLAN performance. Simulation results show that the delay of the proposed collision detection is within few OFDM symbols and probabilities of false alarm and miss detection are low.

Chapter 4

Protocol-based Indoor Position Location Technique Using IEEE 802.11 WLANs

In this chapter, an IPL technique based on IEEE 802.11 data/ACK frame exchange sequences is presented. The distances between two communication stations (one target station and one reference station) are estimated by measuring the round trip propagation time that a data frame and its corresponding ACK frame travel between the target station and the reference station. Once the distances between the target and multiple (typically three) reference stations are available, the 2-dimensional (2D) coordinates of the target station can be determined by the trilateration method.

This chapter is organized as follows. The research motivation is presented in Section 4.1, followed by a review of existing works in Section 4.2. The distance measurement technique using IEEE 802.11 frame timestamps is presented in Section 4.3 and the analysis on RTT estimation error is presented in Section 4.4. The location determination using measured distances based on the trilateration method is discussed in Section 4.5 while system implementation is discussed in Section 4.6. Secion 4.7 summarizes the chapter.

4.1 Research Motivation

Satellite navigation systems, such as the GPS, become more and more popular because of their accuracy and efficiency in outdoor areas, where lines of sight between the user devices and satellites can be normally maintained. However, in scenarios such as indoor sites, tree-covered locations and urban canyons, where the direct signals from satellites are obstructed or severely attenuated, these systems introduce large errors to position location results or even fail to work. Therefore, enabling technologies for IPL systems recently attracts a lot of attentions and research efforts in order to build reliable yet simple-to-deploy indoor navigation and tracking systems.

In this chapter, we developed an IPL system which is integrated with the IEEE 802.11 WLAN networks for indoor scenarios as IEEE 802.11 APs can be found and accessible at almost every place, such as shopping malls, cafes, university campus and government buildings. Since distance measurement is the core operation of trilateration based position location methods, this chapter concentrates on discussing the distance measurement between two communicating wireless stations. In our study, the distance is estimated by observing Time-of-Arrival (TOA) of frames and then measuring the round trip propagation time that an IEEE 802.11 data frame and its corresponding ACK frame take to travel between two stations. When distances between the target station and reference stations are measured, trilateration based IPL system can be employed to locate the position of the target station by determining its coordinates in a 2D space [16, 17, 31]. The proposed distance measurement technique can be completely implemented in software such that the system can be deployed using off-the-shelf WLAN NICs and requires no hardware modification. Therefore, the implementation complexity is drastically reduced and the system deployment is cost-effective.

4.2 Related Works

The IEEE 802.11 WLANs based IPL system has become increasingly popular in both academy and industry. Most existing proposals are based on the RSS fingerprint [9, 20, 50, 54]. The RSS, which is implemented as the received signal strength indicator (RSSI) in IEEE 802.11 standard, is directly available from WLAN NICs. RSS fingerprint approaches locate a device by accessing a pre-determined signal strength map, which is essentially a radio map database containing the pre-measured RSS values and corresponding coordinates for a certain area. Based on measured instantaneous RSS values, RSS fingerprint algorithms calculate target coordinates by comparing current measured RSS values with those in the pre-recorded database. However, to construct an accurate radio map database, these methods suffer from time-consuming off-line training phases. Furthermore, the accuracy of the radio map database is site-specific and subject to environmental changes, such as other radio signals, pedestrians, temperature variation and furniture repositioning [47]. Thus, the suitability of RSS fingerprint approaches for IPL applications is limited.

Trilateration based IPL technique is employed as an alternative to overcome these limitations [16] [31]. For 2D spaces, each measured distance between the target station and a reference station provides a circle centered at the reference point, where the target station lies on. Figure 4.1 shows an example of trilateration [31] for locating a target position in 2D spaces. Trilateration utilizes three reference stations to determine the location of the target. The trilateration takes the distance along with coordinates of reference stations to calculate the position of the target station. The target station is located at the intersection of three circles, centered at each reference. The computed location is unique as long as three references are not aligned [14]. Therefore, accurate distance measurement between reference stations and the target station is one of the key issue in trilateration based IPL systems.

This section provides the necessary literature review relevant to the distance measurement in indoor environment. RSS based and TOA based distance measurement techniques are discussed in the following two sub-sections, respectively.

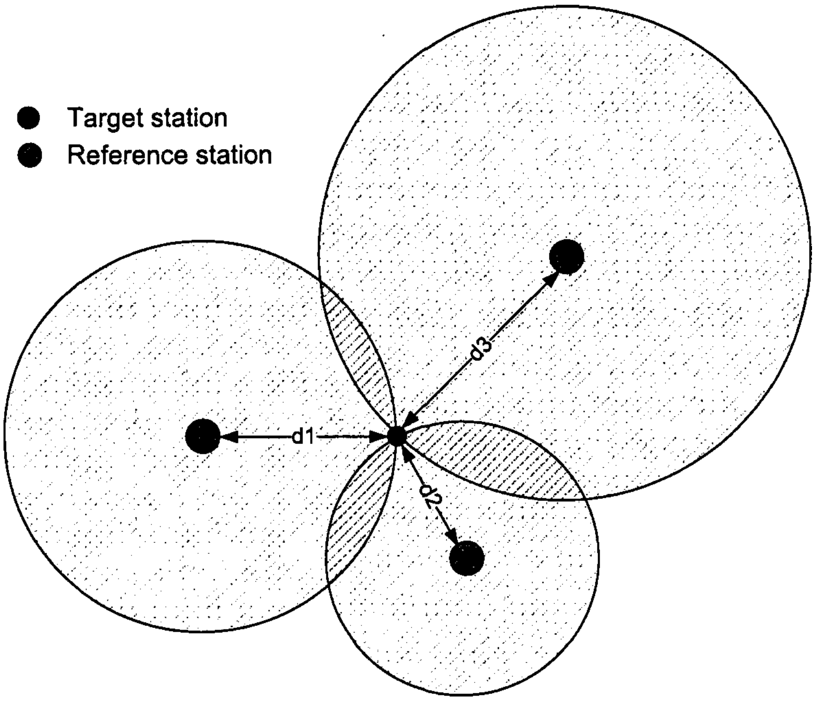


Figure 4.1: Trilateration based position location of a target station using three reference stations.

4.2.1 RSS Based Distance Measurement

RSS is a signal metric that most off-the-shelf wireless interfaces can measure. In the existing studies such as [5], [9] and [10], the RSS information is obtained from beacons of all active APs at the MAC layer of IEEE 802.11 WLANs are used as a metric for distance measurement and target positioning.

Theoretically, RSS measurements are inversely proportional to the distance between the transmitter and the receiver according to the path loss model, which portrays the signal power attenuation as the signal travels through the air. By employing suitable path loss model and necessary off-line training procedures, RSS based distance measurement methods can achieve good estimation accuracy. For acquiring suitable path loss model, it is common to perform a system calibration [51], where values of RSSI and distances are evaluated ahead of time in a controllable environment. The RSS based distance measurement method shows both advantages and disadvantages. The main advantage is its low cost and low timing requirements, because most receivers are capable of estimating the received signal strength without strict timing synchronization. The disadvantage is that in realistic environments, the measured RSS values are highly influenced by noises, surrounding environment and the type of antenna, which make the mathematical path loss model in indoor environments unreliable and highly site-specific, resulting in high inaccuracies of distance estimation.

Because of the fast time-variation of the signal strength at a given distance and difficulties of acquiring accurate signal propagation models for indoor environments, These methods have been demonstrated to be unreliable in real-world applications [47].

4.2.2 TOA Based Distance Measurement

TOA distance measurement techniques measure the time of a radio signal propagating from one station to the other. The propagation delay is directly proportional to the radio signal traveling distance. Given the propagation velocity of the radio signal in the air, the corresponding distance between two stations is easily computed. Two classes of TOA based techniques exist, namely, measuring the one-way trip time (OTT) and measuring the round-trip time (RTT).

In the former approach, the receiver has the knowledge of the start of signal transmission time, either by information attached in the received signal or by specially designed communication protocols. The TOA is then estimated by comparing the transmission time from the transmitter with the reception time at the receiver. The OTT based TOA measurements require strict synchronization between transmitter and receiver to ensure the estimation accuracy, thus making the implementation complex and costly. For the commercially available WLANs NICs, the precision of clock synchronization is insufficient for the deployment of OTT based distance measurement methods.

In the RTT method, the TOA is measured as follows: one wireless station, which is referred to the local station starts the time measurement by transmitting a frame to another station, which is referred to the remote station. The remote station replies to the local station as soon as the reception of the corresponding incoming frame sent from local station is completed. By comparing the time difference between the signal departure time and the corresponding replied signal arrival time at the local station, the RTT is then derived. The distance between two stations is determined by multiplying the measured RTT with the signal propagation velocity and then dividing by two. For IEEE 802.11 WLANs, the RTT based TOA measurements can be achieved by utilizing several existing frame exchange sequences between two stations, such as data/data, data/ACK, RTS/CTS and Probe-request/Probe-response. The RTT approach estimates the round-trip propagation time at the local station, hence the distance is completely determined by the clock of the local station. Therefore the requirement of timing synchronization is loosen, making the implementation simple and cost-effective. Based on these advantages, the RTT method for distance measurement is investigated in this work.

According to the layer where the TOA estimation are taken, the TOA based distance measurement techniques can be classified into two classes as introduced in the following two sub-sections.

4.2.2.1 TOA Estimation at PHY Layer

One of the popular methods which is often employed for TOA estimations is the PHY layer based approach. In this approach, TOA estimation algorithms have full capabilities of manipulating signals at the PHY layer. Dedicated hardware is required to execute corresponding signal processing algorithms to extract TOA information from PHY layer signals. OTT based TOA methods are usually employed for this approach because of the complete knowledge of PHY layer signals, the full control of the hardware and the high precision benefited from the dedicated hardware.

Super-resolution techniques are usually employed in these PHY layer TOA estimations. Super-resolution techniques have been studied in the field of spectral estimation [29]. Recently, a number of researchers have applied super-resolution spectral estimation techniques to time domain analysis. In the literature, the time-delay or TOA estimation problem has been studied with a variety of super-resolution techniques, such as the Matrix Pencil [8], root multiple signal classification (MUSIC) [27], and total least square-estimation of signal parameters via rotational invariance techniques (TLS-ESPRIT) [43]. While these super-resolution techniques can increase time-domain resolution, they also increase the system implementation complexity.

Other approaches employ correlation based methods to detect certain predefined signal structures in IEEE 802.11 frame, such as preambles and training symbols for TOA estimations. For example, in [40], the received signal is correlated with a locally-generated training sequence stored at the receiver to determine the TOA of signals. The channel frequency response is also obtained to refine the initial TOA estimation.

Although measuring the TOA directly at PHY layer signals can result in highly accurate distance estimates, it requires modifications to the WLAN NICs or even dedicated hardware to capture and process signals with extra high clock rate to guarantee high estimation resolution and precision. These additional requirements make these solutions impractical and incompatible for portable commercial IEEE 802.11 WLAN devices.

4.2.2.2 TOA Estimation at Upper Layers

To avoid the compatibility issues of PHY layer TOA estimations as previously mentioned, TOA estimations based on upper layer information is desired to make the implementation of WLANs based IPL systems more feasible with commercial WLAN devices. Since neither the

PHY layer signal nor interfaces of hardware for signal processing are exposed to upper layers by commercial WLAN NICs, this kind of TOA estimation has to focus on the utilization of upper layer features and capabilities provided by IEEE 802.11 standards. The RTT based TOA techniques are usually employed for the upper layer TOA estimations. This is because the RTT based TOA estimation does not require strict synchronization and it takes advantages of existing frame exchange sequences in IEEE 802.11 standards to perform TOA estimations. Such frame exchanges are standard compatible and have been implemented by commercially available WLAN devices.

Since the wireless signal propagates approximately at the speed of light, it is important to accurately estimate the RTT. For IPL applications, nanosecond time resolution is needed to limit the distance measurement error to the scale of a few meters. However, neither the current IEEE 802.11 standards nor the existing WLAN NIC chipsets provide timestamps with the sufficient time resolution. The IEEE 802.11 standard only specifies the timing synchronization function (TSF) with a resolution of 1 μs that can be accessed for stamping frame transmissions and receptions. 1 μs corresponds to a distance of approximately 300 m, which usually exceeds the range of WLANs coverage.

In order to overcome the problem of low resolution timestamps, most existing distance measurement approaches based on upper layer TOA estimations for IEEE 802.11 require modifications to the off-the-shelf WLAN NIC chipsets to acquire higher clock rate and precise timing information. These solutions are referred as hardware-assisted upper layer TOA distance measurement solutions. The internal delay calibration at both transmitter and receiver is employed in [30], using RTS/CTS frame exchanges. In [21] an accurate timestamp on transmission and reception is obtained by capturing a segment of the waveform and then performing a matched filter detection using the probe-request/probe-response exchange. In [18], authors proposed connecting a counter module to a WLAN NIC and using the clock of the connected counter module as the high resolution time base for stamping frame transmissions and receptions. The data/ACK frame exchange is employed for RTT measurement.

Most of the hardware-assisted solutions try to minimize the hardware changes so that their implementations in practice are more feasible than those aforementioned methods which work at the PHY layer. However, modifications to the hardware still introduce difficulties in system implementations and pure software based TOA distance measurement solutions for IPL systems, involving neither additional hardware nor hardware modifications, have been rarely explored.

4.3 Round-Trip Time based Distance Determination Using Frame Exchanges in IEEE 802.11

4.3.1 Frame Exchange Sequences in 802.11 WLAN

As introduced in Section 2.2 in Chapter 2, according to IEEE 802.11 standard, each transmitted data frame is required to be acknowledged by the receiver upon its successful reception after a short interframe spacing (SIFS) period. In the proposed distance measurement approach, we utilize this standard compatible feature to determine RTT, hence the distance between two IEEE 802.11 stations. Since the ACK frames are processed and generated by the NIC with the highest priority, the processing delay as well as random latency can be minimized.

To better illustrate the IEEE 802.11 frame exchange sequence, Figure 4.2 depicts a pair of ICMP ping request/response frame exchange as an example. The source station starts the transmission by sending out a ping request frame to the destination station. After the reception of the frame, the destination station NIC checks if the frame is received correctly. An ACK is sent back to the source station after a SIFS if no error is found in the last

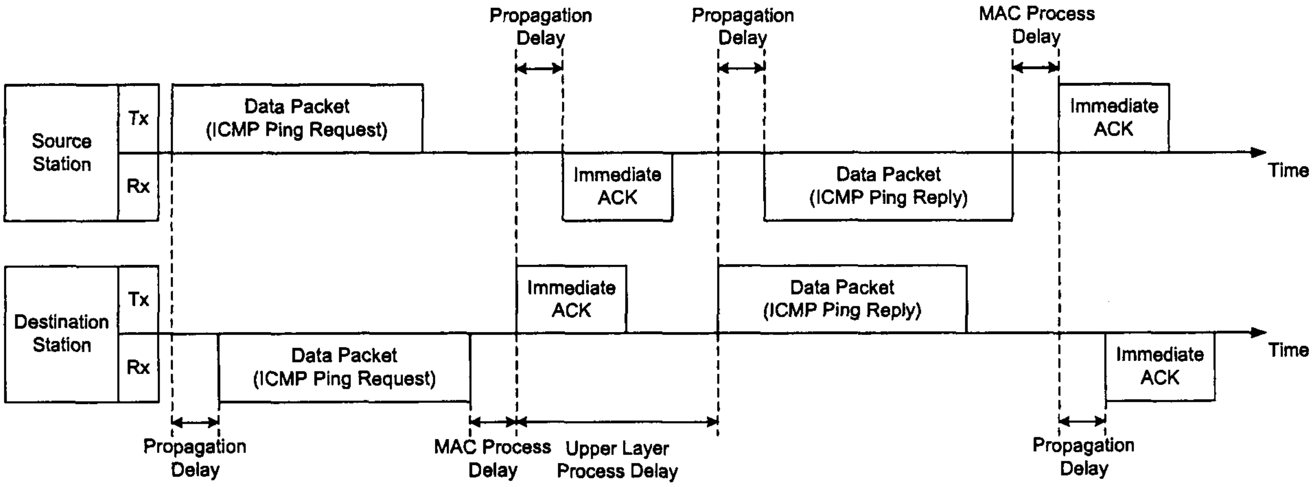


Figure 4.2: The ICMP ping request/response frame exchange sequence.

reception, indicating that the ping request is successfully received. The destination station NIC also passes the received frame to the driver and upper layer software applications running on the destination host machine for further processes. For the case of ping request, a ping reply is generated and sent back to the source station. Upon successful reception of the ping reply frame, the source station also sends an ACK to the destination station, indicating that the ping procedure finishes with success.

4.3.2 Round-Trip Time based Distance Measurement using data/ACK Frame Exchange Sequences

In the proposed distance measurement technique, the standard compatible data/ACK frame exchange sequence is employed to estimate the RTT, hence the distance between two communicating wireless stations. In this section, the timing sequence of IEEE 802.11 data/ACK frame exchange is analyzed in detail. In the following analysis, IEEE 802.11 OFDM PHY layer is focused.

The format of the frame for transmission, known as PLCP protocol data unit (PPDU) in IEEE 802.11, is constructed as shown in Figure 4.3. The PPDU includes the OFDM

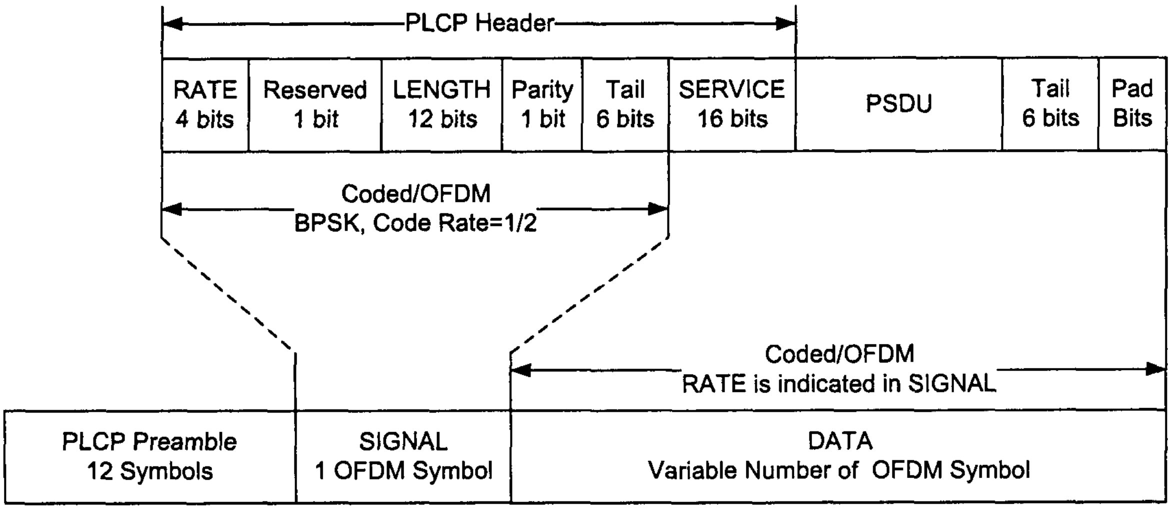


Figure 4.3: The format of IEEE 802.11 PLCP protocol data unit for frame transmissions.

PLCP preamble, OFDM PLCP header, PLCP service data unit (PSDU), tail bits, and pad bits. The PLCP header contains the following fields: LENGTH, RATE, a reserved bit, an even parity bit, and the SERVICE field. Among these PLCP header fields, the LENGTH, RATE, reserved bit, and parity bit (with 6 zero tail bits appended) constitute a separate single OFDM symbol, denoted as SIGNAL, which is transmitted with the most robust combination of BPSK modulation and a coding rate of R = 1/2. The SERVICE field of the PLCP header and the PSDU (with 6 zero tail bits and pad bits appended), denoted as DATA, are transmitted at the data rate described in the RATE field and may constitute multiple OFDM symbols.

The RTT is estimated from the data frame transmission and the corresponding ACK frame reception, as illustrated in Figure 4.4. To start the RTT estimation, the source station starts the transmission by sending a data frame at time instant $t_{\text{tx\_data\_start}}$. After a propagation delay of t_{prop}, the transmitted signal reaches the destination station. The time consumed by transmitting $(TXTIME)$ or receiving $(RXTIME)$ the frame can be expressed

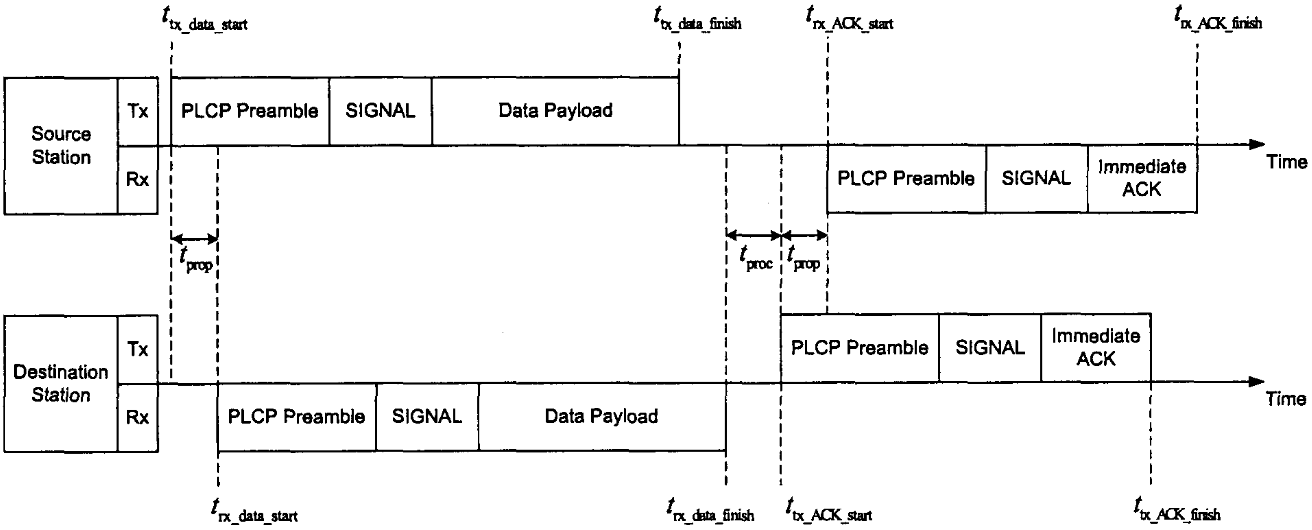


Figure 4.4: The timing sequence of IEEE 802.11 data/ACK frame exchange.

by

$$
\begin{aligned}
& TXTIME = RXTIME \qquad (4.1) \\
= \;& t_{\text{tx\_data\_finish}} - t_{\text{tx\_data\_start}} = t_{\text{rx\_data\_finish}} - t_{\text{rx\_data\_start}} \\
= \;& T_{\text{PREAMBLE}} + T_{\text{SIGNAL}} + T_{\text{SYM}} \times \text{Ceiling}\{(16 + 8 \times L_{\text{payload}} + 6)/N_{\text{DBPS}}\},
\end{aligned}
$$

where T_{PREAMBLE} is the duration of PLCP preamble; T_{SIGNAL} is the duration of the SIGNAL symbol; T_{SYM} is the duration of one OFDM symbol; L_{payload} represents the length of the data payload in bytes and N_{DBPS}, number of data bits per OFDM symbol, is derived from the employed modulation and coding scheme for the current transmission (refer to the column "Data Bits per OFDM Symbol" of Table 2.1 in Chapter 2 for detailed values of N_{DBPS}). Ceiling$\{\cdot\}$ is a function that returns the smallest integer value greater than or equal to its argument value. For IEEE 802.11 OFDM PHY with 20 MHz channel spacing, $T_{\text{PREAMBLE}} = 16\ \mu s$, $T_{\text{SIGNAL}} = 4\ \mu s$ and $T_{\text{SYM}} = 4\ \mu s$ [5].

At the time instant $t_{\text{rx\_data\_finish}}$, the data frame reception terminates at the destination station. The corresponding ACK is sent out upon successful reception of the data frame, after a SIFS delay or after the NIC at the destination station finishes processing the received frame at the PHY layer, whichever is larger. The SIFS time together with the processing time at the destination station is denoted by t_{proc}. Similarly to the data frame transmission, after a propagation delay of t_{prop}, the ACK frame reaches the source station and its reception terminates at time instant $t_{\text{rx\_ACK\_finish}}$. As a result, the value of RTT, t_{RTT}, can be calculated at the source station as

$$\begin{aligned} t_{\text{RTT}} &= t_{\text{rx\_ACK\_start}} - t_{\text{tx\_data\_finish}} \\ &= 2 \times t_{\text{prop}} + t_{\text{proc}}. \end{aligned} \tag{4.2}$$

The signal propagation time is then determined by

$$t_{\text{prop}} = \frac{t_{\text{RTT}} - t_{\text{proc}}}{2}. \tag{4.3}$$

Having the signal propagation time t_{prop}, the distance d between the source station and the destination station can be expressed as follows

$$d = c \times t_{\text{prop}}, \tag{4.4}$$

where c is the velocity of a radio wave propagates through the air ($c \approx 2.998 \times 10^8$ m/s) and t_{prop} is the propagation time in seconds calculated in (4.3).

4.3.3 Remaining Challenges

Although it is straightforward to calculate the distance between two communicating wireless stations by substituting equations (4.1)-(4.3) into (4.4), the proposed RTT based distance measurement approach still faces several challenges. First, the timestamp provided by

WLAN NICs has a discrete value with a resolution of 1 μs, corresponding to a distance resolution of 300 meters. This low distance resolution cannot provide a location precision that an IPL system is expected. Second, ACK frames are purely processed by the NIC hardware. Thus the software, including WLAN NIC driver and upper layer applications, is not notified upon the transmission and reception of ACK frames under normal operation mode, making the timing information related to ACK frames unavailable. Third, according to the timing synchronization function (TSF) specified by the IEEE 802.11 standard, the attachment of transmit timestamp is only mandatory for beacon frames, which are essentially multi-cast frames and require no ACK reply upon reception, making the timing information regarding to the data frame transmission is not available by default. Fourth, the local processing time, t_{proc}, is dependent on the traffic load at the PHY layer and is not provided by the WLAN NIC. In the following section, solutions for these technical challenges are discussed.

4.4 Round-Trip Time Resolution Enhancement

4.4.1 Problem Description

As described Section 4.3, the distance between two communicating wireless stations is estimated by calculating the round-trip signal propagation time from TOA of data frames and corresponding ACK frames. However, the continuous time domain TOA is assigned to one of the finite set of discrete values, referred as timestamps, while the original continuous TOA measurements are not available to the driver or other upper layers applications. As a result, the timestamps available at upper layers are no longer the TOA of the continuous time series, instead, they are discrete representations of the approximate TOA reported by the hardware with limited quantization resolution.

In order to generate frame timestamps, the continuous time is discretized with a res-

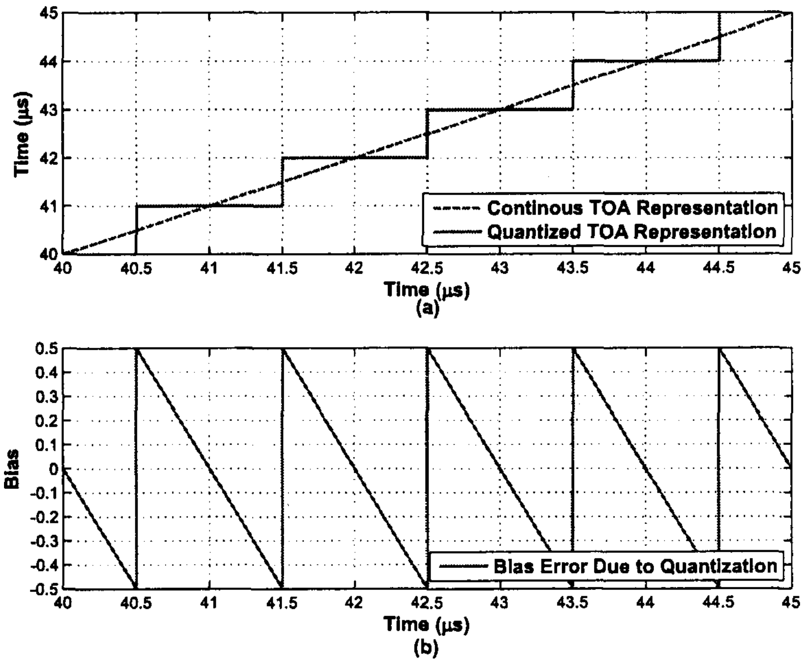


Figure 4.5: Effects of quantization and the corresponding bias error. (a) Continues TOAs and corresponding quantized values. (b) Bias caused by quantization.

olution of 1 μs and the closest discrete value to the frame arrival time is selected as the frame arrival timestamp. Figure 4.5 presents an illustrated example of this timestamp discretization process. The upper plot shows how continuous TOAs discrete are assigned to timestamps, while the lower plot shows the corresponding discretization errors. For example, if a frame arrives between 41.5 μs and 42.5 μs, a timestamp of 42 μs will be assigned to that frame. The minimum discretization error occurs when a frame arrives at the discrete timestamp and the maximum error occurs when a frame arrives at the middle of two consecutive discrete timestamps.

The discretization of the continuous time measurement generates a maximum error of 0.5 μs, which equals to 150 m when converting the signal propagation time to distance. This distance estimation error is even larger than the coverage of IEEE 802.11 WLANs which is generally less than 100 m. Therefore, an RTT estimation resolution of a nanosecond is required to obtain an estimation precision of several meters.

To improve the accuracy of the TOA estimated from the discrete timestamp reported by the hardware, average can be taken over a large number of consecutive RTTs. An interesting result is that an average of TOA measurements only gives a significant resolution improvement if the TOA measurement in the continuous time domain is not "too perfect". In the cases that the TOA measurement error in the continuous time domain is suitably large, several adjacent quantization levels are excited to some extent. Then the TOA measurement error will act as an interpolation mechanism among adjacent quantization levels, giving results at intermediate values between these levels after averaging, thus increasing the resolution of the TOA measurements. This method is based on the assumption that the frame arrival time estimation errors in the continuous time domain, generated by the WLAN NICs, are symmetrically distributed around zero [6] [7]. The details of the method are presented in subsequent sections.

4.4.2 Proposed Solution

4.4.2.1 Mathematical Background

Denote τ as the true TOA value at which the frame arrives at the NIC, let τ_m signify the frame arrival time measured by WLAN NICs in the continuous time domain. The measurement error in the continuous time domain is dependent on the NIC characteristics and we assume a Gaussian distribution for simplicity. With the Gaussian assumption of measurement errors, the NIC measured frame arrival time τ_m is distributed as a Gaussian distribution with the width σ_τ and the mean τ. Therefore, the probability density function (PDF) of TOA measurement τ_m in the continuous time domain is

$$p_{\tau_m}(\tau_m) = \frac{1}{\sqrt{2\pi}\sigma_\tau} e^{-\frac{1}{2\sigma_\tau^2}(\tau_m - \tau)^2}. \tag{4.5}$$

The continuous frame arrival time τ_m is then quantized with a quantization step $\Delta\tau = 1\ \mu s$ by assigning the closest discrete timestamp, t_i, to the frame arrival time, where t_i is the discrete time represented by the ith timestamp bin of a finite set of discrete timestamps.

Since there is no preference for frame arrival time, it is assumed to be uniformly distributed in the ith discrete arrival time bin, $\left(t_i - \frac{\Delta\tau}{2}, t_i + \frac{\Delta\tau}{2}\right)$, and therefore, the quantization error is uniformly distributed in the interval $\left(-\frac{\Delta\tau}{2}, \frac{\Delta\tau}{2}\right)$. As a result, the PDF of quantization error is a rectangular with a width of $\Delta\tau$ and height of $\frac{1}{\Delta\tau}$, centered at the origin.

Subsequently, the PDF of the continuous TOA measurement τ_m assigned to each possible discrete timestamp bin can be considered as integrating the Gaussian PDF (4.5) of the arrival time measurement τ_m over the quantization interval $[-\Delta\tau/2, \Delta\tau/2]$ centered around each timestamp bin t_k, where $t_k = k\Delta\tau$. As suggested by [37], such integrating procedure can be treated as convolving the Gaussian PDF in (4.5) with a rectangle having width $\Delta\tau$ and height $\frac{1}{\Delta\tau}$, and then multiplying the result by a sampling function comprising an infinite train of delta functions along the abscissa, spaced $\Delta\tau$ apart, and each having an area of $\frac{1}{\Delta\tau}$. Consequently, the mean value and the variance of this new PDF can be calculated by evaluating the first and second derivatives of the composite characteristic function at the origin. The average of n discrete random variables is denoted by t.

The characteristic function [36] of the Gaussian PDF (4.5) is given by

$$\Phi_{\tau_m}(\omega) = e^{j\tau\omega - \frac{1}{2}\sigma_\tau^2\omega^2} \tag{4.6}$$

and the PDF of the quantization error, which is an unit area rectangle, has an inverse Fourier transform given by

$$\Phi(\omega) = \frac{\sin(\omega\Delta\tau/2)}{\omega\Delta\tau/2}. \tag{4.7}$$

Therefore, the convolution between the Gaussian PDF in (4.5) and the rectangle quantization error PDF is equivalent to multiplying (4.6) with (4.7).

The process of multiplying the resultant PDF from previous multiplication by the sampling function spaced $\Delta\tau$ apart is represented in the transform domain by the convolution of the characteristic function with the inverse Fourier transform of the sampling function, which is a similar sampling function in the transform domain, comprising an infinite train of unit area delta functions spaced $\frac{2\pi}{\Delta\tau}$ apart along the ω axis. This is equivalent to simply replicating the characteristic function along the ω axis at intervals of $\frac{2\pi}{\Delta\tau}$. The resultant composite characteristic function is

$$\Phi_t(\omega) = \sum_{k=-\infty}^{\infty} \frac{\sin(\omega\Delta\tau/2 - \pi k)}{\omega\Delta\tau/2 - \pi k} e^{j\tau(\omega - \frac{2\pi k}{\Delta\tau}) - \frac{1}{2}\sigma_\tau^2(\omega - \frac{2\pi k}{\Delta\tau})^2}. \tag{4.8}$$

The mth moment of the PDF of t can be obtained from m times of differentiation operations relative to ω [36]. That is

$$D^{(m)}\Phi_t(\omega)|_{\omega=0} = j^m E(t^m). \tag{4.9}$$

As indicated in (4.9), the first and second moments of the PDF of the TOA estimation t assigned to discrete timestamps can be obtained from (4.8) by two differentiation operations, relative to ω. The calculation can be facilitated by factoring each term into three or four simpler expressions. Then, the rules for differentiating products and quotients can be applied to construct the final result from these simpler forms [37]. The mean value of TOA estimation t becomes

$$E(t) = \tau + \frac{\Delta\tau}{\pi} \sum_{k=1}^{\infty} \frac{(-1)^k}{k} e^{-2\left(\frac{k\pi\sigma_\mathcal{T}}{\Delta\tau}\right)^2} \sin\left(\frac{2\pi k\tau}{\Delta\tau}\right). \tag{4.10}$$

Equation (4.10) is a Fourier sine series representation of the mean value. When the frame TOA measurement in the continuous time domain has no error, i.e., $\sigma_\mathcal{T} = 0$, the

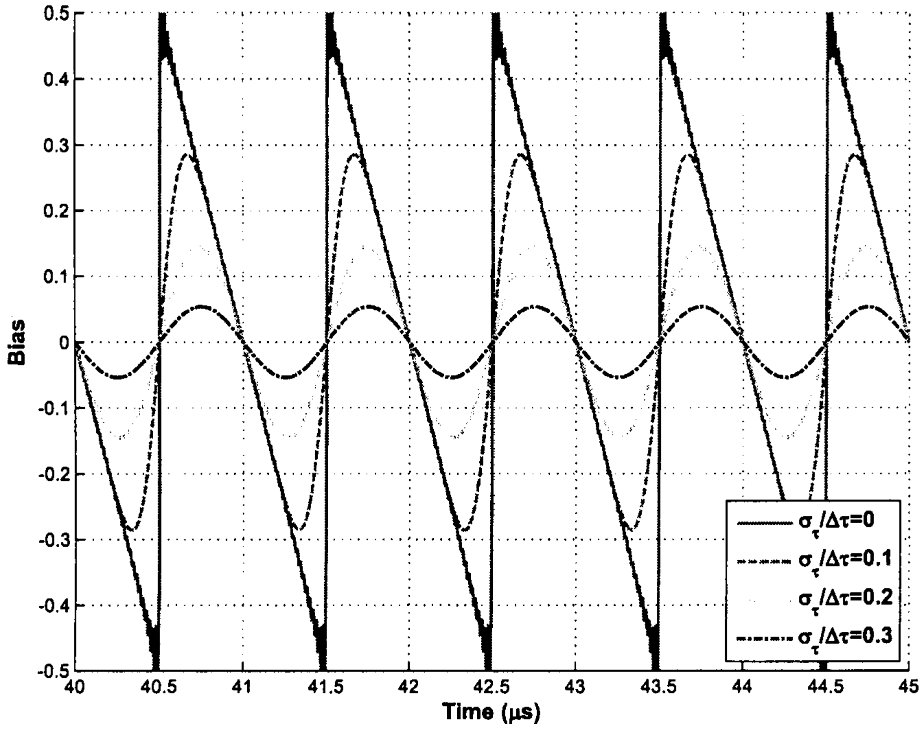


Figure 4.6: Effect of averaging over quantized noised signal.

maximum frame timestamp error is equal to half of the quantization step, i.e., 0.5 μs. In this case, the entire bias error is caused by the quantization and the TOA estimation bias curve is a negative going repetitive "sawtooth" shape centered about the origin, with a peak amplitude of $\pm\frac{\Delta\tau}{2}$ and a period of $\Delta\tau$.

Figure 4.6 illustrates the bias error $e_t = E(t) - \tau$ for a few values of the normalized standard deviation of the frame arrival time estimation error in the continuous time domain, $\sigma_T/\Delta\tau$. The solid blue curve represents the case $\sigma_T = 0$ and has the same shape as the bias curve shown in Figure 4.5. This proves the consistency of the result given by (4.10) with the one shown in Figure 4.5. One observes in this figure that as the estimation error σ_T in the continuous time domain increases, the resultant averaged TOA estimation error decreases. This observation can be further explained by the measured timestamp histogram, for example the one in Figure 4.7.

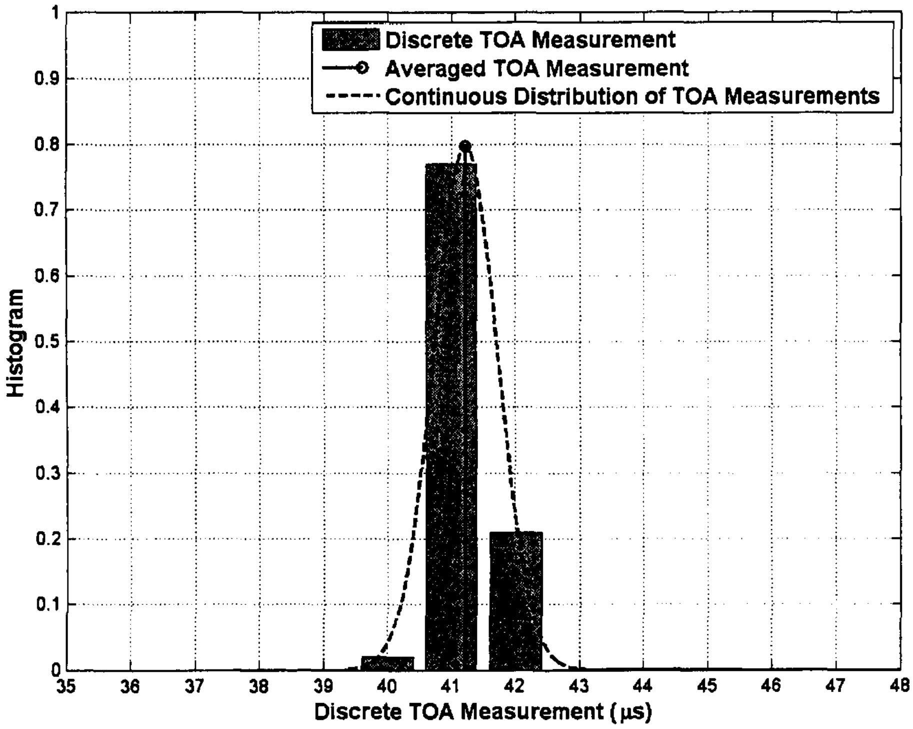


Figure 4.7: The theoretical histogram of discrete timestamps.

In Figure 4.7, the real frame arrival time lies within the interval [40.5, 41.5]. If the WLAN NIC observes this arrival time precisely, i.e., $\sigma_T = 0$, the arrival frames are always assigned a timestamp of 41 μs. As we increase the number of measurements, the assigned timestamps do not change and as a result, the averaged timestamp is also 41 μs and the histogram is a rectangular at interval [40.5, 41.5] with a unit height. This causes an estimation error as large as 0.5 μs to the RTT based TOA estimation. On the other hand, if the NIC of the wireless station estimates the frame arrival time in the continuous time domain with a variance σ_T greater than zero, it is possible that the frame arrival time falls into interval [40.5, 41.5] as well as its neighboring timestamp bins, intervals [39.5, 40.5] and [41.5, 42.5]. As a result, the measured values of frame arrival time are stamped with timestamps 41 μs and possibly, 40 μs and 42 μs. In this case, the frame timestamp histogram includes several rectangles with different heights, for example, as being observed in Figure 4.7. As the number of collected frame timestamps increases, the averaged RTT based TOA estimation over multiple timestamps can result in a value closer to the real TOA, therefore decreases the estimation error.

4.4.2.2 Error Estimation of Averaged TOA over Discrete Timestamps

In practice, only the first term ($k = 1$) in (4.10) is significant and the averaged TOA estimation t over multiple timestamps can be simplified as

$$E(t) \approx \tau - \frac{\Delta\tau}{\pi} e^{-2\left(\frac{\pi\sigma_T}{\Delta\tau}\right)^2} \sin\left(\frac{2\pi\tau}{\Delta\tau}\right). \tag{4.11}$$

According to the approximation given in (4.11), the bias error $e_t = E(t) - \tau$ is sinusoidal and its peak value is

$$(e_t)_{\text{peak}} = \pm\frac{\Delta\tau}{\pi} e^{-2\left(\frac{\pi\sigma_T}{\Delta\tau}\right)^2}. \tag{4.12}$$

In the situation that the arrival time measurement standard deviation is half of the quantization step, $\sigma_T = \frac{\Delta\tau}{2}$, the peak error is $\pm 0.002289\Delta\tau$. Figure 4.7 shows an example of discrete timestamp measurements, where $\tau = 41.2147$ μs, $\Delta\tau = 1$ μs, $\sigma_T = \frac{\Delta\tau}{2}$. The resultant averaged TOA is 41.2125 μs, giving an error of -0.0022 μs in time, or -0.3347 m in distance. This is consistent with what is expected from (4.12).

4.4.2.3 Frame timestamp Error Variance Estimation

The frame timestamp error variance calculation is more difficult, but a good approximation is [37]

$$\sigma_t^2 \approx \frac{1}{n}\left[\sigma_T^2 + \frac{(\Delta\tau)^2}{12}\right] - \frac{1}{n}\left[4\sigma_T^2 + \left(\frac{\Delta\tau}{\pi}\right)^2\right] e^{-2\left(\frac{\pi\sigma_T}{\Delta\tau}\right)^2} \cos\left(\frac{2\pi\tau}{\Delta\tau}\right). \tag{4.13}$$

The cosine term in (4.13) is normally very small due to the exponential factor and can be ignored in most cases. This gives the variation on the average of n of these quantized random variables as

$$\sigma_t^2 \approx \frac{1}{n}\left[\sigma_T^2 + \frac{(\Delta\tau)^2}{12}\right]. \tag{4.14}$$

The simplified equation for the variation on the average of n of these discrete timestamps (4.14) is something that we expected, since according to the probability theory, variances are added when two functions are convolved together. In (4.14), the first term is the variance of the Gaussian distributed TOA measurement in continuous time domain before quantization, and the second term is the variance of the rectangle quantization error PDF.

4.4.2.4 Required Number of Collected Frames

We use two criterions to evaluate the distance measurement, and equivalently the RTT measurement, including the maximum error and the error variance. Since the distance and the RTT are essentially equivalent, and the RTT is derived from discrete timestamps, we will evaluate the precision of frame timestamp estimation instead of distance measurement. The maximum error of the TOA estimation t which averages over multiple timestamps is presented in (4.12) while its variance is evaluated in (4.14).

In (4.12), the maximum error is dependent on the standard deviation of frame arrival time measurement in the continuous time domain, σ_T, and not on the number of collected frames. As this standard deviation increases, the maximum frame timestamp error decreases. However, the frame arrival time measurement error is NIC-dependent and in most situations, this information is not available.

In (4.14), the frame timestamp estimation error is dependent on the number of the collected frames, whose timestamps are used for the averaging calculation. If the timestamp error variance is required to be smaller than an upper bound σ_{max}^2, the required number of collected frames are calculated as

$$n > \frac{12\sigma_\tau^2 + (\Delta\tau)^2}{12\sigma_{\max}^2}. \tag{4.15}$$

4.4.2.5 Summary of RTT based TOA Estimation Using Averaging Method

In this section, we briefly describe our distance measurement technique, based on the analysis and discussion presented so far. The round-trip propagation time is calculated from data frame timestamp and its corresponding ACK frame timestamp by using (4.2) and (4.3). In order to reduce the error variance, a certain number of RTT measurements will be collected and used to calculate the averaged round-trip propagation time. The number of required samples is determined by (4.15). The distance between two stations is derived from the averaged round-trip propagation time, according to (4.4).

The measured distances between a target station and reference stations will be used to determine the location of the target, using trilateration technique, as presented in Section 4.5. The implementation of the presented technique and technical challenges are discussed in Section 4.6.

4.5 Determining the Location in 2D Spaces

In this section, the method of trilateration for determining a location on a 2D surface is introduced. Recall Figure 4.1 which shows the principles of the trilateration method: the target station is located at the intersection of three circles, center at three different reference stations. Unlike triangulation, which uses angle of arrivals together with at least one known distance to calculate the target location, trilateration uses three reference points with known locations together with measured distance between the target and each reference point to determine the location of the target.

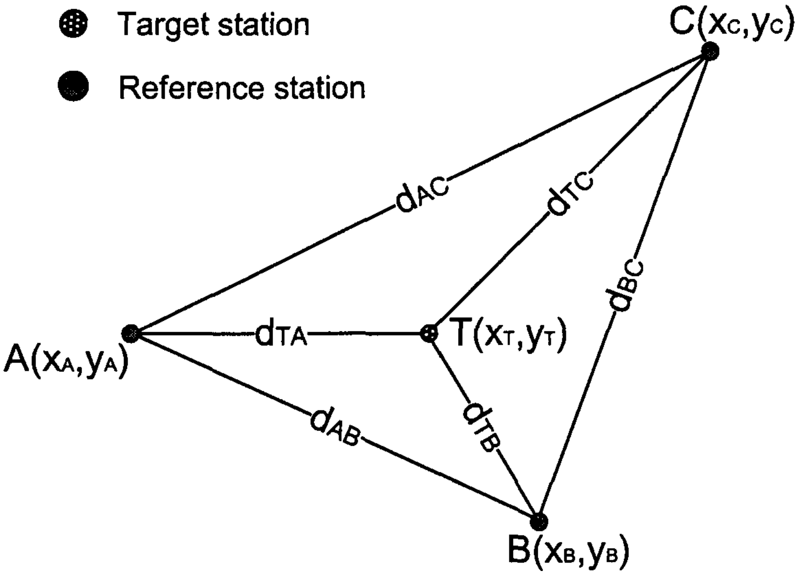


Figure 4.8: Example of solving the triangle for localization.

Figure 4.8 shows an example using the trilateration method for locating a target with three known reference points. Three reference points, A, B and C, are on a 2D surface with known positions, (x_A, y_A), (x_B, y_B) and (x_C, y_C), respectively. These three reference points must not be aligned to uniquely determine the target position. The distance between each reference points, namely d_{AB}, d_{AC} and d_{BC} can be expressed as follows

$$\begin{aligned} d_{AB} &= \sqrt{(x_B - x_A)^2 + (y_B - y_A)^2}, \\ d_{AC} &= \sqrt{(x_C - x_A)^2 + (y_C - y_A)^2}, \\ d_{BC} &= \sqrt{(x_C - x_B)^2 + (y_C - y_B)^2}. \end{aligned} \tag{4.16}$$

Denote T as the target position to be localized with coordinates (x_T, y_T). After applying suitable distance measurement technique, distances between T and each reference point, d_{TA}, d_{TB} and d_{TC}, are determined. Therefore, the task of localizing the target position is converted into solving the coordinates (x_T, y_T) with the knowledge of three distances from the target to three known reference points. According to Figure 4.8, the distance between

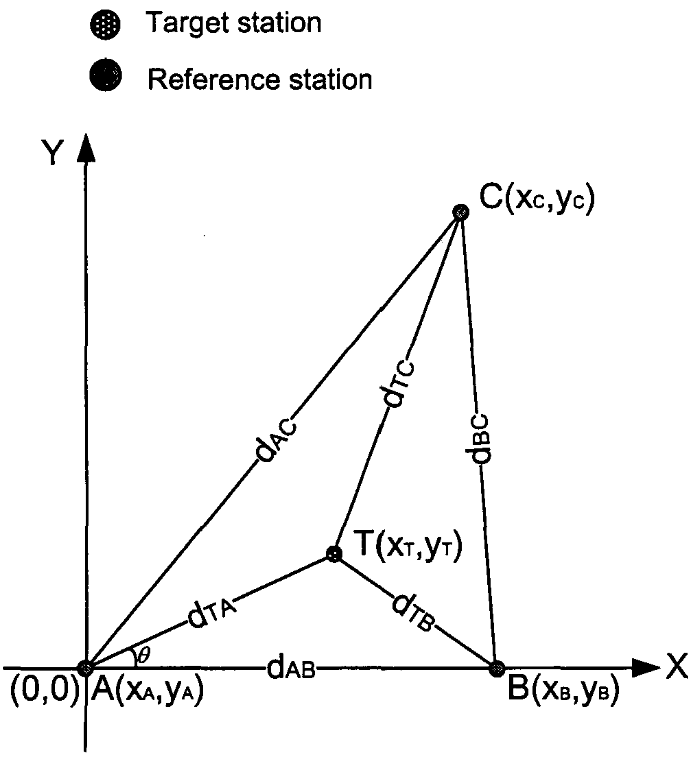


Figure 4.9: Example of axis rotation for simpler target cordinates calculation.

the target station and three references points can be represented by

$$\begin{aligned} d_{TA} &= \sqrt{(x_T - x_A)^2 + (y_T - y_A)^2},. \\ d_{TB} &= \sqrt{(x_T - x_B)^2 + (y_T - y_B)^2}, \\ d_{TC} &= \sqrt{(x_T - x_C)^2 + (y_T - y_C)^2}. \end{aligned} \tag{4.17}$$

In (4.17), we have three equations with two unknowns, which can be solved to find an unique solution. To simplify the calculation of the target coordinates, it is reasonable to rotate ΔABC and align one side of the triangle to one of the 2D axis. As shown in Figure 4.9, the side AB of ΔABC is aligned to the X-axis and A is considered as the origin.

By applying the cosine rule to distances between target T to reference point A and B, we have

$$d_{TB}^2 = d_{TA}^2 + d_{AB}^2 - 2d_{TA}d_{AB}\cos\theta. \tag{4.18}$$

Rearranging (4.18) gives

$$\cos\theta = \frac{d_{TA}^2 + d_{AB}^2 - d_{TB}^2}{2d_{TA}d_{AB}}. \tag{4.19}$$

The value of $\cos\theta$ in (4.19) can be solved since all the distances used in (4.19) have been obtained in the previous measurements. Therefore, the coordinates of target point T can be determined by

$$\begin{aligned} x_T &= d_{TA} \cdot \sin\theta \\ y_T &= d_{TA} \cdot \cos\theta. \end{aligned} \tag{4.20}$$

Note that at this point, the angle θ can not be uniquely determined by (4.19) since ambiguous cases may happen for $\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$. This ambiguity shows that the position of the target cannot be uniquely located with only two reference points. For general scenarios, a third reference point is required to resolve this ambiguity by examining the distance between calculated coordinates and the third reference point. The one fulfills the following equation

$$d_{TC}^2 = (x_C - x_T)^2 + (y_C - y_T)^2, \tag{4.21}$$

should be accepted as the correct coordinates of the target location.

However, the aforementioned ambiguity caused by using two reference points can also be avoided in some practical applications by placing the two reference points at some particular locations. For example, as shown in Figure 4.10, by placing two reference points along one of the external walls of a building, one of the solutions of angle θ, which results in coordinates that fall outside of the building, is considered as invalid and thus can be eliminated. The target location is then uniquely determined based on such setups.

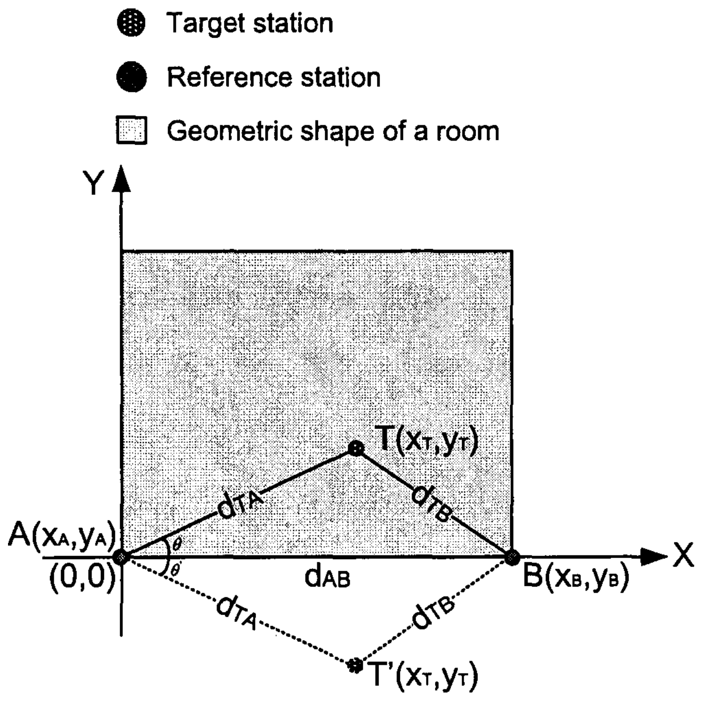


Figure 4.10: Reference point setup to eliminate ambiguity in position location.

Note that in realistic scenarios, the imperfection of distance estimations as well as the inaccurate position information of reference points pose challenges to compute positions using the trilateration method. The circles in Figure 4.1 may not intersect at one point, resulting in a target area rather than a single target location. The uncertainty in distance estimations has motivated number of researches in the literature for locating a target station. One example of such approaches is a probabilistic based method proposed in [45], where errors in distance estimations are modeled as normal random variables. Since this chapter mainly focuses on the estimation of distance between two communicating WLAN stations, the localization algorithm will not be addressed in details.

4.6 System Implementation

In this section, the implementation of the proposed distance measurement approach is presented using commercially available IEEE 802.11 WLAN NICs.

In this approach, the timestamp for each frame is measured by the WLAN NIC rather than the operating system (OS) to minimize the software-dependent latencies. The IEEE 802.11 data/ACK sequence is used to estimate the RTT between two communicating wireless stations. In IEEE 802.11 standard, upon the reception of a data frame at the receiver, an ACK is sent back to the transmitter after a delay of SIFS. The SIFS is 10 μs for IEEE 802.11b/g and 16 μs for IEEE 802.11a. Then, the distance between the two stations is calculated from the estimated RTT.

The reason using the data/ACK sequence instead of data exchange sequences, such as the ICMP ping request/respond sequence, to calculate the RTT is that responses generated by upper layer software applications, such as ping response, are subject to high variable delay introduced by the working load and scheduling schemes of the host OS. In contrast, the immediate ACK is purely handled by the hardware of the WLAN NIC and therefore the latency is more stable and predictable.

4.6.1 The Monitor Station Aided RTT Measurement

As stated in Section 4.3.3, beside the problem of limited resolution provided by frame timestamps for RTT based TOA estimation, there still remains multiple challenges for the implementation of IEEE 802.11 based distance measurement technique for IPL systems using commercial WLAN NICs. To make use of data/ACK frame exchange sequences to determine RTTs between two communicating stations, the exact time of the data frame transmission and the corresponding ACK frame reception are required. However, the driver and upper layer software applications are not aware of the transmission and reception of ACK frames in normal communications since ACKs are purely handled by WLAN NICs. Furthermore, the exact time that the NIC starts the data frame transmission is also not available at driver or upper layer applications.

In order to overcome these problems, a third station, called the monitor station, is employed. In the following, principles of the monitor station is introduced in Section 4.6.1.1, followed by the monitor aided RTT measurement presented in Section 4.6.1.2. In the end of this section, the method to extract timestamps and other information from frames observed by the monitor station is introduced.

4.6.1.1 The Monitor Station

A monitor station is an IEEE 802.11 wireless station that is configured to operate in the monitor mode. In this special mode, the transmit ability of the NIC is disabled to avoid the monitor station from generating any wireless traffics that may cause interferences. On the other hand, the NIC of the monitor station passes all the frames received by its interface to the driver, regardless of the type or the source/destination of the frame. This offers an opportunity for the driver and the upper layer software applications to fully observe the frame exchange sequences in the air and perform subsequent processing.

With the help of the monitor station, all desired frames for RTT calculations are treated as received frames at the monitor station. This avoids the problem that the driver and upper layer software applications, working in the normal stations, are not aware of the ACK frame transmission and cannot observe the exact time of frame transmissions.

4.6.1.2 The Monitor Station Aided RTT Measurement

In this section, the RTT calculation that has been introduced in Section 4.3.2 is modified to take the monitor station into consideration. In the monitor station aided RTT measurement, the monitor station is placed together with the source stations so that the propagation time from the source station to the monitor station is considered as zero. In this sense, the source station is referred as location station, and the destination station is called remote station in the following context. Figure 4.11 illustrates the timing sequence of one pair of typical IEEE

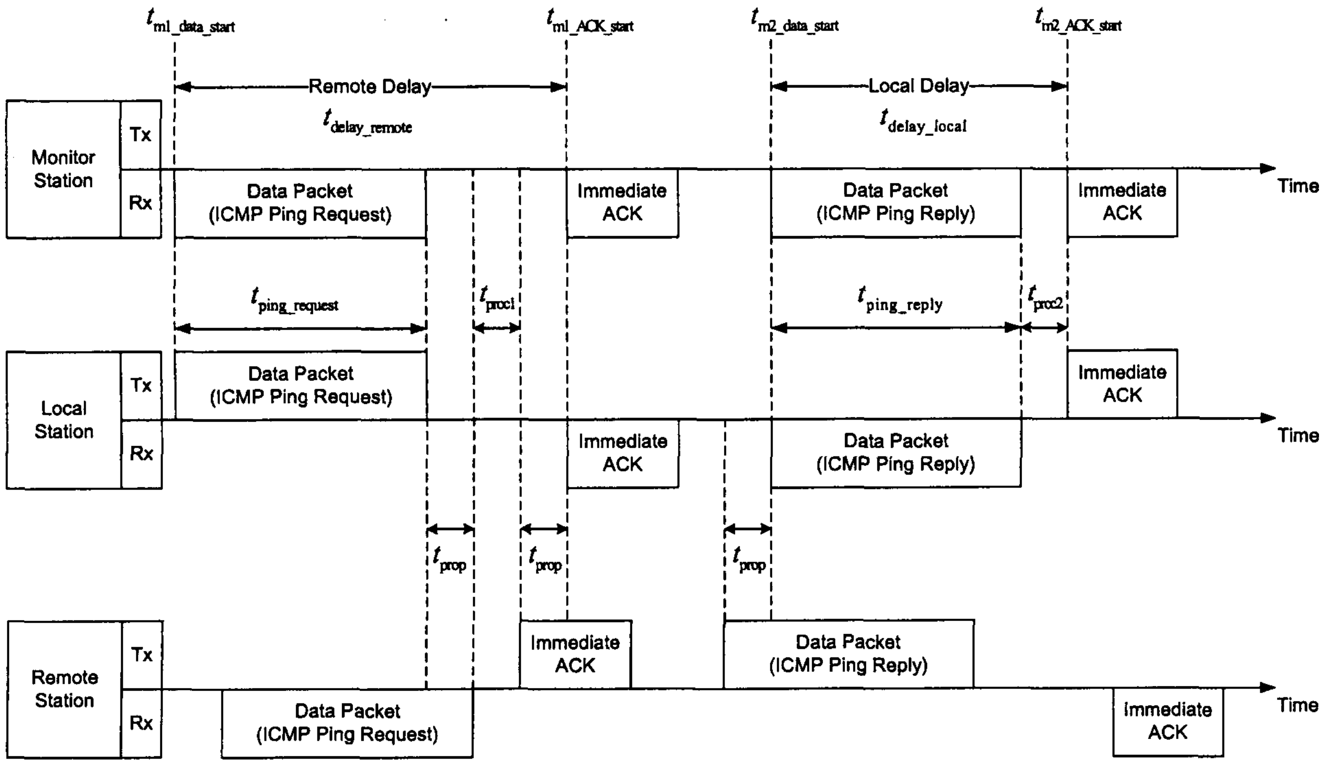


Figure 4.11: The monitor station aided data/ACK timing sequence.

802.11 data/ACK frame exchange sequence. The ICMP ping is employed as an example to demonstrate the procedure without losing generality.

For each ICMP ping request/reply frame exchange, four timestamps are recorded by the monitor station: $t_{\text{m1\_data\_start}}$, $t_{\text{m1\_ACK\_start}}$, $t_{\text{m2\_data\_start}}$ and $t_{\text{m2\_ACK\_start}}$, as shown in Figure 4.11. Since the monitor station is placed together with the source station, the propagation time between the monitor station and the source station can be considered as zero. The collected four timestamps can be approximately treated as the time corresponding to events occur at the source station.

Using these four timestamps, two time intervals, namely $t_{\text{delay\_remote}}$ and $t_{\text{delay\_local}}$, are calculated by

$$t_{\text{delay\_remote}} = t_{\text{m1\_ACK\_start}} - t_{\text{m1\_data\_start}} \tag{4.22}$$

and

$$t_{\mathrm{delay\_local}} = t_{\mathrm{m2\_ACK\_start}} - t_{\mathrm{m2\_data\_start}}, \tag{4.23}$$

where $t_{\mathrm{delay\_remote}}$ refers to the time duration since the start of an ICMP ping frame transmission at the local station until the corresponding ACK frame replied from the remote station is received at the local station; and $t_{\mathrm{delay\_local}}$ represents the time duration since the start of an ICMP ping reply reception until the start of the corresponding ACK frame transmission, both at the local station.

The $t_{\mathrm{delay\_remote}}$ in (4.22) can be rewritten into

$$\begin{aligned} t_{\mathrm{delay\_remote}} &= t_{\mathrm{m1\_ACK\_start}} - t_{\mathrm{m1\_data\_start}} \\ &= t_{\mathrm{prop}} + t_{\mathrm{ping\_request}} + t_{\mathrm{proc1}} + t_{\mathrm{prop}} \\ &= 2t_{\mathrm{prop}} + t_{\mathrm{ping\_request}} + t_{\mathrm{proc1}}, \end{aligned} \tag{4.24}$$

where $t_{\mathrm{ping\_request}}$ is calculated using (4.1) based on the current employed modulation and coding scheme for data transmission as well as the size of the data payload of ICMP ping request, t_{proc1} represents the time period that the remote station WLAN NIC hardware processes the received ping request frame or a period of SIFS, whichever is larger.

Similarly, $t_{\mathrm{delay\_local}}$ in (4.23) can be rewritten into

$$\begin{aligned} t_{\mathrm{delay\_local}} &= t_{\mathrm{m2\_ACK\_start}} - t_{\mathrm{m2\_data\_start}} \\ &= t_{\mathrm{ping\_reply}} + t_{\mathrm{proc2}}, \end{aligned} \tag{4.25}$$

where $t_{\mathrm{ping\_reply}}$ is also calculated using (4.1) based on the current employed modulation and coding scheme for data transmission as well as the size of the ICMP Ping reply payload, t_{proc2} represents the time period that the local station WLAN NIC hardware processes the received ping reply frame or a SIFS period, whichever is larger.

Therefore, the propagation time t_{prop} can be expressed by combining equations (4.24) and (4.25), as follow

$$\begin{aligned} t_{\text{prop}} = \frac{1}{2} &\times [(t_{\text{delay\_remote}} - t_{\text{delay\_local}}) \\ &- (t_{\text{ping\_request}} - t_{\text{ping\_reply}}) \\ &- (t_{\text{procl}} - t_{\text{proc2}})]. \end{aligned} \tag{4.26}$$

In (4.26), one difficulty in calculating the desired signal propagation time t_{prop} is that the hardware processing time at both remote and local station, t_{procl} and t_{proc2} are not directly available. The processing time of the local station, t_{proc2} can be estimated with the two timestamps $t_{\text{m2\_data\_start}}$ and $t_{\text{m2\_ACK\_start}}$ along with frame length and employed modulation coding scheme for the corresponding frame. However, the processing delay introduced by the remote station, t_{procl} is unknown at the monitor station and cannot be directly calculated using the observed timing measurements. This yet poses another advantage of using a monitor station for measuring the RTT. Although the delay introduced by the WLAN NIC is varying from one frame reception to another because of the working load variation, the processing delay at the remote station and the local station can be treated approximately the same for the same hardware platform. Therefore, the local processing delay t_{proc2} can be used as an approximation of t_{procl} as

$$t_{\text{procl}} \approx t_{\text{proc2}}. \tag{4.27}$$

Substituting (4.27) into (4.26), we have

$$
\begin{aligned}
t_{\text{prop}} = \frac{1}{2} \quad \times & \quad ((t_{\text{delay\_remote}} - t_{\text{delay\_local}}) \\
- & \quad (t_{\text{ping\_request}} - t_{\text{ping\_reply}})).
\end{aligned} \tag{4.28}
$$

To extract timing information for RTT based TOA measurements, the monitor station needs the access to the IEEE 802.11 frame header fields, which contains modulation type, frame length, and MAC timestamps so that the desired propagation time in (4.28) can be calculated. In Section 4.6.1.3, the method to obtain the MAC timestamp and employed modulation coding scheme will be introduced in detail.

Furthermore, in the scenario that the transmission rate and frame size of data and control frames is controllable, it is then possible to further simplify the procedure by setting identical transmission rate and frame size for both local and remote stations. By doing so, the calculation of t_{prop} can be further simplified as

$$
t_{\text{prop}} = \frac{1}{2}(t_{\text{delay\_remote}} - t_{\text{delay\_local}}). \tag{4.29}
$$

Equation (4.29) avoids the information extractions and numerical calculations about the frame header type, header length, the payload length, the modulation scheme as well as the hardware process delay, so that the computational cost of RTT estimation can be minimized, making the solution easy to be implemented.

4.6.1.3 Information Extraction from Radiotap Header

The MAC timestamp of a frame is measured by the WLAN NICs upon the reception of the frame. It is then stored in a specific chipset header structure, so that it can be accessed by driver and upper layer software applications. Three different chipset header types, namely

Version (8 bits)	Padding (8 bits)	Length (16 bits)	Presence Flag (32 bits)	Radiotap Fields (Variable bits)

Figure 4.12: The Radiotap header structure and the subsequent Radiotap data field.

PrismHeader, AVS, and the RadioTap headers, are usually implemented depending the types of NICs as well as drivers. Usually, the device drivers have to be configured properly to provide one of these headers.

The Radiotap is designed to balance the need of a hardware-independent, extensible capture format against the need to conserve CPU and memory bandwidth on embedded systems. It is supported by many WLAN NIC vendors, such as Atheros, Broadcom and Intel. The Radiotap header is a mechanism to supply additional information about frames from the driver to user-space applications such as libpcap, and from a user-space application to the driver for transmission. The Radiotap header provides more flexibility for reporting the characteristics of a frame than the legacy Prism or AVS header allows. As shown in Figure 4.12, it allows the driver developer to specify an arbitrary number of data fields by configuring the *Presence Flag* field in the Radiotap header. An IEEE 802.11 NIC driver that supports Radiotap will define its own data structures and embed an instance of an *ieee80211_Radiotap_header* structure at the beginning, followed by subsequent data fields. The *Presence Flag* bitmap is set accordingly to indicate data field presence.

Among the data fields defined for the Radiotap header, the desired frame reception timestamp is extracted by accessing the *IEEE80211_RADIOTAP_TSFT* field of the Radiotap header by the monitor station. This field contains an unsigned 64-bit value, measured in microseconds, of the MAC's 802.11 TSF timer. In theory, for each received frame, this value is recorded when the first bit of the MPDU arrives at the MAC layer. With the timestamps of the data and corresponding ACK frames, both $t_{\text{delay\_remote}}$ and $t_{\text{delay\_local}}$ in (4.28) can be calculated by substituting the corresponding frame reception timestamps for data/ACK frame exchange pairs into (4.24) and (4.25), respectively.

Besides timestamps, the modulation and coding scheme employed by the captured data frame can be also extracted from the Radiotap header for the calculation of the duration of data frame $t_{\text{ping\_request}}$ and $t_{\text{ping\_reply}}$. However, these calculations are not trivial, because the chipsets do not provide information on the PHY preamble used for transmission. For example, the IEEE 802.11g standard supports three different preambles: long (1 Mbps), short (2 Mbps) and g-only (OFDM) preambles, which all have different transmission durations. To overcome this difficulty, a list of all possible preamble types and their corresponding durations should be prepared before the measurement according to standard specifications. When the monitor station starts capturing frames, the measured values can be compared with theoretically calculated values in the pre-prepared list. The closest type of preamble is then considered to be valid and therefore can be used for further calculations.

4.7 Summary

In this chapter, a distance measurement technique is proposed for IPL systems based on existing IEEE 802.11 WLANs infrastructures. The position of a target wireless station is determined by distances between the target and preset reference stations, using the trilateration method. The distance between two wireless stations is estimated by calculating the round-trip propagation time of the monitored data frame and corresponding ACK frame arrival timestamps. In order to improve the RTT estimation accuracy, an averaging method is presented, which profits from the frame arrival time measurement error in the continuous time domain to lower the averaged round-trip propagation time estimation error. The implementation of the presented technique, as well as solutions to technical challenges, are also described.

Chapter 5

Field Tests of Proposed Protocol-based Indoor Position Location Technique

In Chapter 4, a protocol-based distance measurement approach has been presented for estimating distance between two communicating WLAN stations using standardized IEEE 802.11 data/ACK frame exchange sequences. In this chapter, field tests are conducted to evaluate the performance of the distance measurement technique proposed in Chapter 4. All the field tests are carried out in a typical office building (Thompson Engineering Building at the University of Western Ontario) where WLAN APs/stations and other wireless devices co-exist with the distance measurement system to be evaluated.

In the conducted tests, both LOS and NLOS scenarios are considered. Distance is measured with WLAN devices that either have identical platforms (same OS and same WLAN NICs chipset) or non-identical platforms (different OSs and WLAN NICs chipset) to justify the impact of software/hardware platforms to the performance of the presented approach. A preliminary localization system that utilizes the proposed distance measurement technique is also demonstrated in this section for locating a target IEEE 802.11 WLAN station in typical indoor environments.

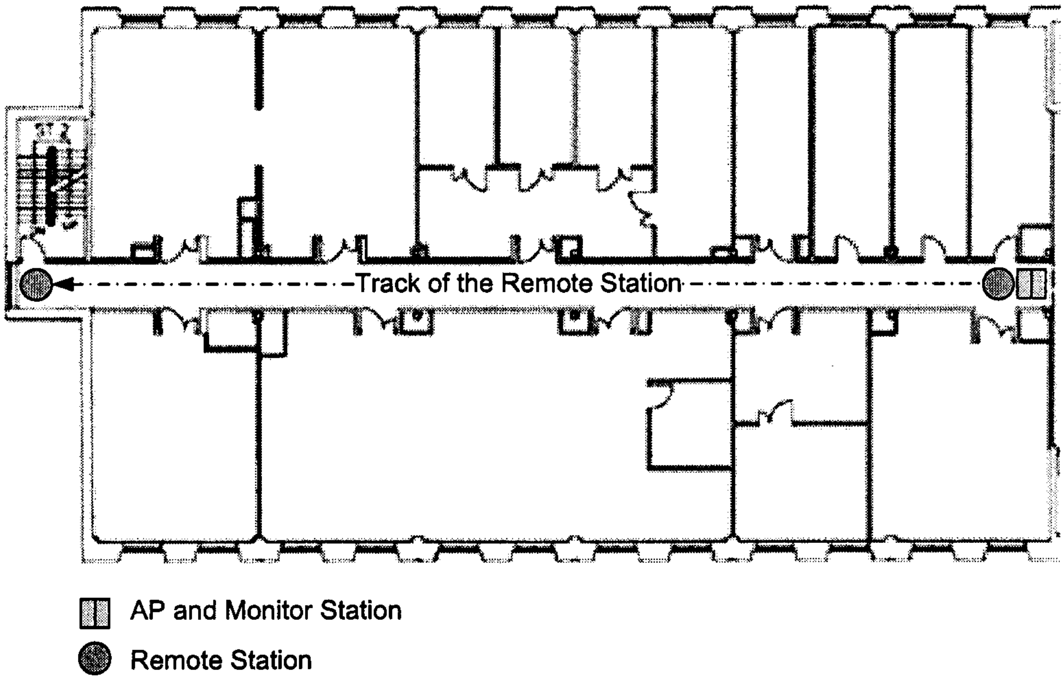


Figure 5.1: The floor plan layout for the LOS test campaign.

5.1 Line-of-sight Test

In this section, the LOS test is conducted. Configurations and the equipment setup, together with measurement results are presented in the following.

5.1.1 Equipment Configurations

The LOS test campaign is done in the hall way as shown in Figure 5.2. The local station and the remote station are configured as IEEE 802.11 station and AP respectively. The third station is configured as the monitor station and is placed together with the local station as shown in Figure 5.2 to capture data/ACK frame exchange sequences between two communicating stations. All three stations are placed about 1.5m away from ground to guarantee a large percentage of the Fresnel-zone, which is an elliptic space around the direct LOS between both stations that free of any obstacles harming the transmission. Moreover, all three stations are equipped with identical Atheros AR5004X wireless platform, which

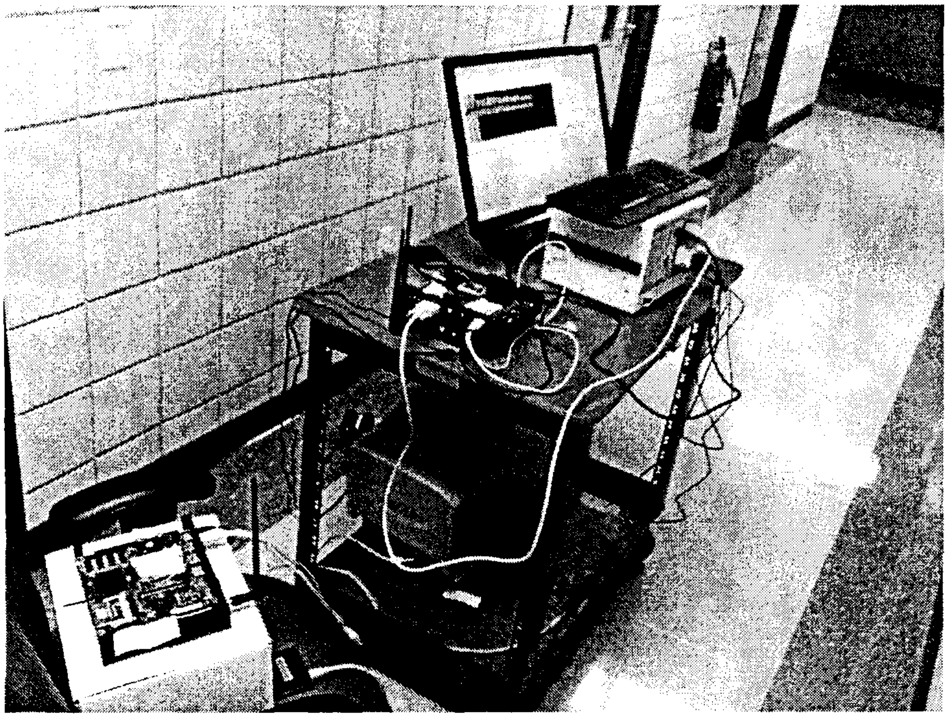


Figure 5.2: Station placement for the LOS test campaign.

consists of an AR5213 MAC chipset and an AR5212 radio chipset. FreeBSD 8.2-stable GENERIC kernel is installed for all three stations as host OS.

The distance to be measured ranges from 0 m to 40 m and tests are conducted for every 4 meters. In each measurement, ICMP ping is employed to generate traffics between the local station and the remote station. The local station is set to transmit ICMP ping request to the remote station every 10 ms until 15000 packets are collected by the monitor station. The modulation coding scheme is chosen to be convolutional coded 16-QAM with a coding rate of $\frac{2}{3}$ for data frame transmission at both two communicating stations. This modulation coding scheme provides a fixed data rate transmission of 36Mbps as shown in Table 2.1 in Chapter 2. According to the analysis given in 4.6.1.2 in Chapter 4, the fixed rate minimizes the measurement variation caused by RAA so that (4.29) can be applied for calculating the round trip propagation time t_{prop}. Since each uni-cast ICMP ping request addressed to one receiver is immediately acknowledged if it is received without errors, an ACK with a rate

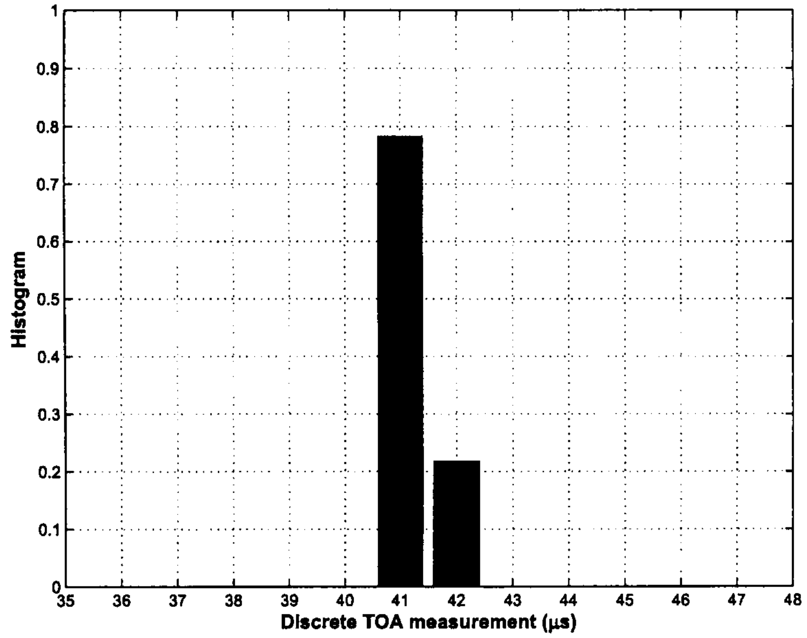


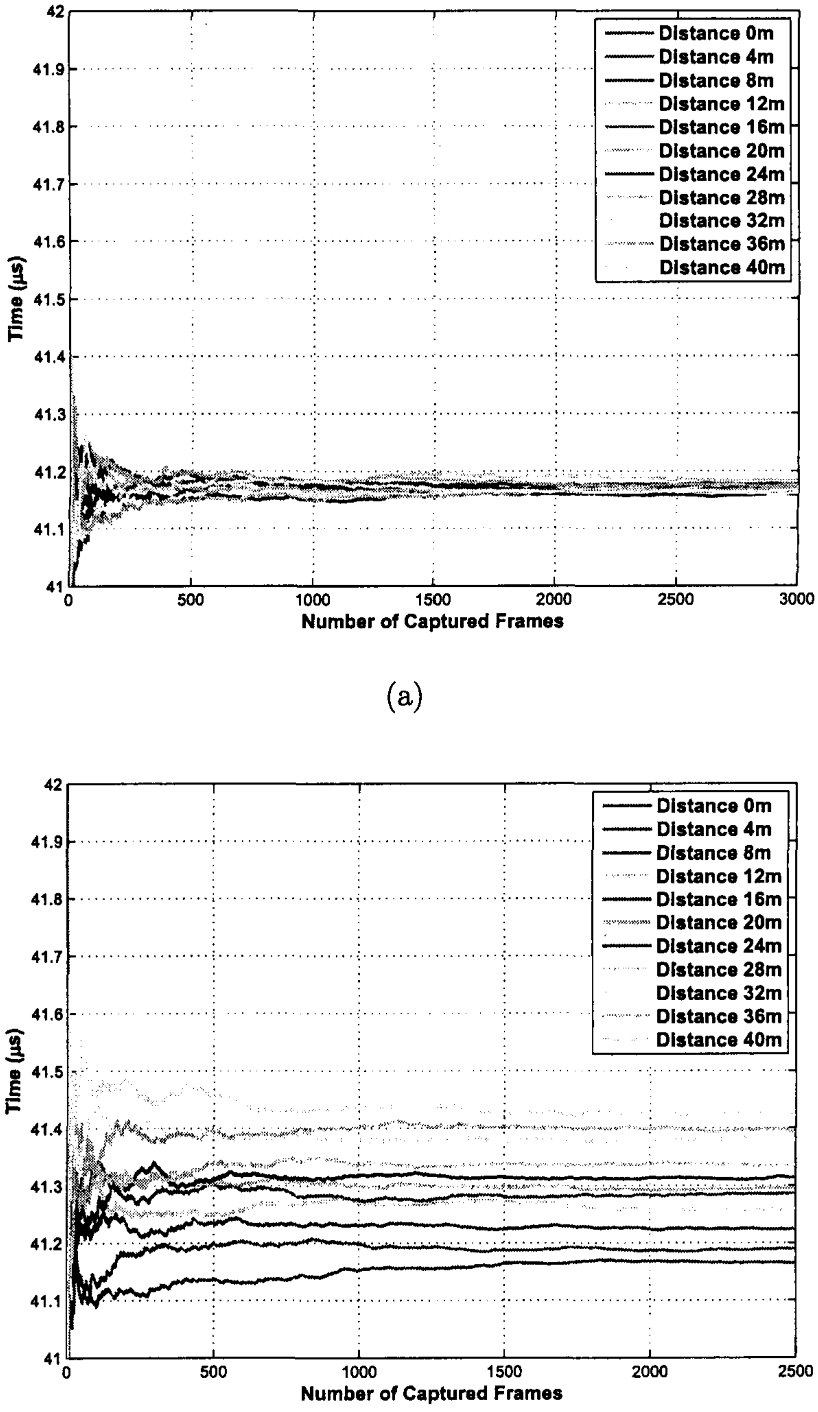
Figure 5.3: The histogram of measured discrete Timestamps of $t_{\mathrm{delay\_remote}}$ at the distance of 8m.

of 24Mpbs is instantaneously sent out after the arrival of the ICMP ping request plus an SIFS. With these two rates and the time difference to be measured, corresponding distance between two remote stations can be estimated. To avoid potential packet retransmission effects, the maximal number of allowed retransmissions is set to zero in all measurements.

Calibration should be initially carried out in the 0m distance in which the remote and local stations are placed close to each other to remove the estimation bias.

5.1.2 Test Results

Figure 5.3 shows the histogram of measured discrete timestamps at the distance of 8 m. It can be seen that the distribution of the discrete timestamps is close to the result in Figure 4.7 under the assumption that the additive noise is Gaussian distributed with the mean equal to the averaged RTT and variance σ_T equal to 0.35.



(a)

(b)

Figure 5.4: The convergence of averaged measurement values in the LOS case: (a) $t_{\text{delay\_local}}$; (b) $t_{\text{delay\_remote}}$.

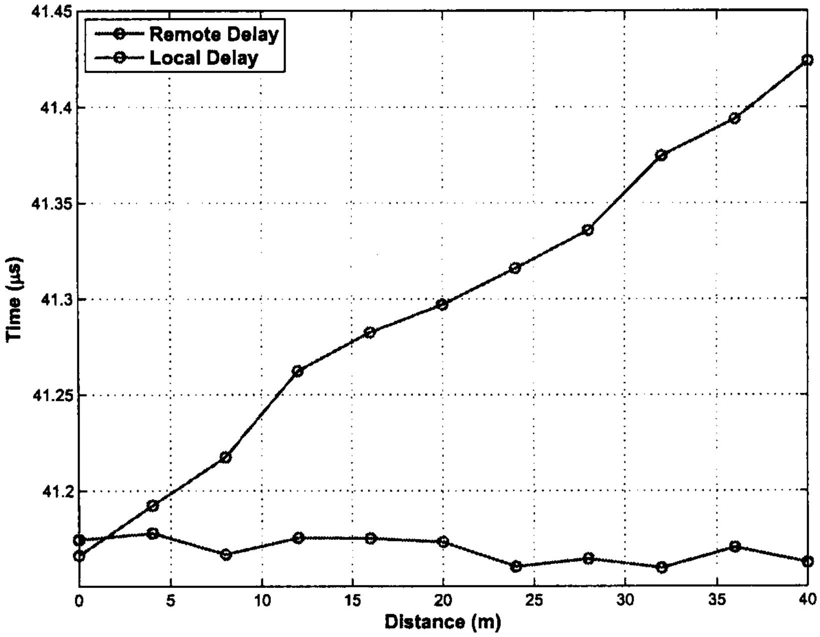


Figure 5.5: The averaged $t_{\text{delay\_local}}$ and $t_{\text{delay\_remote}}$ at each measured distance in the LOS test campaign.

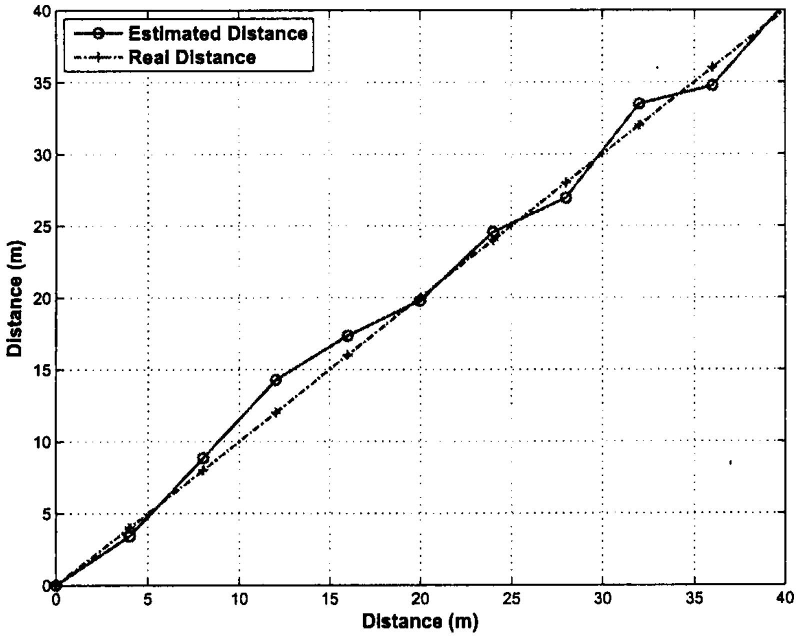


Figure 5.6: The estimated distance compared with real distance in the LOS test campaign.

Figure 5.4 shows the convergence of averaged RTT measurements. For both local and remote stations, the measured TOA value tends to be less fluctuated after averaging 1500 valid measurement samples or more at all measured distances.

The averaged $t_{\text{delay\_remote}}$ and $t_{\text{delay\_local}}$ to be used to calculate the final propagation time t_{prop} in (4.29) are shown in Figure 5.5. The estimated distance is shown in Figure 5.6 along with the real distance as a reference. The estimated distance is close to the real distance where the maximum estimation error is 2.2685m and the minimum error is only 0.2136m.

This estimation precision proves that the protocol-based distance measurement approach is able to be extended to future IPL systems with a high accuracy.

5.2 Non-line-of-sight Test

In this section, the NLOS test is conducted. Configurations and the equipment setup, together with measurement results are presented in the following.

5.2.1 Equipment Configurations

Unlike of the previous LOS test campaign, in this test, the local station and the monitor station are placed inside a isolated office away from the hall way as shown in Figure 5.7 to grantee the non-line-of-sight (NLOS) transmission. The rest of the settings are the same as in the previous LOS test campaign.

5.2.2 Test Results

The averaged $t_{\text{delay\_remote}}$ and $t_{\text{delay\_local}}$ are shown in Figure 5.8 and the estimated distance is shown in Figure 5.9. Compared with results obtained in LOS measurements, variations

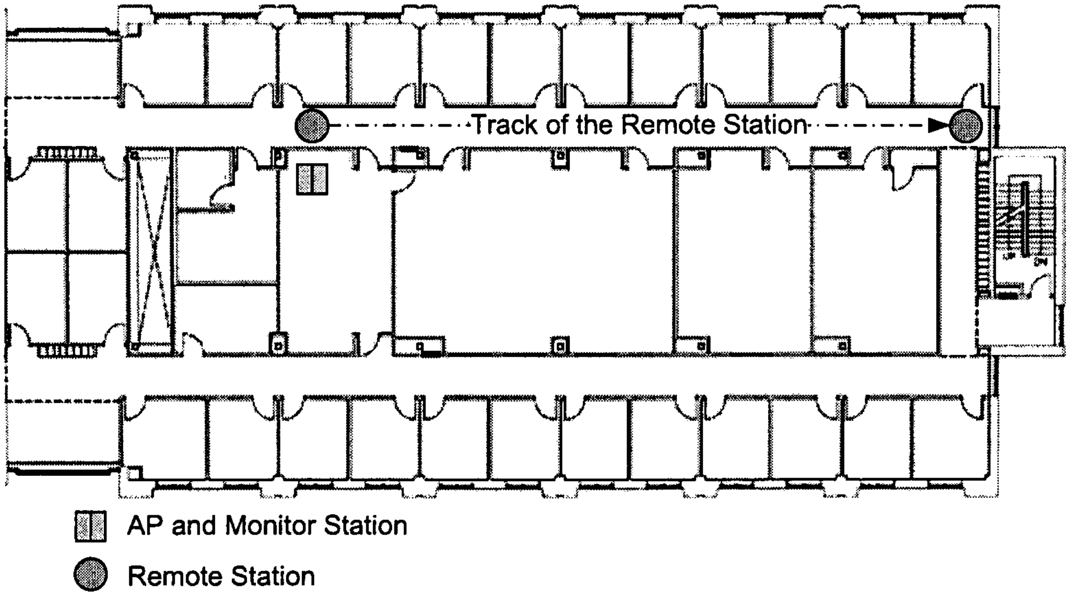


Figure 5.7: The floor plan layout for the NLOS test campaign.

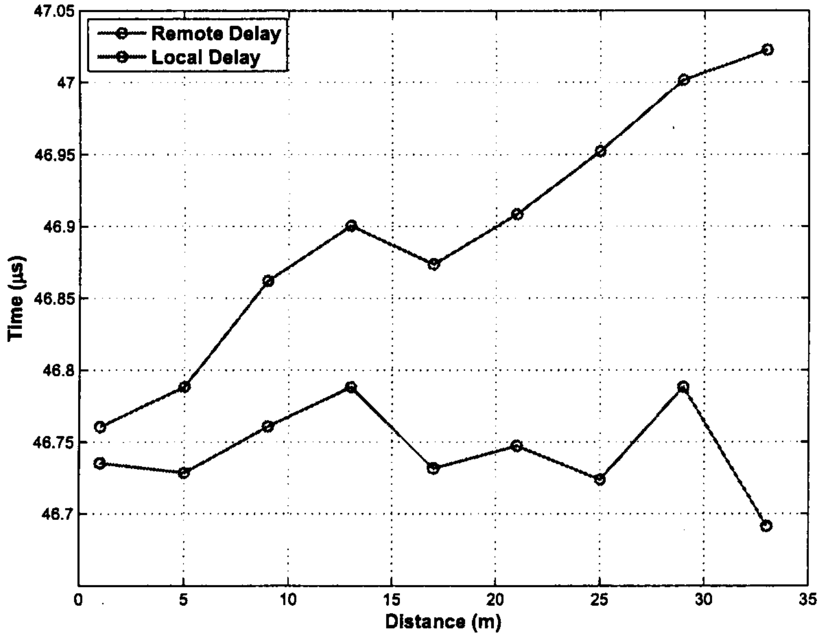


Figure 5.8: The averaged $t_{\text{delay\_local}}$ and $t_{\text{delay\_remote}}$ at each measured distance in the NLOS test campaign.

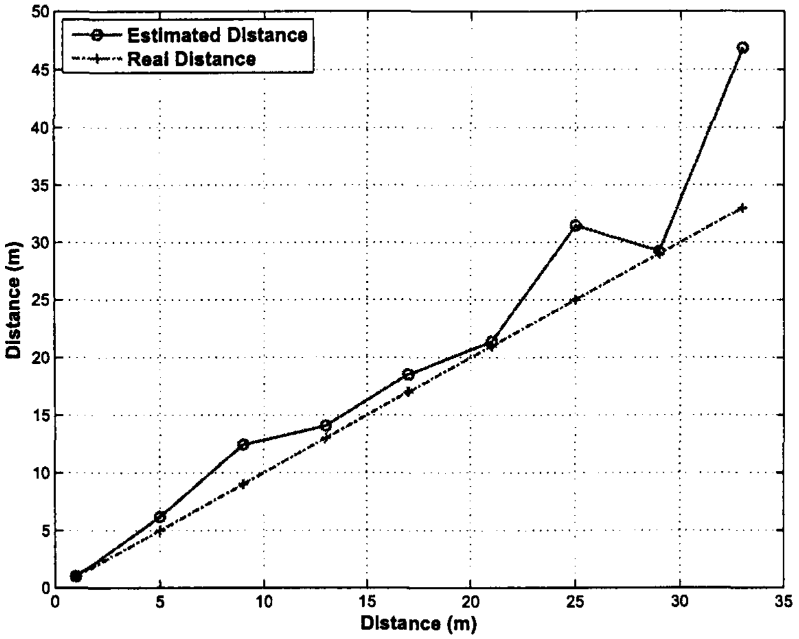


Figure 5.9: The estimated distance compared with the real distance in the NLOS test campaign.

of the averaged RTT values of both local and remote delay are much larger, which result in a larger distance estimation error. This is because in NLOS measurements, DP is not the FDP at the receiving station and the FDP at the receiver is highly time-dependent and location-dependent, the chance that DP is not FDP at the receiving station is larger than it in the LOS test, thus causing a larger variation of the estimated result.

It is also observed that, compared with the result in LOS measurement, the estimated distance in NLOS measurement is larger than the real distance in each measurement. This is not surprising because in the NLOS scenario, or more generally, NDDP scenario, the DP transmission is blocked or weakened by obstacles during the signal propagation. Therefore, the receiver has to rely on either reflected or refracted version of the original signal as an approximation of DP for estimating FDP. These signals with non-DP propagation path have longer propagation delay compared with DP. As a result, the distribution of TOA measurements at the receiver side is no longer symmetrical and measurements with values that greater than the real propagation time are dominant. Consequently, averaging over these measurements results in a positive distance estimation bias at all distances. However, averaged values of TOA measurements are still used as estimations for the NLOS measurement because the actual TOA distribution of non-DPs is difficult to be obtained in realistic.

5.3 Line-of-sight Test with Non-identical Stations

In previous two test campaigns, the hardware platform of two communicating stations as well as the monitor station are identical to each other. However, in more practical cases, the hardware and software platform of one wireless station is not necessarily the same as it in other stations. To evaluate the impact of non-identical stations to the performance of the proposed distance measurement technique, in this section, LOS tests with non-identical stations are conducted. Detailed equipment configurations and corresponding measurement results are presented in the following.

5.3.1 Equipment Configurations

In this measurement campaign, instead of using two identical Atheros WLAN NICs with FreeBSD OS as the local and remote station, the NIC of the remote station is replaced by a Broadcom BCM4312 IEEE 802.11 a/b/g WLAN NIC and the host OS of the remote station is replaced by the Windows 7 Home edition.

Since the driver for BCM4312 for Windows is not an open-source driver, no code-level modifications or adjustments can be done to the driver. Moreover, no special configurations are performed to the host OS except for changing the firewall rules to allow ICMP traffics between the local station and the remote station. The non-identical platforms are more close-to-real because in realistic at least one station evolved in distance measurement and

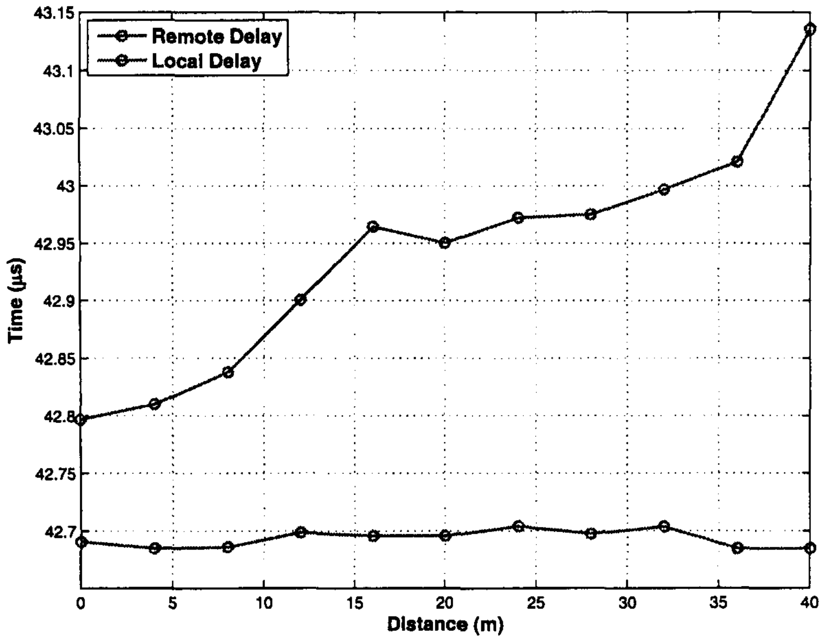


Figure 5.10: The averaged $t_{\text{delay\_local}}$ and $t_{\text{delay\_remote}}$ at each measured distance in the non-identical station test campaign.

IPL systems may use a completely different hardware/software platform and can not be customized for the IPL purpose even at the software level.

Since the remote station is not specially configured for this distance measurement, the RAA implemented in the driver of the remote station WLAN NIC is then responsible for adaptively selecting transmission rate for both data frames and ACK frames. In order to calculate the desired signal propagation time t_{prop} for estimating the distance between two stations, (4.28) should be employed instead of (4.29) to take the different transmit durations introduced by different transmission rates into consideration.

The rest of the settings remain the same as in the LOS test campaign.

5.3.2 Test Results

The averaged $t_{\text{delay\_remote}}$ and $t_{\text{delay\_local}}$ measurements as well as the estimated distance are shown in Figure 5.10 and Figure 5.11, respectively.

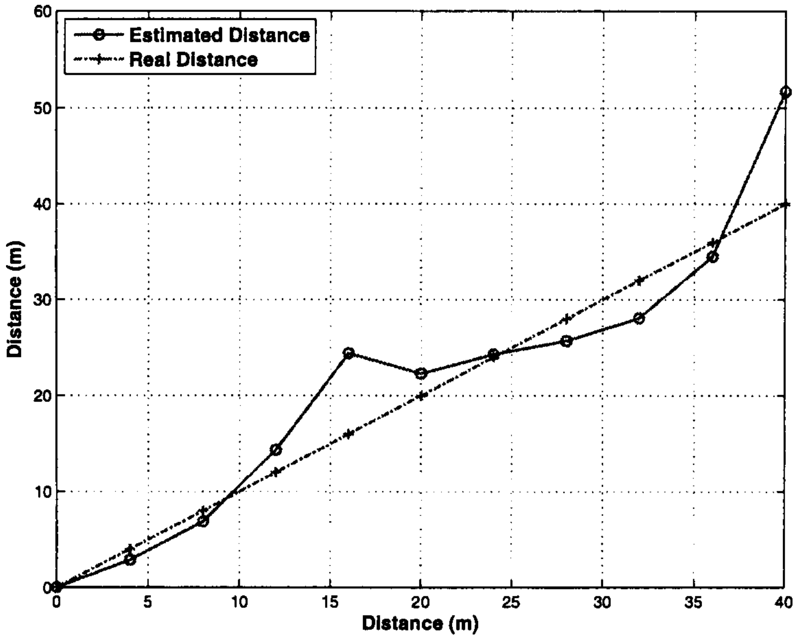


Figure 5.11: The estimated distance compared with the real distance in the non-identical station test campaign.

It can be seen from Figure 5.10 that the averaged time corresponding to the remote station is less stable compared to the averaged local delay as well as the previous LOS measurement where the hardware and software platforms of both remote and local stations are the same. The instability of the remote station introduces additional errors when estimating the distance between two stations. Furthermore, the work load and the process period from hardware and software for two non-identical stations cannot be assumed to be identical or close to each other. It also can be observed from measurement results shown in Figure 5.10 the remote station, which is equipped with Broadcom WLAN NIC running under Windows operating system, presents a different behavior of processing delay compared with the local Atheors based FreeBSD station. Therefore, the method to approximate the remote processing delay by employing (4.27) is not an optimal solution in this test.

5.4 Preliminary Implementation for Indoor Localization

In this section, tests of a preliminary implementation for IPL system are conducted. Two measurement campaigns are carried out to evaluate the performance of the IPL implementation operating in an empty lobby and a small office, respectively. Different communication protocols are employed in these two cases for wireless traffic generations to prove the feasibility of the proposed standard compatible frame exchange based distance measurement technique as well as the IPL system implementation. In the following sections, equipment configurations and measurement results for the each round of field test are presented in detail.

5.4.1 Field Test in Empty Lobby using TCP Traffics

5.4.1.1 Test setups and Equipment Configurations

Recall Figure 4.1 and Figure 4.8 in Chapter 4, in order to uniquely locate a position in a 2-D space, a minimum of three reference points are required. However, it is possible to uniquely determine the location of a target using two reference points with special designs customized by the floor plan of buildings as analyzed in Section 4.5 in Chapter 4.

In this test, two stations are placed at two corners of a rectangle shaped room acting as reference points as shown in Figure 5.12. The distance between these two reference points is pre-measured to the localization procedure. It is obvious from Figure 5.12 that two reference points ideally result in two ambiguous solutions for the coordinates of the target station, namely T and T'. However, only one solution $(\mathrm{T}(\mathrm{x_T}, \mathrm{y_T}))$ falls into the geometric area of the room, which is shown as the shadowed rectangle in Figure 5.12. Therefore, with the help of the floor plan and the knowledge that the target station remains inside the room

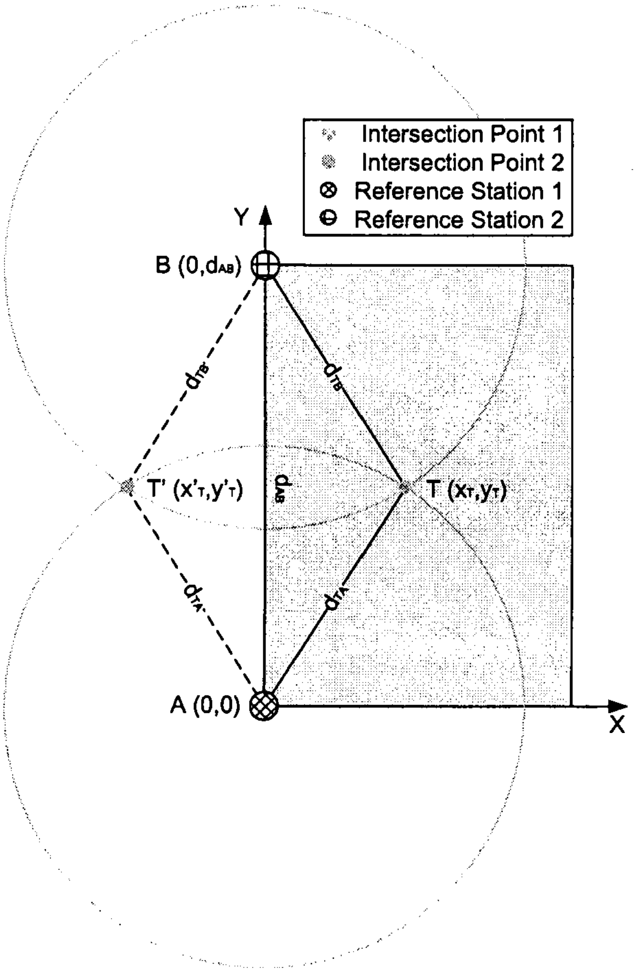
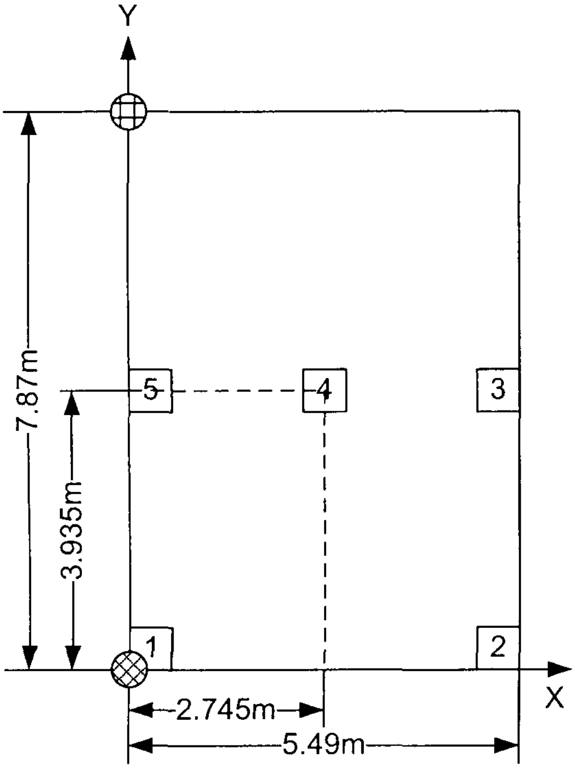


Figure 5.12: Ambiguous solutions with two reference points.

during the measurement, localization results can be further narrowed down since only the location falls inside the room is considered to be valid. As a result, in this specially designed case, two reference points are sufficient for localizing a target station.

Figure 5.13 shows the placement of reference stations as well as locations to be estimated in this campaign. Since the geometric shape of the room is rectangle, axis are constructed along two perpendicular sides of the room to simplify the representation of each location as well as further position calculations. According to the constructed axis, the coordinates of two reference points R_1 and R_2 are $(0, 0)$ and $(0, 7.87)$, respectively. Five target locations are to be estimated as shown in Figure 5.13 and each target location requires two distances to calculate corresponding coordinates of one position to be estimated. The target



1 Target Location 1	P_1 (0,0)
2 Target Location 2	P_2 (5.49,0)
3 Target Location 3	P_3 (5.49,3.935)
4 Target Location 4	P_4 (2.745,3.935)
5 Target Location 5	P_5 (0,3.935)
⊗ Reference Station 1	R_1 (0,0)
⊕ Reference Station 2	R_2 (0,7.87)

Figure 5.13: Floor plan of the room and locations to be estimated.

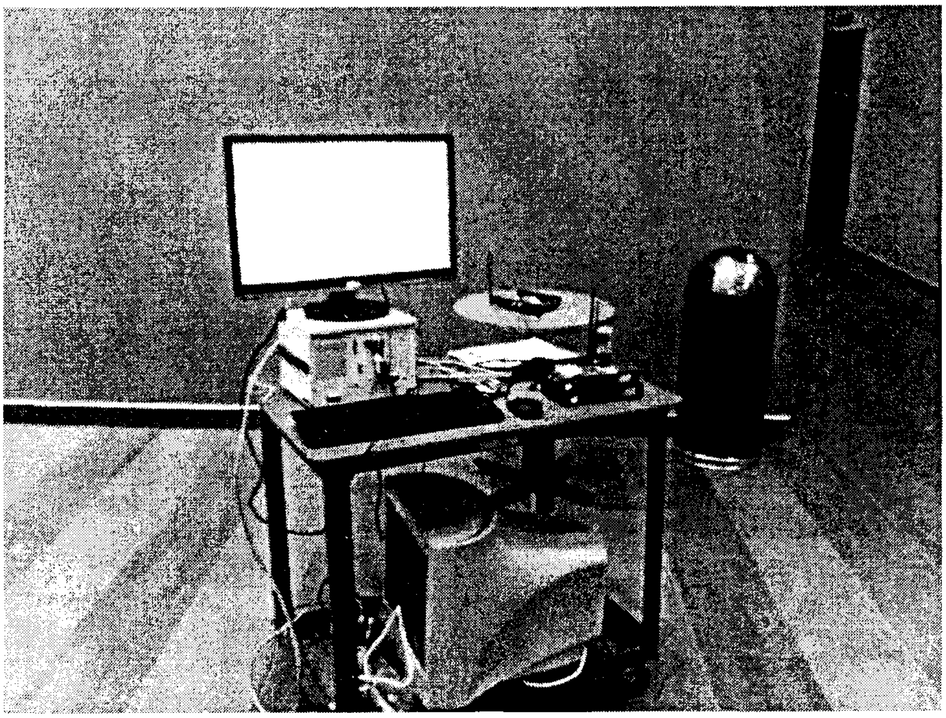


Figure 5.14: Station placement for the indoor localization measurement.

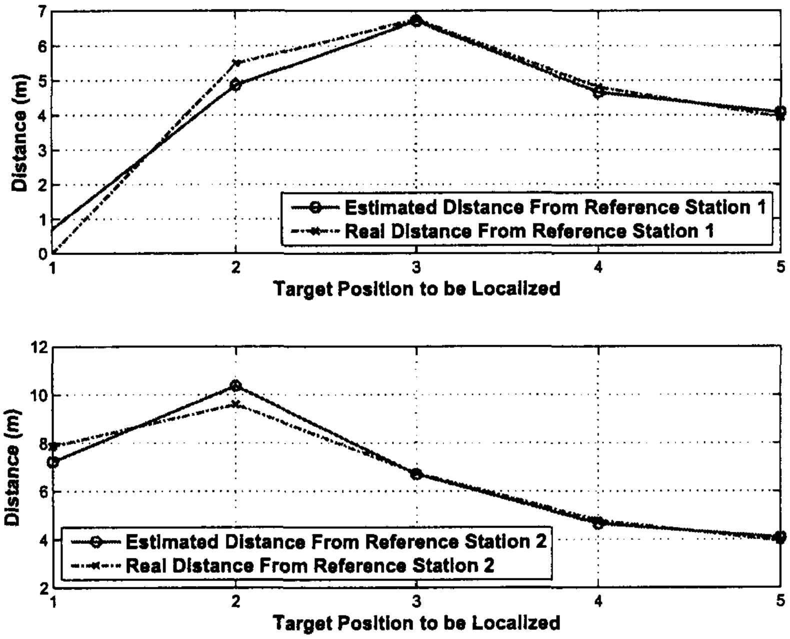


Figure 5.15: Measured distance compared with real distance from two reference stations to each location

station remains stationary during the distance measurement at each location.

In this campaign, normal TCP data exchange sequences are utilized to generate wireless traffics between a reference station and a target station instead of ICMP ping sequences since TCP data exchange sequences are more common in wireless communications. Furthermore, large amount of data traffics increases the number of valid TOA measurements in a given time period, which further accelerates the distance estimation at each location.

5.4.1.2 Measurement Results

The distance measured from two reference points to each of the five positions to be estimated is shown in Figure 5.15, where the top figure and the bottom figure present distances from each target station to reference point R_1 $(0, 0)$ and to the reference point R_2 $(0, 7.87)$, respectively. Red solid curves in Figure 5.15 represent measured distances at each position

Table 5.1: Coordinates of Estimated locations of the target station compared with the corresponding real location

	Real Location	Estimated Location
Location 1	(0, 0)	(0.2792,0.6466)
Location 2	(5.49, 0)	(4.6653,-1.3831)
Location 3	(5.49, 3.935)	(5.4315,3.9335)
Location 4	(2.745, 3.935)	(2.4873,3.9329)
Location 5	(0, 3.935)	(1.0805,3.9340)

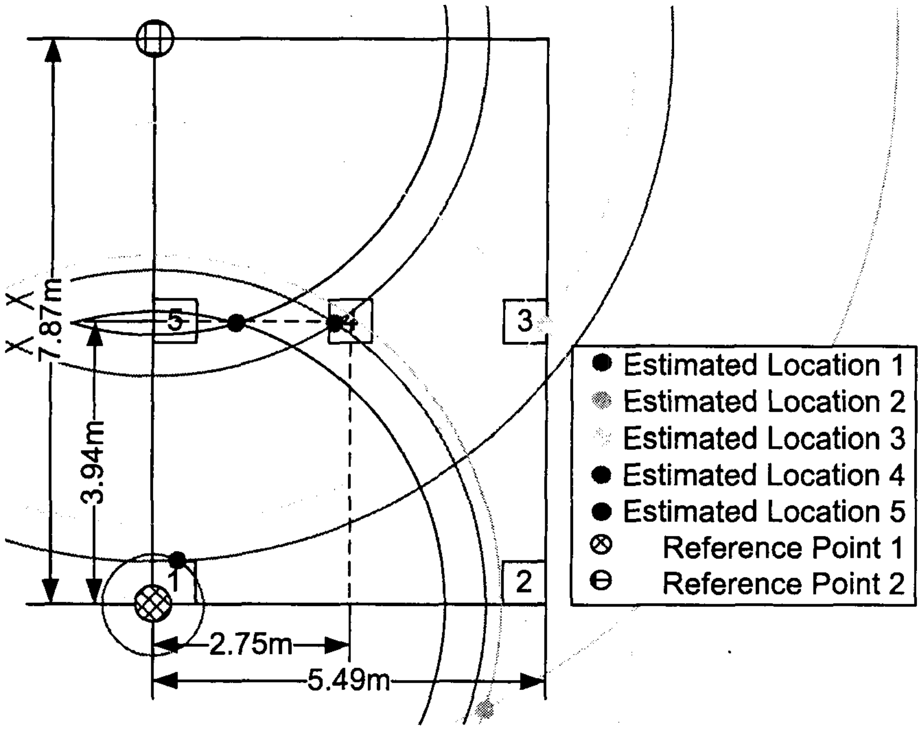
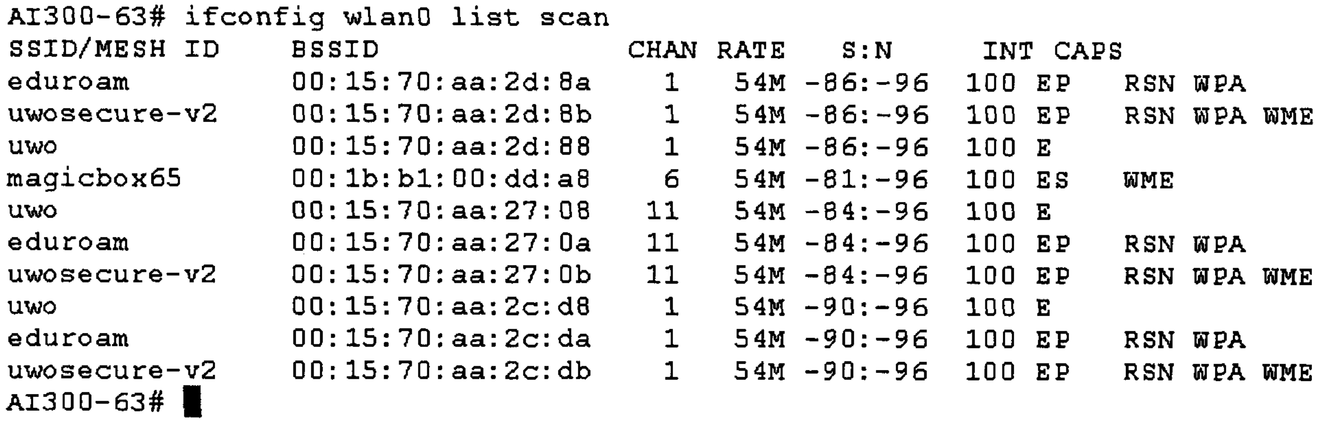


Figure 5.16: Localization results with two reference points.

while blue dash curves demonstrate real distances calculated from position coordinates as references.

Table 5.1 lists calculated coordinates of each position to be estimated. A more intuitive result is shown in Figure 5.16 where distances measured for each position are represented by circles with different colors and intersections of two circles with identical color correspond to the estimated location of a target station. Solutions obtained from trilateration method with negative value on the X-axis are considered invalid according to the floor plan of the



```
AI300-63# ifconfig wlan0 list scan
SSID/MESH ID      BSSID              CHAN RATE    S:N      INT CAPS
eduroam           00:15:70:aa:2d:8a    1   54M -86:-96   100 EP    RSN WPA
uwosecure-v2      00:15:70:aa:2d:8b    1   54M -86:-96   100 EP    RSN WPA WME
uwo               00:15:70:aa:2d:88    1   54M -86:-96   100 E
magicbox65        00:1b:b1:00:dd:a8    6   54M -81:-96   100 ES    WME
uwo               00:15:70:aa:27:08   11   54M -84:-96   100 E
eduroam           00:15:70:aa:27:0a   11   54M -84:-96   100 EP    RSN WPA
uwosecure-v2      00:15:70:aa:27:0b   11   54M -84:-96   100 EP    RSN WPA WME
uwo               00:15:70:aa:2c:d8    1   54M -90:-96   100 E
eduroam           00:15:70:aa:2c:da    1   54M -90:-96   100 EP    RSN WPA
uwosecure-v2      00:15:70:aa:2c:db    1   54M -90:-96   100 EP    RSN WPA WME
AI300-63# █
```

Figure 5.17: High density wireless signals sensed by an IEEE 802.11 WLAN station in a typical office environment.

room. An unique estimated solution for each position can therefore be determined.

It is observed from Figure 5.16 that all the estimated locations are close to the corresponding real locations, thereby proving the protocol-based distance measurement is useful for IPL systems.

5.4.2 Field Test in Small Office using UDP Traffics

In this section, a field test campaign is conducted in a small office where the wireless environment is more complicated. This harsh wireless environment is mainly caused by two reasons. First, larger number of multipaths exist within a small office environment since the wireless signal can be reflected multiple times by walls and objects before attenuated below the receive threshold at the destination station, increasing the TOA measurement uncertainty at the monitor station. Second, the density of wireless signals is much higher in this typical office environment. Figure 5.17 shows an example that ten IEEE 802.11 APs operating on various wireless channels can be sensed by wireless stations placed in this office. Such high density of wireless traffics increases the background noise level as well as the probability of frame transmission collisions. Since the proposed distance measurement technique is based

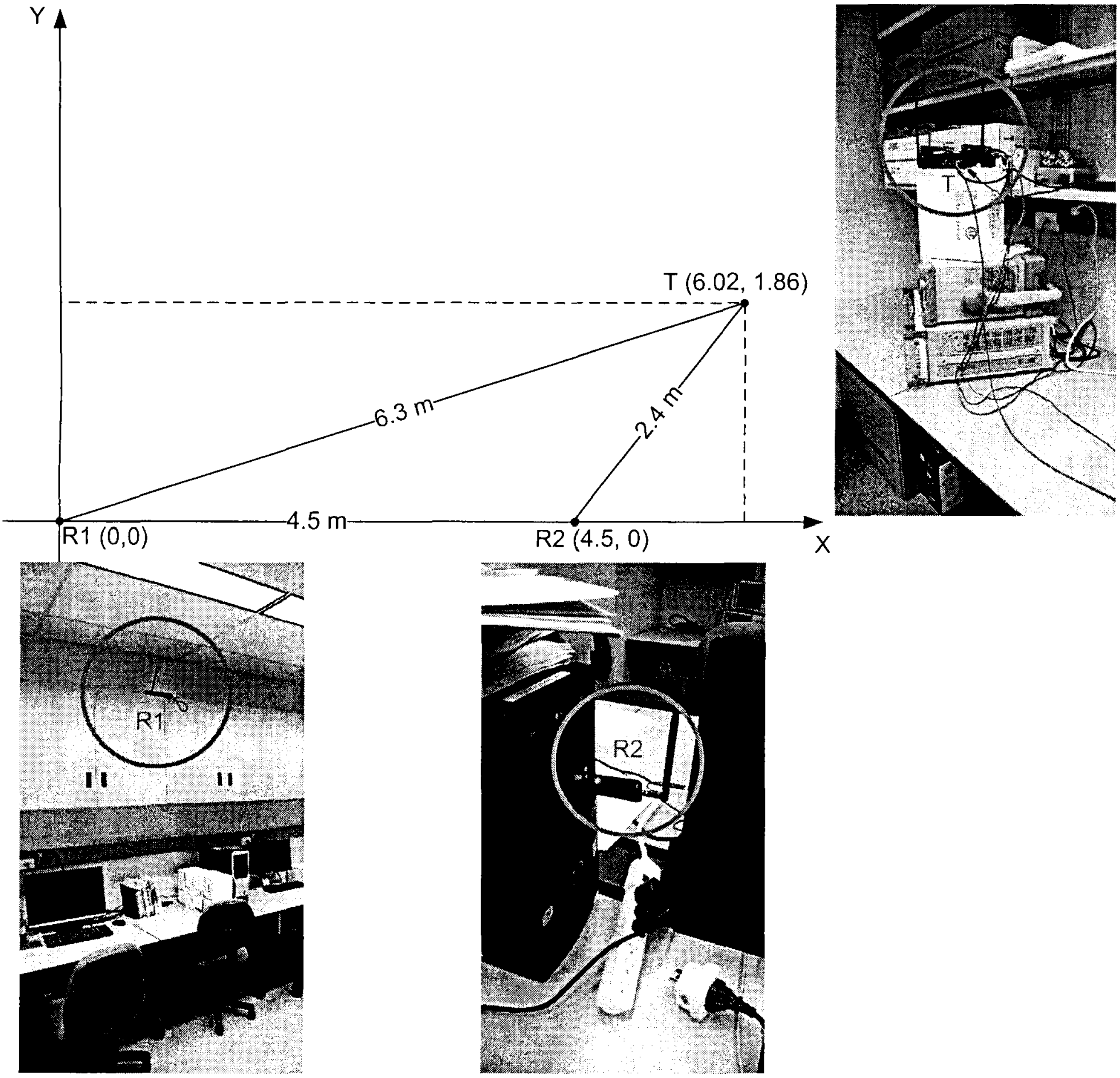


Figure 5.18: Placement of wireless stations and corresponding coordinates used in this test.

on frame exchange sequences, high frame loss rate can reduce the effectiveness of the distance determinations, hence affects the precision of localizations.

5.4.2.1 Test setups and Equipment Configurations

Similar to Section 5.4.1, in this field test campaign, two reference stations $R1(0,0)$ and $R2(4.5,0)$ are employed as shown in Figure 5.18 and the distance between these two reference stations (4.5 m) is pre-measured and considered to be known during the localization. It can also be observed from Figure 5.18 that the two reference stations are running on non-identical platforms. $R1$ is a FreeBSD station using Atheros AR5004X wireless platform which is the same as the target station, while $R2$ is a Windows station using Realtek RTL8187 USB wireless adapter, which is different from the target station.

In this test campaign, the target station is configured to automatically take turns to communicate with one of those two reference stations so that the corresponding distance from the target station to each reference station can be periodically updated for automatic target coordinates calculation. UDP data transmissions with data payload size equal to 20, 30, 50 and 100 bytes are employed to evaluate the impact of various length of transmitted frames to distance measurement results. Different numbers of TOA measurements used for averaging are also considered to evaluate the stability of the proposed protocol-based distance measurement technique.

5.4.2.2 Measurement Results

Table 5.2 and 5.3 present the variance of averaged RTT measurement with different combinations of frame data payload size and number of TOA measurements for averaging. According to these two tables, the size of frame data payload has little impact to the stability of distance measurement for both identical stations and non-identical station cases. Increasing the number of TOA measurement for averaging, on the other hand, is able to reduce the

Table 5.2: Variance of averaged TOA estimation using identical stations with different selections of data payload size and number of TOAs to be averaged

Data payload length (Byte)	20	30	50	100
No. of TOA for Averaging				
5000	6.04×10^{-5}	6.04×10^{-6}	6.04×10^{-5}	5.77×10^{-5}
10000	1.10×10^{-5}	6.45×10^{-6}	6.05×10^{-5}	3.29×10^{-5}
15000	4.59×10^{-6}	6.04×10^{-6}	3.34×10^{-6}	1.47×10^{-5}

Table 5.3: Variance of averaged TOA estimation using non-identical stations with different selections of data payload size and number of TOAs to be averaged

Data payload length (Byte)	20	30	50	100
No. of TOAs for Averaging				
5000	2.03×10^{-4}	2.19×10^{-5}	4.14×10^{-4}	6.69×10^{-6}
10000	1.50×10^{-4}	2.20×10^{-5}	3.21×10^{-4}	4.69×10^{-6}
15000	8.83×10^{-5}	1.65×10^{-5}	2.48×10^{-4}	2.93×10^{-6}

fluctuations of RTT measurement results. Moreover, measurements with Windows station are less stable, which is consistent with the observations in Section 5.3.

The estimated target station position compared with the real position of target station is presented in Figure 5.19. The data payload size and number of TOA measurements for averaging are chosen to be 30 bytes and 10000, respectively. According to Table 5.2 and 5.3, smaller values of these two parameters reduce the measurement stability while larger payload size or averaging window results in longer measurement delays. It can be observed from Figure 5.19 that most estimated positions are distributed around the real position within a range of 3 meters. Figure 5.20 and Figure 5.21 illustrate the detailed position estimation error distribution. According to these two figures, most of the estimation errors are ranging from 0.5 m to 1.5 m while over 90% of estimation errors are less than 2 meters. This result further proves the efficacy of the proposed protocol-based distance measurement technique for IPL implementations in realistic indoor scenarios.

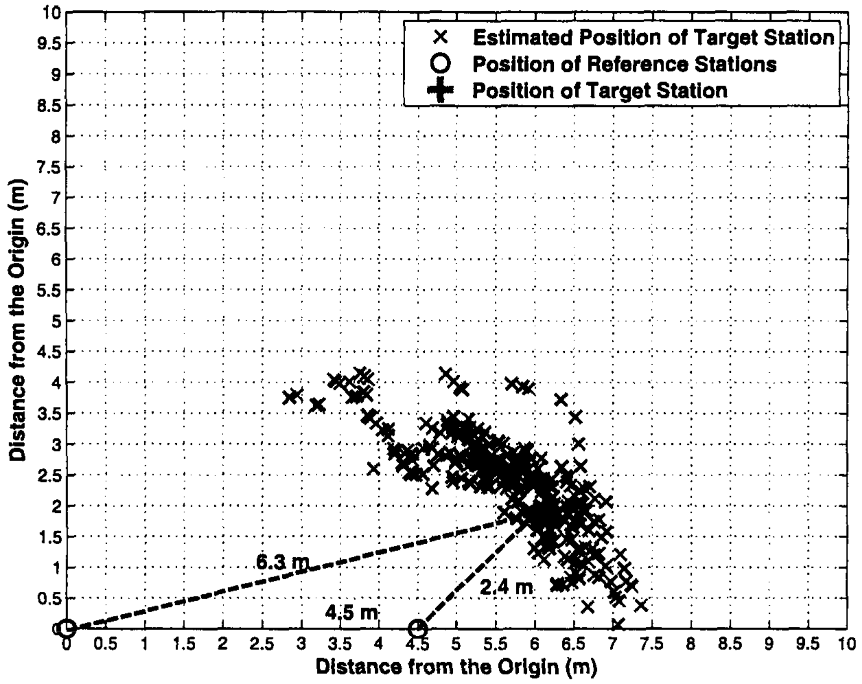


Figure 5.19: Estimated target station position compared with the real position of the target station.

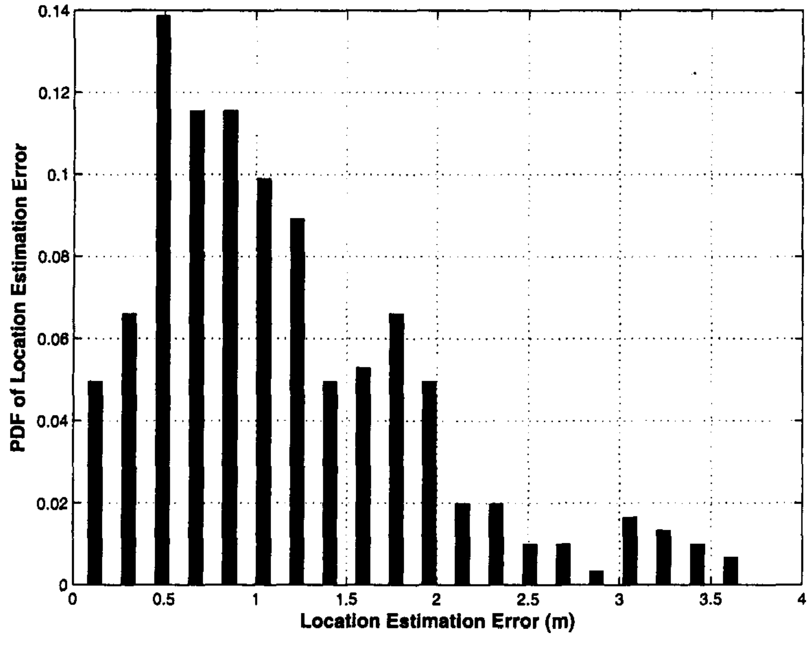


Figure 5.20: The PDF of the position estimation error compared with the real position of the target station.

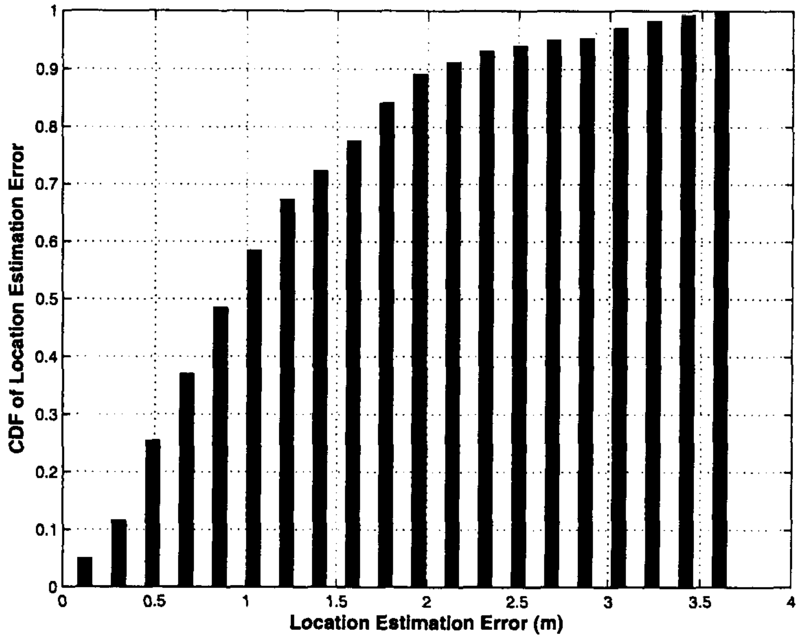


Figure 5.21: The CDF of the position estimation error compared with the real position of the target station.

It is worth noticing that the distance measurement error in the above field tests does not increase for longer distances, therefore the distance measurement technique for IPL proposed in Chapter 4 can be further extended into other wireless communication systems with wider coverage in which RTT can be calculated using frame exchange sequences. For example, in IEEE 802.16 WiMAX [3] specifications, the subscriber station initializes the RTT measurement by transmitting the ranging request (RNG-REQ) frame to the base station. The propagation time is estimated at the base station and replied to the subscriber station using ranging response (RNG-RSP) frame. Moreover, the base station is able to transmit unsolicited RNG-RSP frames to command the subscriber station to update RTT information [19]. Consequently the distance measurement technique can take the advantage of this standard specified mechanism to calculate the distance between two stations for position location applications.

5.5 Summary

In this chapter, field tests for evaluating the proposed protocol-based distance measurement technique in IEEE 802.11 WLANs with commercial available wireless stations are presented. Field test results have shown that propagation delays extracted from observed frame exchange sequences at the monitor station closely relative to distances and the proposed approach is able to estimate the distance with a measurement error of only few meters. Moreover, a preliminary IPL system is also presented in which the target wireless station is located using the trilateration method. Field test results demonstrate that the proposed approach can be further integrated with more advanced trilateration algorithms into IPL systems for robust and precise target localizations.

Chapter 6

Conclusion

As IEEE 802.11 WLANs have been massively deployed for flexible and economical broadband communications in both public venues and residential areas, many efforts have been made to improve QoS requirements of WLANs. On the other hand, growing applications based on WLANs have attracted much research attentions. IPL system is one promising application which combines IEEE 802.11 wireless communications with a position location network.

In this thesis, a collision detection algorithm based on PHY layer SINR is proposed to detect the occurrence of collisions during frame transmissions. Moreover, an IEEE 802.11 WLANs based IPL system with improved locationing accuracy is developed with existing IEEE 802.11 WLANs infrastructures.

6.1 Research Contributions

Research contributions of this thesis include:

- A collision detection algorithm for loss diagnosis in IEEE 802.11 WLANs is proposed based on PHY layer SINR values. The algorithm is designed for fast detecting collisions with low false alarm probability so that it can be further integrated into existing RAAs for performance enhancement.

- A protocol-based distance measurement technique for IPL systems is presented, in which the existing infrastructures of IEEE 802.11 WLANs are utilized. Standard compatible frame exchange sequences are employed to measure the distance between two IEEE 802.11 wireless stations without dedicated hardware or hardware modifications.

- A preliminary IPL system based on the proposed protocol-based distance measurement technique is implemented for realistic target localization in indoor environments.

- Field tests have been conducted to evaluate the presented protocol-based indoor distance measurement method using wireless stations with commercial IEEE 802.11 WLAN NICs in realistic indoor environments. Location estimation results demonstrate the effectiveness of the presented technique for locating a target wireless station in various indoor environments.

6.2 Future Work

There are several topics related to the presented research worth further developing. Some of them are listed as follows:

- A rate adaptation solution which integrates the proposed collision detection algorithm for loss differentiation is desired. It is expected to implement such rate adaptation solution as a part of the driver for IEEE 802.11 WLAN NICs in order to further evaluate and calibrate the proposed algorithm in more realistic scenarios.

- In order to further refine the precision and stability of the presented protocol-based distance measurement method, algorithms combining more metrics, such as interrupt events and RSSI values, are expected to enhance the distance measurement performance.

- Algorithms for advanced trilateration are desired to enhance the robustness of position location systems. Furthermore, target tracking algorithms are expected to locate moving wireless devices by fast position estimations and movement predictions.

References

[1] Supplement to IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: High-speed physical layer in the 5 GHz band. *IEEE Std 802.11a-1999*, page i, 1999.

[2] Supplement to IEEE standard for information technology- telecommunications and information exchange between systems- local and metropolitan area networks- specific requirements- part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher-speed physical layer extension in the 2.4 GHz band. *IEEE Std 802.11b-1999*, pages i –90, 2000.

[3] IEEE standard for information technology- telecommunications and information exchange between systems- local and metropolitan area networks- specific requirements- part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *ANSI/IEEE Std 802.11, 1999 Edition (R2003)*, pages i –513, 2003.

[4] IEEE standard for information technology- telecommunications and information exchange between systems- local and metropolitan area networks- specific requirements part ii: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001)*, pages i –67, 2003.

[5] IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, pages C1 –1184, 12 2007.

[6] B. Alavi. *Distance measurement error modeling for time-of-arrival-based indoor geolocation.* PhD thesis, WORCESTER POLYTECHNIC INSTITUTE, 2006.

[7] B. Alavi and K. Pahlavan. Modeling of the toa-based distance measurement error using uwb indoor radio measurements. *Communications Letters, IEEE*, 10(4):275–277, 2006.

[8] A.A. Ali and AS Omar. Time of arrival estimation for wLAN indoor positioning systems using matrix pencil super resolution algorithm. In *Proceedings of the 2nd Workshop on Positioning, Navigation and Communication, WPNC*, volume 5, pages 11–20, 2005.

[9] P. Bahl and V.N. Padmanabhan. Radar: An in-building rf-based user location and tracking system. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 775–784. Ieee, 2000.

[10] P. Bahl, V.N. Padmanabhan, and A. Balachandran. Enhancements to the radar user location and tracking system. *Microsoft Research*, 2000.

[11] M. Basseville and I.V. Nikiforov. *Detection of abrupt changes: theory and application.* Citeseer, 1993.

[12] G. Bianchi. Performance analysis of the IEEE 802.11 distributed coordination function. *Selected Areas in Communications, IEEE Journal on*, 18(3):535–547, 2000.

[13] J.C. Bicket. *Bit-rate selection in wireless networks.* PhD thesis, Citeseer, 2005.

[14] J.J. Caffery and G.L. Stuber. Overview of radiolocation in cdma cellular systems. *Communications Magazine, IEEE*, 36(4):38–45, 1998.

[15] S. Choi, K. Park, and C. Kim. On the performance characteristics of wLANs: revisited. In *ACM SIGMETRICS Performance Evaluation Review*, volume 33, pages 97–108. ACM, 2005.

[16] M. Ciurana, F. Barceló, and S. Cugno. Indoor tracking in wLAN location with toa measurements. In *Proceedings of the 4th ACM international workshop on Mobility management and wireless access*, pages 121–125. ACM, 2006.

[17] M. Ciurana, F. Barcelo-Arroyo, and F. Izquierdo. A ranging method with IEEE 802.11 data frames for indoor localization. In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pages 2092–2096. IEEE.

[18] M. Ciurana, F. Barcelo-Arroyo, and F. Izquierdo. A ranging method with IEEE 802.11 data frames for indoor localization. In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pages 2092–2096. IEEE.

[19] C. Eklund, R.B. Marks, K.L. Stanwood, and S. Wang. IEEE standard 802.16: a technical overview of the wirelessmantm air interface for broadband wireless access. *Communications Magazine, IEEE*, 40(6):98–107, 2002.

[20] E.P. Engine. 4.0. ekahau positioning engine datasheet. version 1.0. helsinki: Ekahau, 2006.

[21] S.A. Golden and S.S. Bateman. Sensor measurements for wi-fi location with emphasis on time-of-arrival ranging. *Mobile Computing, IEEE Transactions on*, 6(10):1185–1198, 2007.

[22] R. Jain, A. Puri, and R. Sengupta. Geographical routing using partial information for wireless ad hoc networks. *Personal Communications, IEEE*, 8(1):48–57, 2001.

[23] A. Kamerman and L. Monteban. WaveLAN®-ii: a high-performance wireless LAN for the unlicensed band. *Bell Labs technical journal*, 2(3):118–133, 1997.

[24] J. Kim, S. Kim, S. Choi, and D. Qiao. Cara: Collision-aware rate adaptation for IEEE 802.11 wLANs. In *IEEE INFOCOM*, pages 1–11. Citeseer, 2006.

[25] Y.B. Ko and N.H. Vaidya. Location-aided routing (lar) in mobile ad hoc networks. *Wireless Networks*, 6(4):307–321, 2000.

[26] M. Lacage, M.H. Manshaei, and T. Turletti. IEEE 802.11 rate adaptation: a practical approach. In *Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pages 126–134. ACM, 2004.

[27] X. Li and K. Pahlavan. Super-resolution toa estimation with diversity for indoor geolocation. *Wireless Communications, IEEE Transactions on*, 3(1):224–234, 2004.

[28] MadWiFi. http://sourceforge.net/projects/madwifi.

[29] D.G. Manolakis, V.K. Ingle, and S.M. Kogon. *Statistical and adaptive signal processing*, volume 1. Artech House, 2005.

[30] D.D. McCrady, L. Doyle, H. Forstrom, T. Dempsey, and M. Martorana. Mobile ranging using low-accuracy clocks. *Microwave Theory and Techniques, IEEE Transactions on*, 48(6):951–958, 2000.

[31] W. Murphy and W. Hereman. Determination of a position in three dimensions using trilateration and approximate distances. *Colorado School of Mines*, 1999.

[32] K. Pahlavan, P. Krishnamurthy, and A. Beneat. Wideband radio propagation modeling for indoor geolocation applications. *Communications Magazine, IEEE*, 36(4):60–65, 1998.

[33] K. Pahlavan, P. Krishnamurthy, A. Hatami, M. Ylianttila, J.P. Makela, R. Pichna, and J. Vallstron. Handoff in hybrid mobile data networks. *Personal Communications, IEEE*, 7(2):34–47, 2000.

[34] Q. Pang, V.C.M. Leung, and S.C. Liew. A rate adaptation algorithm for IEEE 802.11 wLANs based on MAC-layer loss differentiation. In *Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on*, pages 659–667. IEEE, 2005.

[35] Q. Pang, S.C. Liew, and V.C.M. Leung. Design of an effective loss-distinguishable MAC protocol for 802.11 wLAN. *Communications Letters, IEEE*, 9(9):781–783, 2005.

[36] A. Papoulis, S.U. Pillai, and S. Unnikrishna. *Probability, random variables, and stochastic processes*, volume 196. McGraw-hill New York, 1965.

[37] R. W. Potter. *The art of measurement: Theory and practice*. Prentice Hall PTR, 2000.

[38] P. Qiu and D. Hawkins. A rank-based multivariate CUSUM procedure. *Technometrics*, 43(2):120–132, 2001.

[39] T.S. Rappaport. *Wireless communications*. Prentice Hall PTR, 2002.

[40] H. Reddy, G. Chandra, P. Balamuralidhar, SG Harihara, K. Bhattacharya, and E. Joseph. An improved time-of-arrival estimation for wLAN-based local positioning. In *Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on*, pages 1–5. IEEE, 2007.

[41] C. Reis, R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan. Measurement-based models of delivery and interference in static wireless networks. In *Proceedings of the*

2006 conference on Applications, technologies, architectures, and protocols for computer communications, pages 51–62. ACM, 2006.

[42] M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, and J. Zahorjan. Measurement-based characterization of 802.11 in a hotspot setting. In *Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*, pages 5–10. ACM, 2005.

[43] H. Saarnisaari. TLS-ESPRIT in a time delay estimation. In *Vehicular Technology Conference, 1997 IEEE 47th*, volume 3, pages 1619–1623. IEEE, 1997.

[44] R.A. Serway and J.W. Jewett. *Physics for scientists and engineers*, volume 1. Brooks/Cole Pub Co, 2009.

[45] M.L. Sichitiu and V. Ramadurai. Localization of wireless sensor networks with a mobile beacon. In *Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference on*, pages 174–183. IEEE, 2004.

[46] A. Smailagic and D. Kogan. Location sensing and privacy in a context-aware computing environment. *Wireless Communications, IEEE*, 9(5):10–17, 2002.

[47] H. Velayos and G. Karlsson. Limitations in range estimation for wireless LAN. In *Proc. 1st Workshop on Positioning, Navigation and Communication (WPNC04), Hannover, Germany.* Citeseer, 2004.

[48] G. Verdier, N. Hilgert, and J.P. Vila. Optimality of CUSUM rule approximations in change-point detection problems: Application to nonlinear state–space systems. *Information Theory, IEEE Transactions on*, 54(11):5102–5112, 2008.

[49] A. Vlavianos, L.K. Law, I. Broustis, S.V. Krishnamurthy, and M. Faloutsos. Assessing link quality in IEEE 802.11 wireless networks: Which is the right metric? In

Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on, pages 1–6. IEEE, 2008.

[50] WhereNet. Wireless solutions for tracking and managing assets. [online]. "`http://www.wherenet.com`".

[51] K. Whitehouse and D. Culler. Calibration as parameter estimation in sensor networks. In *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 59–67. ACM, 2002.

[52] S.H.Y. Wong, H. Yang, S. Lu, and V. Bharghavan. Robust rate adaptation for 802.11 wireless networks. In *Proceedings of the 12th annual international conference on Mobile computing and networking*, pages 146–157. ACM, 2006.

[53] S. Xu and T. Saadawi. Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks? *Communications Magazine, IEEE*, 39(6):130–137, 2001.

[54] M. Youssef. Horus: A wLAN-based indoor location determination system. *Department of Computer Science, University of Maryland*, 2004.

[55] J.H. Yun and S.W. Seo. Novel collision detection scheme and its applications for IEEE 802.11 wireless LANs. *Computer communications*, 30(6):1350–1366, 2007.

[56] J. Zhang, K. Tan, J. Zhao, H. Wu, and Y. Zhang. A practical snr-guided rate adaptation. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 2083–2091. IEEE, 2008.