Survey of WiFi Positioning using Time-Based Techniques

Ahmed Makki, Abubakr Siddig, Mohamed Saad, and Chris Bleakley

School of Computer Science & Informatics (CSI), University College Dublin (UCD), Belfield, Dublin 4, Ireland
phone: + (353) 1 716 2915, fax: + (353) 1 269 7262,
email: {ahmed.makki, abubakr.siddig}@ucdconnect.ie, {mohamed.saad,chris.bleakley}@ucd.ie

Abstract

Estimating the position of mobile devices with high accuracy in indoor environments is of interest across a wide range of applications. Many methods and technologies have been proposed to solve the problem but, to date, there is no "silver bullet". This paper surveys research conducted on indoor positioning using time-based approaches in conjunction with the IEEE 802.11 Wireless Local Area Network standard (WiFi). Location solutions using this approach are particularly attractive due to the wide deployment of WiFi and because prior mapping is not needed. This paper provides an overview of the IEEE 802.11 standards and summarizes the key research challenges in 802.11 time-based positioning. The paper categorizes and describes the many proposals published to date, evaluating their implementation complexity and positioning accuracy. Finally, the paper summarizes the state-of-the-art and makes suggestions for future research directions.

Keywords: indoor localization, IEEE 802.11, positioning, localization, ranging, time of arrival, wireless.

1. Introduction

Rapid innovation in the area of wireless data communication has brought a wave of new applications to mobile phone and laptop users worldwide. The widespread deployment of wireless devices has attracted researchers to study the feasibility of utilizing embedded Radio Frequency (RF) transceivers to provide Location Based Services (LBS) to users, as well as communication services. Positioning devices with high accuracy in indoor environments is of interest for a range of applications. Enhanced personal indoor navigation services are desirable in large facilities, such as airports, hospitals, factories and shopping malls [1], and are of particular importance to individuals with visual impairments [2]. Automated location tracking of personnel and goods has the potential to improve efficiency and response times in logistics [3]. Detection of occupancy patterns has proven effective in reducing building heating requirements [4]. On-the-spot advertising and coupon services have been proposed as methods for attracting and retaining customers. Accurate navigation for building evacuees, as well as track-

ing of firefighters, is of great interest to emergency services [5]. In the security domain, location-based data access control, or geo-fencing, is seen as a way to enhance traditional password-based access control mechanisms [6].

The Global Positioning System (GPS) is widely used for outdoor localization. It provides good accuracy (2-3 m). However, it does not work well indoors due to attenuation of the RF signals from the GPS satellites by the building fabric. Many technologies has been applied to the problem of indoor location, including ultrasonic [7, 8], InfraRed (IR) [9], Ultra Wide Band (UWB, IEEE 802.15.4a) [10], WiFi (Wireless Local Area Network IEEE 802.11) [11] and Bluetooth [12]. Ultrasonic and IR approaches offer high accuracy at low cost but typically only provide proximity detection and require line of sight (LOS) between the transmitter and receiver. In comparison to WiFi, Bluetooth, which is currently being used for proximity beacons, lacks range (typically 5-10 m) and so requires a high density of newly deployed nodes. UWB, while offering very good ranging accuracy, has a low data rate

and a very small installed base. WiFi positioning is particularly attractive due to the large number of WiFi-enabled devices already deployed. The ideal solution would be that the existing fixed WiFi infrastructure could be exploited for the purposes of accurate positioning with no hardware modification and without time-consuming manual RF mapping of the positioning space. This would open the way to near ubiquitous indoor positioning at very low cost.

Initial research on WiFi positioning, circa 2000, focused on Received Signal Strength Indicator (RSSI) ranging and fingerprinting [13]. This approach is easy to apply since standards compliant devices make the RSSI reading available at the application layer. However, RSSI ranging provides poor accuracy in buildings because RSSI is not well correlated with distance due to multipath. Fingerprinting methods seek to avoid this problem by using RSSI maps to record the variation of RSSI with position. RSSI maps are built by recording the RSSI observed from all in-range Access Points (APs) at reference points, typically on a 2 m grid, throughout the building. Mobile devices estimate their position by observing the RSSI readings for all in-range APs, i.e. their RSSI signature, and searching the map for the reference position with the best matching signature. The method is standards compliant and so can be used on existing devices but only provides an accuracy of around 3 m [13, 14]. Map building is onerous in terms of effort and the stored maps degrade when people or large objects are moved [14]. For more details on fingerprinting methods, the reader is referred to surveys in [14–18]. To improve accuracy and avoid the need for construction and maintenance of RSSI maps, researchers have proposed the use of time-based methods.

Time-based approaches seek to determine the distance between nodes based on observing the Time Of Arrival (TOA), and possibly the Time Of Transmission (TOT), of an RF signals. While challenging due to the high speed of propagation of the signals, these approaches have the potential for high accuracy positioning without the need for mapping and could replace, or enhance, existing RSSI methods. Time-based methods have shown promise. Nevertheless, many open research challenges remain. While most existing research has used older WiFi standards, continuing advances in WiFi technology and standards are providing new opportunities to address these challenges.

This survey focuses on time-based approaches to the indoor WiFi location estimation problem. To the best of the authors' knowledge, this is the first survey paper addressing time-based WiFi positioning systems. Herein, we consider previous published proposals and make suggestions for potential future developments in the field. The aims of this paper are to provide a comprehensive retrospective of previous work together with a springboard for future work in this promising but challenging area.

In section 2, we provide an overview of the 802.11 standard from the point of view of localization. Section 3 provides background on the principal time-based geometric location estimation algorithms. Section 4 examines the key research challenges in time-based WiFi location estimation. Section 5 surveys all previously proposed time-based WiFi location estimation techniques. Section 6 discusses our findings and makes suggestions for future work. Finally, section 7 concludes the paper. A list of acronyms used in this paper is provided in Table 1 for the reader's reference.

2. IEEE 802.11 Standard

2.1. Overview

IEEE standard 802.11 (also known as WiFi or WLAN) [19, 20] is a wireless communications technology mainly used to deliver Internet Protocol communication services. This standard describes the PHYsical layer (PHY) and Medium Access Control sub-layer (MAC) specification for wireless connectivity between fixed, portable and moving stations within a local area. Many amendments of IEEE 802.11 have been ratified, IEEE 802.11a/b/g/n/ac, and the under development IEEE 802.11ax, are concerned with enhancing communication speed. IEEE 802.11e/i/v/s/p amendments focus on quality of service, security, network management, mesh networking and vehicular environments, respectively.

IEEE 802.11 can also be employed to provide location estimation services. To date, researchers have focused on IEEE 802.11a/b/g. However other standards such as IEEE 802.11n/ac/v/ax, can play an important role in enhancing localization due to their extra features. The following subsections examine IEEE 802.11 from a localization point of view. A summary of the standards is provided in Table 2.

Table 1: List of acronyms.

Abbreviation	Definition	Abbreviation	Definition
ACK	Acknowledgement	MU-MIMO	Multi-user MIMO
AP	Access Points	MUSIC	MUltiple SIgnal Classication
BMP	Beam-space Matrix Pencil	NLOS	Non-Line of Sight
CCK	Complementary Code Keying	OFDM	Orthogonal Frequency Division Multiplexing
CFR	Channel Frequency Response	OS	Operating System
CIR	Channel Impulse Response	OWPT	One Way Propagation Time
CPU	Central Processing Unit	PBCC	Packet Binary Convolutional Coding
CSMA/CA	Carrier Sensing Multiple Access with Collision Avoidance	PCB	Printed Circuit Board
CTS	Clear To Send	PDU	Protocol Data Unit
DCF	Distributed Coordination Function	PHY	Physical Layer
DIFS	DCF Inter Frame Space	PLCP	Physical Layer Convergence Protocol
DSSS	Direct Sequence Spread Spectrum	RF	Radio Frequency
DTDOA	Differential Time Difference of Arrival	RFID	Radio Frequency IDentification
ESPRIT	Estimation of Signal Parameters via Rotational Invariance Technique	RN	Reference Node
FD	Frame Detection	RSSI	Received Signal Strength Indicator
FEC	Forward Error Correction	RTS	Request To Send
FFT	Fast Fourier Transform	RTT	Round Trip Time
FPGA	Field Programmable Gate Array	SIFS	Short Inter Frame Space
GPS	Global Positioning System	SMiLE	SMart integrated Localization Extension
ICMP	Internet Control Message Protocol	SNR	Signal to Noise Ratio
IEEE	Institute of Electrical and Electronics Engineers	STS	Short Training Sequence
IFFT	Inverse Fast Fourier Transform	TDOA	Time Difference of Arrival
IFS	Inter Frame Space	TOA	Time Of Arrival
IQ	In-phase and Quadrature	TOE	Time of Emission
IR	InfraRed	TOF	Time of Flight
LBS	Location Based Services	TOT	Time of Transmission
LOS	Line of Sight	TSC	Time Stamp Counter
LTS	Long Training Sequence	TSF	Time Synchronization Function
MAC	Medium Access Control	UMP	Unitary Matrix Pencil
MD	Mobile Device	UWB	Ultra Wide Band
MIMO	Multiple Input Multiple Output	VNA	Vector Network Analyzer
MP	Matrix Pencil	WLAN	Wireless Local Area Network

2.2. IEEE 802.11 Channel Access Method

The IEEE 802.11 standard for WLAN defines a Distributed Coordination Function (DCF) mechanism for accessing the medium based on a Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) protocol. Optionally the standard defines a centralized MAC protocol, Point Coordination Function (PCF) [21], to support collision free and time bounded services. In this paper we limit our description to the main aspects of the DCF concept. For more information about the medium access mechanism, readers are directed to [21]. DCF uses mandatory periods of idle time on the transmission medium known as Inter Frame Space (IFS) and allows for priority access to the wireless medium. The two most important IFS times are the Short Inter Frame Space (SIFS) (about 10 μs for 802.11b) and the DCF Inter Frame Space (DIFS) (about 50 μs for 802.11b). DCF consists of a basic two way handshaking access mode as well as an optional Request-to-send (RTS)/Clear-to-send (CTS) four-way handshaking access mode [21].

In basic access mode, the node senses the channel to determine whether another node is transmitting before initiating a transmission. If the medium is idle for a DIFS time interval, the transmission will proceed. Otherwise if the medium is busy, the node defers its transmission until the end of the current transmission, and checks again if the medium is idle for a DIFS time interval. In the case of successful packet reception, a positive acknowledgement (ACK) is transmitted by the receiver node to the transmitter node after a SIFS time interval [21]. A SIFS time interval is used to give priority access to ACK packets [20], e.g. if two nodes try to access the medium at the same time, the one that has to wait for a SIFS time interval (10 μs for 802.11b), i.e. in the case of ACK, wins over another node that has to wait for the DIFS time interval (50 μs for 802.11b), i.e. in the case of data.

In RTS/CTS access mode, as in basic access mode, the sender node waits until the channel is sensed idle for a DIFS time interval. Then instead of transmitting the data packet, the sender node transmits an RTS frame. The receiver replies with a CTS frame after a SIFS time interval. The sender then sends data after a SIFS time interval. After that, the receiver replies with an ACK frame after a SIFS time interval [21]. The timing behavior of 802.11 using RTS/CTS access is presented in Figure 1 for a transmitter, receiver and any arbitrary monitoring node.
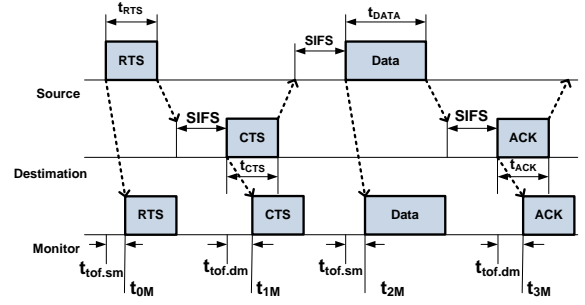

Figure 1: RTS/CTS access mechanism [22, 23].

2.3. IEEE 802.11a

The 802.11a standard released in 1999 uses an Orthogonal Frequency Division Multiplexing (OFDM) based air interface (physical layer) [24]. It operates in the 5 GHz band with a maximum net data rate of 54 Mbps, plus error correction. The following subsections briefly describe aspects of the standard.

2.3.1. Orthogonal Frequency Division Multiplexing

OFDM is a multi-carrier modulation technique that employs overlapping, orthogonal narrowband signals. As shown in Figure 2, a standard OFDM transmitter performs Forward Error Correction (FEC), data interleaving, Inverse Fast Fourier Transform (IFFT), guard interval addition, Inphase and Quadrature (IQ) modulation and power amplification. An OFDM receiver commonly integrates a low noise amplifier, IQ signal detection, guard interval removal, Fast Fourier Transform (FFT), de-interleaving and error correction. IEEE 802.11a uses 64 FFT points (sub-carriers), of which 12 sub-carriers form the guard band, i.e. do not carry any data. The remaining 52 sub-carriers consist of 48 data sub-carriers and 4 pilot sub-carriers. 64 samples of the IFFT output comprise one OFDM symbol; the last 16 samples are copied and prepended at the beginning of each OFDM symbol as the cyclic prefix.

2.3.2. IEEE 802.11a Preamble

The preamble is used to communicate to the receiver that data is on its way. Technically speaking, it is the first portion of the Physical Layer Convergence Protocol/Procedure (PLCP) Protocol Data Unit (PDU). The preamble allows the receiver to acquire the wireless signal and synchronize with the transmitter. The frame structure of IEEE 802.11a
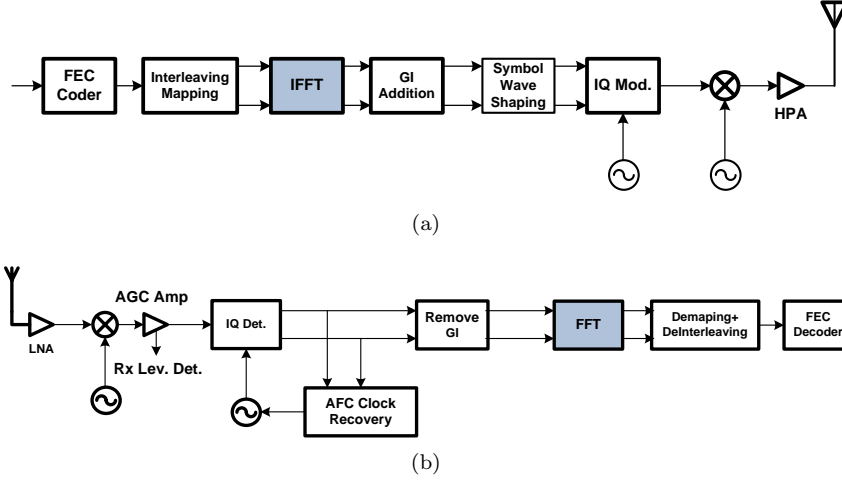
4

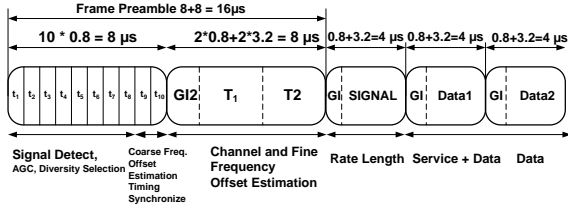Figure 2: OFDM block diagrams (a) transmitter and (b) receiver [19].

Figure 3: Frame structure of IEEE 802.11a/g [19][25].

is presented in Figure 3. The preamble consists of 10 short OFDM symbols with a duration of 0.8 μs each and 2 long OFDM symbols with a duration of 3.2 μs each. The Short Training Sequence (STS) is mainly used for coarse timing and frequency synchronization, and the Long Training Sequence (LTS) for fine frequency synchronization and channel estimation.

2.4. IEEE 802.11b

IEEE 802.11b is an amendment released in 1999 to provide data rates up to 11 Mbps using Direct Sequence Spread Spectrum (DSSS) modulation at 2.4 GHz [26]. An 11-bit Barker sequence with Differential Binary Phase Shift Keying (DBPSK) and Differential Quadrature Phase Shift Keying (DQPSK) are used to obtain data rates of 1 Mbps and 2 Mbps, respectively. Higher data rates employ Complementary Code Keying (CCK).

Two different preambles are defined by the standard: short (72 bits) and long (144 bits). The long preamble consists of a 128-bit Sync (synchronization) field that consists of scrambled bits used

for synchronization and a 16-bit SFD (Start Frame Delimiter) field that indicates the start of PHY-dependent parameters. In the short preamble, the Sync field is 56 bits consisting of scrambled bits and the SFD field is presented in reversed bit order. The preamble is used by the receiver to perform the necessary synchronization operations and must be transmitted at 1 Mbps with a DBPSK modulation. The header is transmitted at 2 Mbps using a DQPSK modulation in the case of a packet with a short preamble to reduce overhead.

2.5. IEEE 802.11g

In June 2003, a third amendment was ratified: 802.11g [27]. This standard combines the features of both amendments 802.11a and 802.11b to support data rates of up to 54 Mbps in the 2.4 GHz band. The standard uses either DSSS, OFDM, or both and provides backward compatibility with 802.11b devices. The frame structure of IEEE 802.11g working in OFDM mode is similar to that of IEEE 802.11a as presented in Figure 3 [28].

2.6. IEEE 802.11n

The IEEE 802.11n amendment [29] was published in October 2009 and added Multiple-Input Multiple-Output antenna (MIMO) technology, packet aggregation, and security improvements. The standard supports 2.4 GHz and 5 GHz frequency bands (i.e. dual bands) and the transmission rate is greater than 100 Mbps. Using MIMO, the transmitting WLAN device splits a data stream into multiple parts, called spatial streams, and

transmits each spatial stream through separate antennas to corresponding antennas at the receiving end. The amendment improves the network throughput over the two previous standards i.e. 802.11a/g, with the use of four spatial streams (MIMO) together with a wider-bandwidth channel of 40 MHz. As an optional feature, the standard allows beam-forming. This amendment provides a significant improvement in range, i.e. the maximum distance that a mobile device can communicate with an AP with acceptable performance is approximately 70 m compared to 35 m for previous standards.

2.7. IEEE 802.11ac

The IEEE 802.11ac amendment was published in December 2013 [30]. In contrast to previous amendments, 802.11ac is aimed at improving total network throughput as well as individual link performance, with possible integration of cellular systems. It builds on the 802.11n standard by introducing: wider bandwidth (up to 160 MHz vs. 40 MHz) in the 5 GHz band, more spatial streams through MIMO (up to 8 streams vs. 4 streams), denser modulation (up to 256-QAM vs. 64-QAM), and the addition of multi-user MIMO (MU-MIMO) with up to four clients. MU-MIMO is adopted to improve spectrum efficiency by allowing transmission of multiple data frames to multiple users simultaneously [31]. The standard has mandatory support for 20, 40, and 80 MHz channels, and optional support for 160 MHz (contiguous) or 80+80 MHz (non-contiguous) [32].

2.8. IEEE 802.11ax

WLAN devices are currently being deployed at increased density to enhance communication throughput and reliability. This increases the interference between neighboring devices, potentially degrading network performance. Current standardization efforts are focused on increasing link throughput, rather than on efficient use of spectrum, and user experience such as latency. In March 2014, the IEEE Standards Association (IEEE-SA) approved IEEE 802.11ax to standardize performance for dense networks with a large number of devices and APs. It is anticipated that actual deployment of the standard will take place, at the earliest, in late 2019. The amendment allows backward compatibility and coexistence with legacy IEEE 802.11 devices operating in the same band [31].

2.9. 802.11v Time Stamping

The IEEE 802.11v amendment [33] was ratified on February 2011 and introduces wireless network management capabilities to the IEEE 802.11 family of standards. It defines mechanisms and services to allow WLAN devices to exchange information about network topology, including information on the RF environment such as channel usage, interference reporting, and timing measurement. It also enables remote configuration of clients while they are connected to the network.

3. Time-Based Location Estimation

The following subsections describe the terms and algorithms used in time-based geometric positioning.

3.1. Time Of Flight

Time Of Flight (TOF) is defined as the time that the signal takes to travel from Node A to Node B. If the TOF is known, the physical separation (or range) of the nodes can be calculated based on the TOF and the known propagation speed of the signal.

In one-way ranging, the sender transmits a packet and records the Time of Transmission (TOT) t_{ot}. The Time of Transmission (also known as the Time Of Emission, TOE) is defined as the time instant at which the sender sends a particular packet, as recorded by the sender. The receiver receives the packet and records the Time Of Arrival (TOA) t_{oa}. TOA is defined as the time instant at which the receiver receives the packet, as recorded by the receiver. If the nodes are time synchronized, the TOT and TOA can be shared and the TOF t_{of} calculated according to:

$$t_{of} = t_{oa} - t_{ot} \tag{1}$$

The range r between the nodes can be estimated as:

$$r = c.t_{of} \tag{2}$$

where c is the propagation speed of the signal. In the RF case, c is equal to the speed of light.

In the 2D location estimation case, the position of a Mobile Device (MD) can be determined from three range estimates to fixed Access Points (APs) with known positions by means of trilateration. Each MD-AP range r_i places the MD's position

Table 2: Summary of IEEE 802.11 amendments.

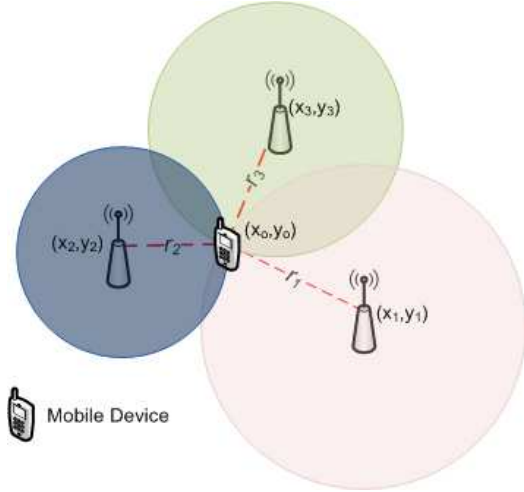| IEEE 802.11 amendment	a	b	g	n	ac	ax
Frequency Band	5	2.4	2.4	2.4/5	5	2.4/5
Modulation	OFDM	DSSS	DSSS /OFDM	OFDM	OFDM	OFDM
Beam-forming Capable	NO	NO	NO	YES	YES	NA
Maximum Number of Spatial Streams	1	1	1	4	8	NA
Channel Width (MHz)	20	22	20	20/40	20,40,80 (mandatory), 160, and80+80 (optional)	NA
Maximum Data Rate per Stream (Mbps)	54	11	54	72/150	87/200/433/867	NA

Figure 4: 2D localization using trilateration.

(x_0, y_0) on the circumference of a circle, with radius r_i, centered on the co-ordinates of AP i, (x_i, y_i):

$$(x_0 - x_i)^2 + (y_0 - y_i)^2 = r_i^2 \qquad (3)$$

Solving three equations for three APs, determines the position of the MD, as illustrated in Figure 4. The equations can be solved using a closed form solution [34, 35] or a numerical method [22]. Often numerical methods are preferred since they are more tolerant to errors in the range estimates. Spherical multi-lateration techniques can be used to reduce error in the case of more than three APs [22].

While conceptually simple, this method typically does not work well in WiFi systems because of the lack of tight time synchronization between devices. As with all time-based methods, due to the high propagation speed, small delay estimation errors lead to large ranging errors (e.g. 1 ns TOF error is equal to a 0.3 m ranging error).

3.2. Round Trip Time

In this technique (also known as two-way ranging), the sender transmits a packet and records the TOT t_{ot}, the receiver receives this packet and replies, via ACK or any other suitable packet, after a processing time delay t_{proc} [11]. The time difference from when the transmitter sends the packet until the time that it receives the response t_{oa} is the Round Trip Time (RTT):

$$t_{rtt} = t_{oa} - t_{ot} \qquad (4)$$

Expressed as function of the TOF and the processing time delay :

$$t_{rtt} = 2t_{of} + t_{proc} \qquad (5)$$

The TOF can then be estimated as :

$$t_{of} = (t_{rtt} - t_{proc})/2 \qquad (6)$$

and the sender-receiver range calculated as described previously.

The RTT technique has the advantage of not requiring synchronization between the transmitter and receiver. However, the processing delay at the remote end must be fixed and known precisely.

7

3.3. Time Difference of Arrival

There are two variants of Time Difference of Arrival (TDOA). The first uses one receiver with unknown position (the MD) and multiple senders with known positions (APs) [36]. The senders are synchronized and send packets simultaneously. The receiver measures the differences in the TOAs of the packets from the senders. This approach is similar to the GPS concept. However, it does not typically work well for 802.11 due to collisions between the packets. The second variant uses one transmitter (the MD) and multiple, synchronized receivers with known positions (the APs) [36]. The MD transmits a packet, which is received by $N+1$ receivers. Based on the N differences in the TOAs, the position of the receiver can be determined in N dimensions. The MD position is determined using hyperbolic multilateration [14]. For each TDOA observation, the MD (x_0, y_0) is known to lie on a hyperboloid with constant range difference between two receivers (x_i, y_i) [14]. The equation of the hyperbola is illustrated in Figure 5 and can be expressed as:

$$R_{i,j} = \sqrt{(x_i - x_0)^2 + (y_i - y_0)^2} \\ - \sqrt{(x_j - x_0)^2 + (y_j - y_0)^2} \quad (7)$$

The location of the MD can be found by solving the N equations derived from all $N+1$ APs, either using closed form [37] or numerical methods [14], as illustrated for the 2D case in Figure 5.

This second variant is more applicable to WiFi based location but is dependent on the accuracy of TOA estimation at the APs and on the accuracy of their timing synchronization. In some cases, an additional wired interconnection is provided between the APs for the purposes of achieving accurate synchronization.

3.4. Differential Time Difference of Arrival

Differential Time Difference of Arrival (DTDOA) uses one MD, one Reference Node (RN) and multiple receivers (APs) [38]. The RN and receivers are fixed and their positions are known. In the first step, the RN transmits a packet and the receivers record its TOA. This step allows the system to determine the time synchronization of the APs. In the second step, the MD transmits a packet, and the receivers again record the TOAs. Each receiver calculates the TDOA between the RN packet arrival and the MD packet arrival. These differences
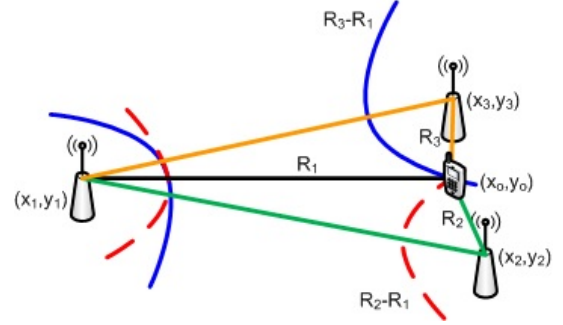

Figure 5: 2D positioning using TDOA and hyperbolic multilateration.

are then used to estimate the location of the MD. One RN in addition to $N+1$ receivers is needed for localization in N dimensions.

Mathematically, the process can be described using the following steps. First, the t_{doa1} for the MD relative to AP1 and AP2 can be defined as:

$$t_{doa1} = (\sqrt{(x_2 - x_0)^2 + (y_2 - y_0)^2} \\ - \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2})/c \quad (8)$$

Similarly, the t_{doa2} for the RN relative to AP1 and AP2 in can be defined as:

$$t_{doa2} = (\sqrt{(x_2 - x_R)^2 + (y_2 - y_R)^2} \\ - \sqrt{(x_1 - x_R)^2 + (y_1 - y_R)^2})/c \quad (9)$$

The DTDOA for the MD and RN relative to AP1 and AP2 can be expressed as:

$$t_{dtdoa12} = t_{doa1} - t_{doa2} \quad (10)$$

Generalizing, the location of the MD is found by solving the set of equations given by:

$$c.t_{dtdoaij} = (\sqrt{(x_j - x_R)^2 + (y_j - y_R)^2} \\ - \sqrt{(x_i - x_R)^2 + (y_i - y_R)^2}) \\ - (\sqrt{(x_j - x_0)^2 + (y_j - y_0)^2} \\ - \sqrt{(x_i - x_0)^2 + (y_i - y_0)^2}) \quad (11)$$

Winkler et al [39, 40] and Zan Li et al [38] provide more detail on the solution. An example system using three APs and one RN to determine the MD's position is illustrated in Figure 6.

This approach has the advantage of not needing additional synchronization of the APs. However, the method is prone to errors due to differences in the clock drift of the receivers if the delay between the RN and MD transmissions is large.
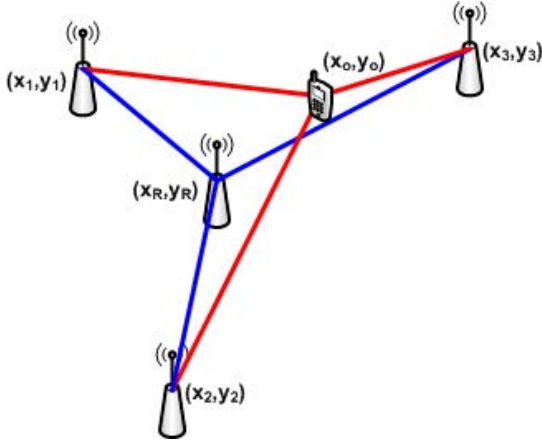
Figure 6: DTDOA localization method.

4. Research Challenges

The fundamental challenge in time-based RF localization systems is in accurately determining the inter-node range by measuring the packet TOAs and, in some cases, the TOTs. Researchers seek to solve this problem with the least possible changes to the 802.11 standard. Following are some of the barriers to solving the problem.

4.1. Timing Resolution

Due to the high speed of light, sub 3 nanosecond TOF resolution is required to achieve sub-meter ranging accuracy. Off-the-shelf IEEE 802.11 transceivers measure TOA at the device-driver level, by means of the Timing Synchronization Function (TSF). This has a resolution of roughly $1 \mu s$, corresponding to a radio propagation resolution of 300 m [11]. This resolution can be improved by averaging and statistical means. Alternatively, resolution may be enhanced by measurement at the physical layer.

4.2. Bandwidth

TOA estimation relies on identifying the instant of observation of a specific feature in the received signal. Typically, this feature is the peak of the cross-correlation of the received and expected signals. In theory, in a system with infinite bandwidth, the peak will be impulsive in the time domain, leading to high timing accuracy [41]. In practice, in a system with finite bandwidth, the pulse becomes wider in time, making estimation of the delay of the peak more susceptible to noise. Current 802.11a/b/g WLANs are classified as narrow

band systems with bandwidths of about 20 MHz. This limits sample-level TOA estimation accuracy to about 7.5 m [11, 41] without using averaging or phase estimation techniques. As the bandwidth associated with newer standards increases, e.g. 802.11n/ac/ax, this may assist in improving the accuracy of TOA estimation.

4.3. Sampling Rate

In conventional systems, sampling rate limits the resolution of the TOA. In order to achieve finer time resolution, a higher sampling frequency or special signal processing is required. The baseband sampling frequency of IEEE 802.11a/b/g standards is about 40 MHz, i.e. twice the signal bandwidth (Nyquist criterion).

4.4. Noise

All measurements are subjected to random noise, including thermal noise and circuit noise [41]. Averaging can be used to reduce the effects of noise. However, this increases energy consumption and measurement duration.

4.5. Multipath

In most indoor environments, the RF signal at the receiver consists of a signal propagating along the direct path from the transmitter plus reflected and delayed copies of the transmitted signal. In communications, multipath can be used to improve the reliability by combining the direct and reflected signals using rake receivers [42]. However, only the direct-path is useful for ranging. Thus the direct path component must be uniquely identified and separated from the multipath components. As illustrated in Figures 7 and 8, due to attenuation of the direct path and/or constructive multipath interference at other delays, the direct TOA path may not correspond to the delay of the cross-correlation peak. This makes identification of the arrival of the direct path component difficult.

In MIMO, multiple antennas are used at both the transmitter and the receiver. The signals from these antennas are combined to minimize errors and optimize data speed. This technology may be beneficial in reducing the impact of multipath.

4.6. Collisions

Since 802.11 uses a shared medium, collisions between packets from different APs can occur and must be eliminated from the measurement process.
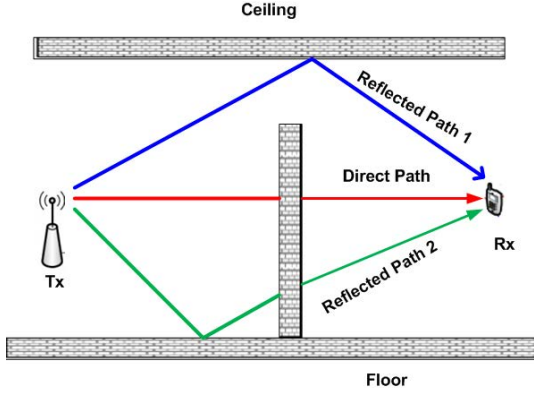
Figure 7: Multipath example showing propagation of three rays.

4.7. Non-Line of Sight

Non-line of sight (NLOS) occurs when the direct path (or Line Of Sight, LOS) between the transmitter and receiver is blocked by some RF opaque obstacle. In this case, the receiver timestamp will be based on the arrival time of the NLOS signal, that is a signal reflected from another object. This signal has a longer path and so the range is over-estimated.

4.8. In-Band Interferers

The 802.11 band is used by a number of other devices, particularly Bluetooth, and can be subject to environmental interferers, such as microwaves.

4.9. Signal Model

Overall, the received signal $y(t)$ can be described as:

$$y(t) = \sum_{i=0}^{M} a_i.x(t - \tau_i) + w(t) \qquad (12)$$

where M is the number of multipath components, $x(t)$ is the transmitted signal, a_i is the amplitude of the ith path, τ_i the relative delay of the ith path and $w(t)$ is additive white noise and interference.

4.10. Time Synchronization

802.11 devices are not normally tightly synchronized. Each node has its own independent, free-running clock. Even after synchronization is performed, synchronization error grows rapidly with time due to frequency offset between the devices' clocks. This drift is largely dependent on the clock's current operating temperature and on crystal cut angle. The standard mandates an maximum drift
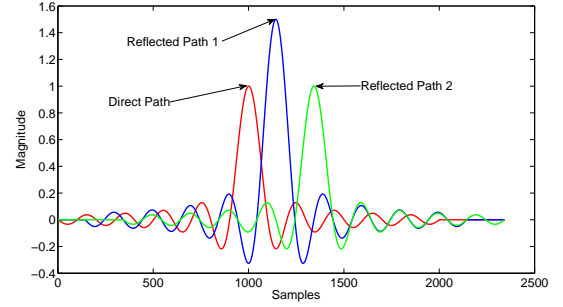
(a)
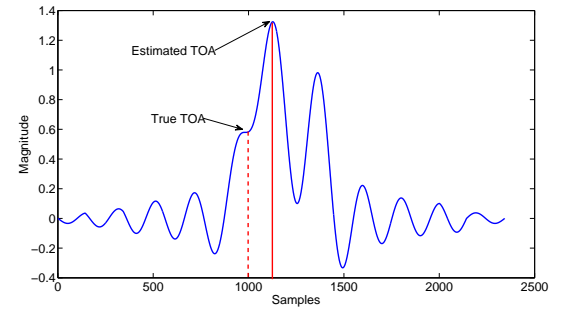
(b)

Figure 8: (a) Cross-correlation of multipath components with transmitted signal (b) Cross-correlation of received signal with transmitted signal. The direct path TOA (dotted) precedes the cross-correlation peak (solid).

of 25 ppm [23]. Inaccuracies in timing synchronization between nodes are a limiting factor in several time-based positioning methods.

5. Time-Based Positioning Methods

Time-based WiFi location estimation methods can be classified according to the communication layer at which they are implemented [43]. Generally speaking, lower layer methods offer greater accuracy at the cost of greater implementation complexity. The following subsections describe previously proposed time-based WiFi localization methods grouped according to layer. The techniques and their properties are summarized in Table 3.

5.1. Application Layer Software Methods

This subsection focuses on techniques applied at the application layer by means of software, without hardware or Medium Access Control (MAC) layer software modifications.

In 2005, Gunther and Hoene [11] proved that off-the-shelf IEEE 802.11 cards can be used to estimate range. They used a two-way TOA (RTT) method based on data and acknowledgment (DATA/ACK) packets together with statistical methods to overcome the low resolution of the standard timestamp hardware timers. Packets were directly sniffed at the MAC layer and forwarded to the application layer for post-processing by means of the operating system without any hardware or software modification. They succeeded in achieving a mean ranging error of about 8 m using 1,000 packet transmissions. To reduce the number of packets needed, in [22] Hoene and Willmann introduced a four-way TOA approach. This used the Request-to-Send and Clear-to-Send (RTS/CTS) packets (see Figure 1) such that the sender, receiver and an arbitrary monitoring node could measure TOF. This halved the number of packets need to obtain the same number of observations as in the two-way method. Their algorithm was implemented in open source software called Goodtry. It is a generic pure software solution using unmodified WLAN chip sets. Experimental results show that software-based trilateration based on Goodtry has an accuracy of about 4 m. In [44], the authors compared "Goodtry" with other RF indoor localization technologies including RFID and Bluetooth. RFID and Bluetooth achieved positioning accuracies of about 0.5 m over short distances, while WLAN yielded an accuracy of about 4 m over longer distances.

5.2. MAC Layer Hardware Methods

Promising results from off-the-shelf equipment encouraged researchers to seek improvements in localization accuracy and overcome the low resolution of the standard timestamp used by the hardware timers by making minor modifications to existing WLAN cards. Access to the MAC layer was exploited to provide more direct measurements of time, avoiding unpredictable delays in the interlayer interfacing, frame encoding and decoding, driver communication, and/or operating system intermediation.

In [45], a research group at the Technical University of Catalonia, Barcelona, improved localization accuracy by increasing the resolution of the timestamp. They built a counter based on the WLAN card clock running at 44 MHz. RTT was measured using RTS/CTS. The counter started when the end of an RTS frame was detected and stopped when the corresponding CTS frame arrived. Three hundred RTT measurements were used to reduce the effects of noise. The AP processing delay was calibrated by placing the AP and MD at zero separation. The estimated distance was divided by an empirical coefficient (k=1.32) to correct the measured value. Ranging errors varied from an average of 2.82 m when empirical coefficients were not used to 0.64 m when they were. A trilateration algorithm was used to locate their MD in 2D, achieving errors within 2.3 m in 90% of cases using three APs. They also evaluated the possibility of using empirical tables to convert the average measured RTT to the corresponding ground truth range measurement. This method achieved an accuracy better than 2 m in 56% of cases. All measurements were taken in a real indoor working environment without differentiating between LOS and NLOS. In [46] and [47], the team improved positioning accuracy by introducing MD tracking capability to their system by means of a Kalman filter. This approach achieved high accuracy: better than 0.9 m in 66% of cases in LOS conditions. In [48], they used DATA/ACK RTT combined with statistical post-processing of propagation time and processing delay estimates, to obtain better than 1 m mean ranging accuracy when using an empirical statistical estimator and a mean ranging error of 2.63 m using statistical methods based on averaging. The experiments were conducted in a LOS environment.

Continuing with this approach, in [49, 50], Bahillo et al designed a Printed Circuit Board (PCB) counter for measuring RTT. The AP processing delay was directly measured using a PCB in a calibration step and was kept constant. After analyzing the statistical approach previously proposed, they introduced linear regression fitted to the statistical estimate of the RTT measurements at each distance as a robust method for estimating the distance between two WLAN nodes in any environment. Three different scenarios were considered, an outdoor case (EXT) with a few streetlamps, trees and people; an indoor corridor case (COR) with wooden and metal doors and some people; and an indoor office case (OFC) with furniture and people working on their PCs. In all scenarios, a direct path existed between the MD and the AP. The ranging accuracies were on average approximately 1 m, 1.5 m and 1.7 m for the scenarios EXT, COR and OFC, respectively. A scaling parameter based on the Weibull distribution improved results by 0.2 m on average. Accuracy can deteriorate to 3 m if the

linear regression is applied to an unknown environment, due to differences in multipath. In [51], the team added real-time location capabilities, achieving a precision of better than 3.51 m in 50% of cases in a hard multipath and NLOS indoor environment. A detailed overview of their work is provided in [52] and [53].

Kim et al [54] suggested overcoming the low timestamp resolution of the standard hardware timers by using an additional hardware TPU (Time Processing Unit) specifically for positioning, placed between the MAC and PHY, to reduce error. The method uses independent hardware that stores the TOT and TOA. This theoretically eliminates the error in data processing between the physical and MAC layers. To our knowledge, the method was not evaluated experimentally or in simulation.

5.3. MAC Layer and Driver Software Methods

Hardware customization to overcome the low standard timestamp resolution presents a barrier to implementation, consequently a number of MAC layer and driver software approaches have been proposed. They augment the software in the WLAN cards in such a way that packets can be timestamped more accurately than at the application layer without modifying the hardware.

Ciurana et al [55] at the Technical University of Catalonia proposed a mechanism to obtain the RTT by modifying the WLAN driver to use the Central Processing Unit (CPU) clock as a time base by accessing the Time Stamp Counter (TSC). TSC is a 64-bit register containing a counter, each clock tick of the CPU increments the TSC. Timestamping is performed by the OS via interrupts at the instant that the MAC data frame is transferred to the physical layer for transmission and at the instant when the ACK frame is received at the MAC layer. The difference between the timestamps is an estimate of the RTT. Statistical processing was applied over several RTT estimates to reduce the effect of noise. Empirical results show ranging error is less than 2 m in indoor and outdoor LOS environments. Stability analysis for the proposed algorithm can be found in [56]. A CPU timestamp counter offering nanosecond resolution was also used by Schauer et al [57]. In their work, they preferred using NULL-ACK-sequences due their shorter length and lower likelihood of collision. Various types of hardware and environments were used in their study. In an ideal environment, using a band-pass filter, and taking the average of a series of measurements, they

achieved a mean ranging error of less than 1.3 m. In office environments, accuracy was around 5 m. It is worth mentioning that, using different hardware, i.e. replacing a HP laptop with a Samsung laptop in an office environment, resulted in a mean error of 275 m and little correlation between estimated and real distances could be found.

Casacuberta and Ramirez [58] presented and compared three different software-based RTT methods using the Internet Control Message Protocol (ICMP) ping communication. The first method used the standard time synchronization function. This approach obtained the RTT using the 1 μs resolution timestamp in the MAC header of a wireless frame. The second method exploited the CPU's timestamp counter to obtain better resolution. The third approach used the WLAN card clock. In all cases, statistical methods were used to increase accuracy. The methods achieved accuracies of about 2.8, 1.5, and 4.4 m, respectively in a LOS environment. In similar work, Wibowo et al [5] used a counter based on the 44 MHz device clock to measure RTT. The remote processing delay was calibrated by placing devices with 0 m separation initially. Statistical processing was used to improve accuracy. Better than 2 m accuracy was achieved in LOS conditions. Driver modifications were also used by Giustiniano et al in [59]. They performed localization based on the MAC idle time (SIFS) combined with the SNR. They assumed the receiver would send the ACK after the exact SIFS period, i.e. 10 μs (see Section 2.2). They considered the MAC idle time as consisting of the RTT, the SIFS, and the Frame Detection (FD) time which is highly dependent on the SNR of the received ACK. They conducted measurements to determine the true FD for various MAC idle times and SNRs. To estimate location, the MD estimated the RTT by measuring the MAC idle time and using the SNR to compensate for the FD. Their system achieved sub-meter accuracy in 80% of cases in a LOS environment.

While most researchers focused on two-way ranging, a small number investigated one-way ranging. Wang et al [60], in theoretical and simulation studies, investigated the feasibility of using One Way Propagation Time (OWPT) with improved time resolution and synchronization. According to the method, TOF is obtained by subtracting the TOT of a beacon frame at an AP from the TOA at the MD. The method assumes driver modification at the MD to get nanosecond time resolution by exploiting the card clock. They developed an algo-

rithm to deal with the non-adjustable low resolution AP clock by selecting the proper beacon timestamp among several readings. A calibration synchronization algorithm was developed as well. According to their work, it is possible to achieve sub-meter accuracy using OWPT. The idea of using the beacon timestamp and MAC timestamp was also discussed by Gholoobi and Stavrou [61]. Their method utilized a beacon timestamp (TOT at AP) for synchronization and a MAC timestamp (TOA at MD) for localization. The beacon interval and service set identifier packets were used to filter the data. System calibration was performed at zero distance separation between the AP and MD. Statistical processing was used to overcome the low resolution of the clock. They achieved a mean error of less than 2.5 m in a LOS environment.

5.4. Time Domain Physical Layer Methods

Measuring TOA at the physical layer can lead to more accurate distance estimates since the variations in timing introduced in the upper layers are avoided. However, complex custom hardware must be added. The following subsections report physical layer algorithms.

5.4.1. Sample Level Methods

Time domain methods estimate the TOA at the receiver before the FFT (see Figure 2 (b)). These methods mostly employ cross-correlation of the received signal with a reference signal. Typically, the short training or long training symbols are used for estimation. The following paragraphs focus on time domain methods which utilise the sampled baseband signal.

Two-way ranging using probe request-probe response exchange was employed by two Intel engineers in [6] to capture waveforms at the source node on transmission of a packet and on reception of the response. Matched filtering was applied to obtain the TOT and TOA estimates. The AP processing delay was calibrated using direct measurements and a customized AP. Antenna and frequency diversity were used to combat multipath. They compared TOA measurements with RSSI measurements and concluded that TOA is more accurate. They achieved localization root mean square error in the range 1.1-5.5 m from various APs when using multipath mitigation. The results degraded to 4.1-13.9 m without multipath mitigation. Sub-meter accuracy was achieved using a directional antennae.

A matched filtering and time averaged power technique was proposed by Geiger [62] to detect TOA in 802.11b. The slope of the time-averaged power was used as a gross estimate of the start of the frame and a peak finder was employed to obtain a finer grained measurement. Using this method, a resolution of 40 ns (approximately 12 m) in the TOA timestamps was obtained in simulation. Reddy et al [63, 64] also proposed a two-stage algorithm. The received signal was correlated with a reference signal stored in the receiver to obtain a coarse estimate of the TOA. The Long Training Sequence was used to estimate the Channel Impulse Response (CIR). Five peaks around the maximum sample were chosen as possible paths. Since the start of the CIR is not certain, the system hypothesized a number of different candidate CIRs of the same length and including the maximum peak. Distorted reference signals were generated via convolution of the original reference signal with these candidates. The distorted reference signals were then correlated with the received signal. The approximate CIR was selected as the candidate giving the largest correlation peak, and the position of the maximum path represented the offset between the coarse TOA estimate and the true estimate. The refined estimate was obtained by subtracting this offset from the initial estimate. Matlab simulations showed the superiority of the proposed algorithm over a conventional cross-correlation method with an absolute error less than 50 ns (approximately 15 m) in 90% of the cases. However, no experimental study was conducted.

Researchers have also considered synchronization problems in the context of localization. An asynchronous time-based location determination system, called PinPoint was presented in [65]. According to the method, every pair of nodes in the network makes four one-way range measurements with measurement of TOT and TOA. Nodes perform one-way ranging then swap roles and repeat this process once. High clock resolution is employed to perform timestamping. The timestamps information is shared between the two nodes to determine the clock offset drifts and to estimate range. PinPoint achieved location accuracy of about 1.5 m in indoor LOS conditions.

Voltz and Hernandez explored the multipath problem in [66], identifying the LOS signal in an unknown multipath channel, using a maximum likelihood estimator for calculation of the TOA of the OFDM signals in a multipath environment. Based

13

on simulation, an error of less than 20 ns (approximately 6 m) was achieved in 90% of cases.

5.4.2. Sub-Sample Methods

In the conventional baseband matched filtering approach, the sampling frequency limits the time resolution of a single TOA measurement. However, some researchers have sought to extract sub-sample information, either by using special signal processing methods or higher sampling rates.

Konig et al [23] proposed a time domain cross-correlation between the received signal and a time-continuous Barker signal to calculate the TOA as the delay of the peak correlation. Sub-sample accuracy was achieved by repeating the process with various sub-sample offsets. The offset giving the largest peak was selected as correct. An accuracy of 1.17 m was achieved using this approach in a LOS environment. Sub-sample offset estimation was also discussed by He et al [67] when exploiting the characteristics of the FFT and IFFT to develop three estimation strategies: peak detection, modified maximum peak-to-leakage ratio detection and Channel Frequency Response (CFR) reconstruction. They were able to achieve an error of less than 2 m in 90% of cases in a LOS environment.

Similarly, Exel et al [68] designed and implemented a digital receiver and transmitter board called SMiLE (SMart integrated Localization Extension) that included a Field Programmable Gate Array for signal processing [68, 69]. They estimated the TOA after symbol detection and compensated for the digital processing delay, analog processing delay and fractional error in estimating the actual TOA. A squaring synchronizer was used to estimate the fractional sampling error. Localization was based on TDOA [36]. For synchronization, they adjusted clock rates by distributing a single frequency over the network via Ethernet clocking and the clock offsets were determined in the SMiLE boards. Under good conditions, i.e. a LOS stationary environment and no people or objects moving, their claimed accuracy was around 5 cm. This accuracy is well in excess of other methods. In part, this is due to the accuracy of the implemented physical layer signal processing using an ADC with 220 MHz sampling clock [68], and a local clock for timestamping and synchronization operating at a frequency of greater than 1 GHz. Overall, the approach can be considered as a high resolution multi-node clock synchronization technique with very accurately calibrated fixed delays. Although not clear in the paper, it seems that synchronization takes a long time to converge. Final results are reported after 100,000 packets.

Nur et al [25, 70] overcame the low sampling frequency of existing WLAN hardware by using a high sampling rate device to perform signal capture at 1 GS/s. The sampled signal obtained was post-processed using their Improved FOCUSS for Arrival Time Estimation (IFATE) algorithm to estimate the channel and the TOA. IFATE is an iterative estimation algorithm that provides the ability to detect closely spaced multipath components under WLAN operational environments. In experiments and simulation, sub-meter accuracy was achieved in indoor LOS environments.

In [71], to overcome the limited sampling frequency problem, the authors of this paper proposed a two-step TOA estimation algorithm using only the baseband signal. In the first step, the algorithm obtains a sample-level resolution estimate of the TOA by finding the peak of the absolute value of the cross-correlation of the in-phase and quadrature received signals with the known transmitted symbol. In the second step, the algorithm refines this estimate to sub-sample resolution by estimating the phase delay of the received signal based on the gradient of a linear fit to the phase difference between the transmitted and received sub-carriers in the frequency domain. The algorithm was applied to the LTS symbol of the 802.11g preamble. In real-world experiments, the algorithm was found to achieve a mean TOA estimation error of 49 cm in a low multipath LOS environment.

5.5. Frequency Domain Physical Layer Methods

Super resolution algorithms have been proposed for WiFi ranging recently. In these methods, TOA is estimated at the receiver in the frequency domain, i.e. after the FFT in OFDM systems (see Figure 2 (b)) as depicted in Figure 9. As reported in [72], so called super resolution techniques can significantly improve the performance of TOA estimation compared to conventional time domain techniques due to their ability to improve the spectral efficiency of the measurement system.

The concept of MUltiple SIgnal Classification (MUSIC) and Estimation of Signal Parameters via Rotational Invariance Technique (ESPRIT) super resolution approaches is to separate the signal subspace from the noise subspace using eigen-decomposition of the sample correlation matrix and

to realize precise estimation utilizing the orthogonality between the two subspaces. High accuracy results, about 18 cm ranging error, were reported in simulations of the MUSIC algorithm [73]. Much lower accuracy, i.e. around 5 m in 50% of cases, was obtained in [74] using a different simulation setup. In [75], using a modified MUSIC algorithm, called Root-MUSIC, experimental results showed high precision ranging with ranging errors less than 0.5 m in 71% and less than 1 m in 93% of cases. To eliminate the search procedure inherent in MUSIC, the ESPRIT algorithm was utilized since it can estimate the signal parameter directly from the eigenvalues. The authors of [76] provide a comparison between the two algorithms based on Matlab simulation and a LOS channel. ESPRIT outperforms MUSIC but the achieved accuracy is still low, around 5 m.

The authors of [77] studied the use of Matrix Pencil (MP) algorithms for TDOA estimation. The Matrix Pencil (MP) super resolution algorithm processes the data directly without forming a covariance matrix, i.e. snapshot-by-snapshot analysis is used. The frequency domain Channel Transfer Function (CTF) is obtained from the received OFDM symbol. The MP algorithms use a single snapshot of the CTF to estimate the time delays and TDOA of the direct path signals in the presence of multipath. The performance of various realisations of the MP algorithms were compared for OFDM IEEE 802.11 systems. These realisations were tested using two cables of different lengths connected between the transmitter and receiver. In [78], the authors investigated the use of channel sweeping and a Vector Network Analyzer (VNA) for CTF estimation rather than extraction from an OFDM symbol. In both papers [77, 78], sub-nano second (sub-meter) accuracy was obtained experimentally.

In [79], the authors compared experimentally the performance of 4 super-resolutions methods for TDOA location estimation in a real-world experimental setup. The methods evaluated were Root-MUSIC, ESPRIT, and MP. Both the LTS and STS were used. A combined wired and wireless channel was used in the experiments. It was found that, the Root-MUSIC algorithm gives the most accurate TDOA estimation with an error of 3.5 ns (approximately 1m) when STS is used. On the other hand, when utilizing LTS, ESPRIT is the most accurate estimator with an error of 3.2 ns (approximately 1 m).

6. Discussion and Future Directions

Roughly speaking, when the multipath environment is unknown, typical accuracies indoors of 4 m, 2-3 m, and 1-2 m are achievable using application [22], MAC/driver [51] and physical layer [23] methods, respectively. In all cases, statistical methods are used to enhance accuracy by post-processing the raw measurements. Although access to the lower layers provides increased timing resolution, it is clear that this does not translate directly to increased ranging accuracy. In most cases, improvements in accuracy have been limited by the presence of multipath.

In recent years, time resolution has been further enhanced by the introduction of sub-sample methods leading to sub-meter ranging accuracies [70]. To date, the best ranging accuracy has been reported by the SMilE project (5 cm) [36]. It is worth noting that these results were produced under low multipath conditions with a high degree of calibration and wired timing synchronization.

As well as addressing the timing resolution challenge, a number of papers have sought to explicitly reduce or separate the effects of multipath [6]. Dealing with multipath was shown to improve accuracy by 3 m in the case of [6]. However, the flexibility and effectiveness of these techniques over a wide range of multipath conditions is unclear.

Super resolution approaches offer an interesting alternative to the previous trend of enhancing time resolution. The reported results have been mixed: sub-meter to 10 m [73][74]. Much of this work has been simulation based. More experimental results for this class of algorithm would be useful. Computational complexity and sampling rate are also concerns. In terms of cost, flexibility and ease of deployment, application layer, MAC Layer, and driver-based software techniques are much more attractive than MAC and Physical Layer hardware techniques since they exploit off-the-shelf equipment with no or minor changes. It is worth noting that some Physical Layer approaches require significant signal processing and computational resources [55].

Recent and future advances in IEEE standards are expected to be positively reflected in improvements in positioning accuracy. The introduction of IEEE 802.11v means that authentication and association between the MD and AP are no longer necessary to initiate a RTT between nodes [80]. In addition, timestamping of the transmission and re-

Figure 9: MUSIC super resolution algorithms [18].

Table 3: Summary of time-based methods (Category: 1= application layer, 2= MAC layer supported with hardware, 3= MAC layer supported with software, 4= time domain physical layer, 5= frequency domain physical layer; Challenge addressed: TR= timestamp resolution, MP=multipath, SY=synchronization, and SF=sampling frequency; Evaluation method: M=experimental measurement, S=simulation; Accuracy in m; Environment: Line Of Sight or Non-Line Of Sight).

Ref.	Cat.	Chal.	Method	Eval.	Accuracy	Env.
[11]	1	TR	RTT	M	1D mean ranging error of 8 m	LOS
[22]	1	TR	four way TOA	M	2D mean positioning error of 4 m	LOS
[44]	1	TR	four way TOA	M	2D mean positioning error of 4 m	LOS
[45]	2	TR	RTT	M	1D ranging error of 2 - 2.3 m in 90% of cases	LOS & NLOS
[46]	2	TR	RTT	M	1D ranging error of 1.4 m in 90% of cases	LOS
[48]	2	TR	RTT	M	1D mean ranging error of 0.81 m to 2.63 m	LOS
[47]	2	TR	RTT	M	1D ranging error of 1.4 m in 90% of cases	LOS
[49, 50]	2	TR	RTT	M	1D mean ranging error of 1 - 1.7 m	LOS
[51]	3	TR	RTT	M	2D positioning error of 3.51 m in 50% of cases	NLOS & hard multipath
[55]	3	TR	RTT	M	1D mean ranging error of 1.7 m	LOS
[57]	3	TR	RTT	M	1D mean ranging error of 1.33 - 4.24 m and 27 - 275 m with HP and samsung hardware respectively	LOS
[58]	3	TR	RTT	M	1D mean ranging error of 1.5 - 4.4 m	LOS
[5]	3	TR	RTT	M	1D mean ranging error of 1.46 - 2.1 m	LOS
[59]	3	TR	RTT	M	1D ranging error of 1 m in 80% of cases	LOS
[60]	3	TR + SY	one way TOA	S	1D mean ranging error < 1 m	LOS
[61]	3	TR + SY	one way TOA	M	1D mean ranging error of 2.5 m	LOS
[6]	4	SF + MP	RTT	M	1D RMSE in the range 1.1 - 5.5 m	LOS/NLOS
[63, 64]	4	2	TOA	S	error < 50 ns (15 m approx.) in 90% of cases	NA
[65]	4	SY	TOA	M	2D mean positioning error of 1.2 - 1.8 m	LOS/NLOS
[66]	4	MP	TOA	S	error < 20 ns (6 m approx.), in 90% of cases	Hard multipath
[23]	4	SF	four way TOA	M	1D mean ranging error of 1.17 m	LOS
[67]	4	SF	TDOA	M	2D positioning error of 2 m in 90% of cases	LOS
[69]	4	SF	TDOA	M	2D mean positioning error of 5 cm	LOS
[25, 70]	4	SF	TOA	M	1D mean ranging error of 0.62 m	LOS
[71]	4	SF	TOA	M	1D mean ranging error of 0.49 m	LOS
[73]	5	SF	TOA	S	1D mean ranging error of 0.18 m	AWGN SNR
[74]	5	SF	TOA	S	1D ranging error of 5 m in 50% of cases	NA
[75]	5	SF	TOA	M	1D ranging error of 1 m in 93% of cases	LOS
[76]	5	SF	TOA	S	1D mean ranging error of 5 m	LOS
[78]	5	SF	TOA	M	1D mean ranging error < 1 m	LOS
[77]	5	SF	TOA	M	1D mean ranging error< 1 m	Cables
[79]	5	SF	TDOA	M	error < 3.5 ns (1 m approx.)	Cable+NLOS

16

ception of frames is allowed using a high-resolution clock (nanoseconds accuracy) [80]. This provides a high accuracy time synchronization mechanism between nodes. In a simulation study, the authors of [80] assessed the impact of the IEEE 802.11v standard on time-based positioning systems. They evaluated the commonly adopted RTT ranging approach (see Section 3.2) with and without IEEE 802.11v capabilities. Their conclusion was that IEEE 802.11v can provide important benefits to RTT-based positioning in terms of ease of deployment and flexibility in the number of nodes which may lead to broader exploration of the RTT-based techniques. However, the simulation results do not show significant improvements for 802.11v over 802.11b/g in terms of accuracy. To the authors' knowledge, the v amendment has not yet been commercialized and no experimental results have been reported. MIMO, beam-forming and the wider bandwith of IEEE 802.11ac are expected to be helpful in minimizing the effects of multipath and sample accuracy TOA detection problems. In addition, IEEE 802.11ax allows dense networks. It is likely that co-operative positioning will help to minimize the effect of interference, reduce the probability of NLOS, and reduce the effects of noise since measurements can be averaged from many sources.

A number of avenues for future research are evident.

Firstly, the RF environments in which experimental studies have been conducted are highly variable. This leads to difficulties in comparing the reported results. It would be advantageous to have metrics and models which consistently and unambiguously describe real-world experimental RF environments so that comparisons can be made. Most channel models are designed for communications purposes and so use statistical models which do not capture the interplay between multipath and location. RF modelling using ray-tracing techniques does capture this correspondence and may be more suitable for this purpose [81].

Secondly, improved methods for mitigating multipath are needed. Many time-based methods show promise in low multipath environments but fail in high multipath environments. An interesting alternative to the use of enhanced post-processing of the signal is the use of antennae arrays with beam-steering and beam-forming capabilities at the transmitter and receiver, respectively [82]. In addition modern classification methods may be helpful in addressing the problem of direct path TOA identification.

Thirdly, it is clear that sub-sample resolution is needed for high accuracy. While much progress has been made on this aspect of the problem, it is not clear that current state-of-the-art approaches are sufficiently robust and reliable. From a power consumption perspective, it is desirable that sub-sample resolution is achieved without increases in the baseband sampling frequency. This requirement points to the need for improved signal processing algorithms.

Fourthly, little work has been done on co-operative multi-node WiFi positioning, i.e. fusing information from multiple 802.11 nodes. Exploiting higher node density has the potential to increase accuracy through increased averaging. This approach would seen to be inline with the ongoing explosion in the number of WiFi devices in the built environment. While promising from a location point-of-view, there are many unsolved issues in terms of media access and security.

7. Conclusions

This paper has surveyed research conducted on time-based WiFi location estimation systems. The area is active with numerous systems and techniques developed. There has been a clear progression over the years in attempts to increase time resolution in order to enhance ranging accuracy. This progression has seen systems perform timestamping and TOA estimation at successively lower layers in the stack. Although a small number of papers have reported sub-meter accuracy in LOS, low multipath environments, there are still many unresolved issues in dealing with multipath and NLOS. To date, the best positioning accuracy has been reported by the SMilE project (5 cm) [36]. The method has shown its superiority under low multipath conditions with a high degree of calibration and wired timing synchronization. However, accuracy dramatically deteriorates in hard multipath or NLOS conditions. This paper has indicated a number of avenues for further research which may fruitfully address these challenges and improve upon the current state-of-the-art.

Acknowledgment

References

[1] F. Evennou, F. Marx, Advanced integration of WiFi and inertial navigation systems for indoor mobile positioning, Eurasip Journal on Applied Signal Processing 2006 (2006) 1–11.

[2] R. Mautz, Indoor positioning technologies, Ph.D. thesis, ETH Zürich (2012).

[3] D. Zhang, F. Xia, Z. Yang, L. Yao, W. Zhao, Localization technologies for indoor human tracking, in: 5th Int. Conf. on Future Information Technology, 2010, pp. 1–6.

[4] Y. Agarwal, B. Balaji, R. Gupta, J. Lyles, M. Wei, T. Weng, Occupancy-driven energy management for smart building automation, in: Proc. of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, 2010, pp. 1–6.

[5] S. B. Wibowo, M. Klepal, D. Pesch, Time of Flight ranging using off-the-self IEEE 802.11 WiFi tags, in: Proc. of the Int. Conf. on Positioning and Context-Awareness, 2009.

[6] S. A. Golden, S. S. Bateman, Sensor measurements for Wi-Fi location with emphasis on time-of-arrival ranging, IEEE Transactions on Mobile Computing 6 (2007) 1185–1198.

[7] M. M. Saad, C. J. Bleakley, T. Ballal, S. Dobson, High-accuracy reference-free ultrasonic location estimation, IEEE Transactions on Instrumentation and Measurement 61 (2012) 1561–1570.

[8] M. M. Saad, C. J. Bleakley, S. Dobson, Robust high-accuracy ultrasonic range measurement system, IEEE Transactions on Instrumentation and Measurement 60 (2011) 3334–3341.

[9] C. D. McGillem, T. S. Rappaport, Infra-red location system for navigation of autonomous vehicles, in: Proc. of IEEE Int. Conf. on Robotics and Automation, 1988, pp. 1236–1238.

[10] M. M. Saad, C. J. Bleakley, M. Walsh, T. Ye, High accuracy location estimation for a Mobile Tag using one-way UWB signaling, in: Ubiquitous Positioning, Indoor Navigation, and Location Based Service, 2012, pp. 1–8.

[11] A. Günther, C. Hoene, Measuring round trip times to determine the distance between WLAN nodes, in: Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems, Springer, 2005, pp. 768–779.

[12] J. Hallberg, M. Nilsson, K. Synnes, Positioning with bluetooth, in: 10th Int. Conf. on Telecommunications, ICT, Vol. 2, 2003, pp. 954–958.

[13] P. Bahl, V. N. Padmanabhan, RADAR: An in-building RF-based user location and tracking system, in: Proc. of the 19th Annual Joint Conf. of the IEEE Computer and Communications Societies, Vol. 2, 2000, pp. 775–784.

[14] H. Liu, H. Darabi, P. Banerjee, J. Liu, Survey of wireless indoor positioning techniques and systems, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews 37 (2007) 1067–1080.

[15] V. Honkavirta, T. Perala, S. Ali-Loytty, R. Piché, A comparative survey of WLAN location fingerprinting methods, in: 6th Workshop on Positioning, Navigation and Communication, 2009, pp. 243–251.

[16] G. Sun, J. Chen, W. Guo, K. R. Liu, Signal processing techniques in network-aided positioning: a survey of state-of-the-art positioning designs, IEEE Signal Processing Magazine 22 (2005) 12–23.

[17] Y. Gu, A. Lo, I. Niemegeers, A survey of indoor positioning systems for wireless personal networks, IEEE Communications Surveys & Tutorials 11 (2009) 13–32.

[18] Z. Yang, Z. Zhou, Y. Liu, From RSSI to CSI: Indoor localization via channel response, ACM Computing Surveys (CSUR).

[19] 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(Revision of IEEE Std 802.11-2007) (2012) 1–2793.

[20] B. P. Crow, I. Widjaja, J. G. Kim, P. T. Sakai, IEEE 802.11 wireless local area networks, IEEE Communications Magazine 35 (1997) 116–126.

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

[22] C. Hoene, J. Willmann, Four-way TOA and software-based trilateration of IEEE 802.11 devices, in: IEEE 19th Int. Symp. on Personal, Indoor and Mobile Radio Communications, 2008, pp. 1–6.

[23] S. König, M. Schmidt, C. Hoene, Precise time of flight measurements in IEEE 802.11 networks by cross-correlating the sampled signal with a continuous barker code, in: IEEE 7th Int. Conf. on Mobile Adhoc and Sensor Systems, 2010, pp. 642–649.

[24] IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band, IEEE Std 802.11a (1999) 1–102.

[25] K. Nur, S. Feng, C. Ling, W. Ochieng, Application of the improved FOCUSS for arrival time estimation (IFATE) algorithm to WLAN high accuracy positioning services, in: Ubiquitous Positioning, Indoor Navigation, and Location Based Service, 2012, pp. 1–8.

[26] 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 (2000) 1–90.

[27] 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 Amendment 4: Further Higher Data RateEx-

tension in the 2.4 GHz Band, IEEE Std 802.11g.

[28] R. Khanduri, S. Rattan, A. Uniyal, Understanding the Features of IEEE 802.11 g in High Data Rate Wireless LANs, International Journal of Computer Applications 64 (8) (2013) 1–5.

[29] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput, IEEE Std 802.11n (2009) 1–565.

[30] IEEE Standard for Information technology– Telecommunications and information exchange between systemsLocal and metropolitan area networks– Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications–Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz., IEEE Std 802.11ac (2013) 1–425.

[31] D.-J. Deng, K.-C. Chen, R.-S. Cheng, Ieee 802.11 ax: Next generation wireless local area networks, in: International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, 2014, pp. 77–82.

[32] O. Bejarano, E. W. Knightly, M. Park, Ieee 802.11 ac: from channelization to multi-user mimo., IEEE Communications Magazine 51 (2013) 84–90.

[33] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: IEEE 802.11 Wireless Network Management, IEEE Std 802.11v (2011) 1–433.

[34] Y. Zhou, A closed-form algorithm for the least-squares trilateration problem, Robotica 29 (2011) 375–389.

[35] D. E. Manolakis, Efficient solution and performance analysis of 3-D position estimation by trilateration, IEEE Transactions on Aerospace and Electronic Systems 32 (1996) 1239–1248.

[36] S. Schwalowsky, H. Trsek, R. Exel, N. Kero, System integration of an IEEE 802.11 based TDoA localization system, in: Int. IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication, 2010, pp. 55–60.

[37] M. D. Gillette, H. F. Silverman, A linear closed-form algorithm for source localization from time-differences of arrival, IEEE Signal Processing Letters 15 (2008) 1–4.

[38] Z. Li, D. C. Dimitrova, D. H. Raluy, T. Braun, TDOA for narrow-band signal with low sampling rate and imperfect synchronization, in: 7th Wireless and Mobile Networking Conference, 2014, pp. 9–16.

[39] F. Winkler, E. Fischer, E. Graß, G. Fischer, A 60 GHz OFDM indoor localization system based on DTDOA, 4th Information Society Technologies Mobile and Wireless Communications Summit.

[40] F. Winkler, E. Fischer, E. Grass, P. Langendörfer, An indoor localization system based on DTDOA for different wireless LAN systems, in: 3rd Workshop on Positioning, Navigation and Communication, 2006.

[41] A. Bensky, Wireless positioning technologies and applications, Artech House, 2007.

[42] N. Kong, T. Eng, L. B. Milstein, A selection combining scheme for RAKE receivers, in: 4th IEEE Int. Conf. on Universal Personal Communications, 1995, pp. 426–430.

[43] K. Muthukrishnan, G. T. Koprinkov, N. Meratnia, M. E. M. Lijding, Using time-of-flight for WLAN localization: feasibility study, Technical report, Centre for Telematics and Information Technology University of Twente, Enschede (2006).

[44] P. Vorst, J. Sommer, C. Hoene, P. Schneider, C. Weiss, T. Schairer, W. Rosenstiel, A. Zell, G. Carle, Indoor positioning via three different RF technologies, in: 4th European Workshop on RFID Systems and Technologies, 2008, pp. 1–10.

[45] F. Izquierdo, M. Ciurana, F. Barceló, J. Paradells, E. Zola, Performance evaluation of a TOA-based trilateration method to locate terminals in WLAN, in: 1st Int. Symp. on Wireless Pervasive Computing, 2006, pp. 1–6.

[46] M. Ciurana, F. Barceló, S. Cugno, Indoor tracking in WLAN location with TOA measurements, in: Proc. of the 4th ACM int. workshop on mobility management and wireless access, 2006, pp. 121–125.

[47] M. Ciurana, F. Barcelo-Arroyo, S. Cugno, A novel TOA-based indoor tracking system over IEEE 802.11 networks, in: 16th IST Mobile and Wireless Communications Summit, 2007, pp. 1–5.

[48] M. Ciurana, F. Barcelo-Arroyo, F. Izquierdo, A ranging system with IEEE 802.11 data frames, in: IEEE Radio and Wireless Symposium, 2007, pp. 133–136.

[49] J. Prieto, A. Bahillo, S. Mazuelas, J. Blas, P. Fernández, R. Lorenzo, RTS/CTS mechanism with 802.11 for indoor location.

[50] A. Bahillo, J. Prieto, S. Mazuelas, R. M. Lorenzo, J. Blas, P. Fernandez, IEEE 802.11 distance estimation based on RTS/CTS two-frame exchange mechanism, in: IEEE 69th Vehicular Technology Conference, 2009, pp. 1–5.

[51] J. Prieto, A. Bahillo, S. Mazuelas, R. Lorenzo, J. Blas, P. Fernández, Adding indoor location capabilities to an IEEE 802.11 WLAN using real-time RTT measurements, in: Wireless Telecommunications Symposium, 2009, pp. 1–7.

[52] A. Bahillo, P. Fernández, J. Prieto, S. Mazuelas, R. M. Lorenzo, E. J. Abril, Distance estimation based on 802.11 RTS/CTS mechanism for indoor localization, Advances in Vehicular Networking Technologies. Rijeka: In-Tech (2011) 217–236.

[53] A. Bahillo, S. Mazuelas, R. M. Lorenzo, P. Fernández, J. Prieto, R. J. Durán, E. J. Abril, Accurate and integrated localization system for indoor environments based on IEEE 802.11 round-trip time measurements, Journal on Wireless Communications and Networking.

[54] J. Kim, J.-K. Hong, L. Dong-Jin, S.-S. Lee, Time stamping method using additional TPU for improvement of positioning precision, in: Int. Conf. on ICT Convergence, 2012, pp. 105–106.

[55] M. Ciurana, D. López, F. Barceló-Arroyo, SofTOA: Software ranging for TOA-based positioning of WLAN terminals, in: Location and Context Awareness, Springer, 2009, pp. 207–221.

[56] M. Ciurana, D. Giustiniano, A. Neira, F. Barcelo-Arroyo, I. Martin-Escalona, Performance stability of software TOA-based ranging in WLAN, in: Int. Conf. on Indoor Positioning and Indoor Navigation, 2010, pp. 1–8.

[57] F. D. Lorenz Schauer, M. Maier, Potentials and Limitations of WIFI-Positioning Using Time-of-Flight, in:

Int. Conf. on Indoor Positioning and Indoor Navigation, 2013, pp. 1–9.

[58] I. Casacuberta, A. Ramirez, Time-of-Flight positioning using the existing wireless local area network infrastructure, in: Int. Conf. on Indoor Positioning and Indoor Navigation, 2012, pp. 1–8.

[59] D. Giustiniano, S. Mangold, Caesar: carrier sense-based ranging in off-the-shelf 802.11 wireless LAN, in: Proc. of the 7th Conf. on Emerging Networking Experiments and Technologies, 2011.

[60] X. Wang, T.-F. Lu, L. Chen, Synchronization and time resolution improvement for 802.11 WLAN OWPT measurement, in: Proc. of the Int. MultiConference of Engineers and Computer Scientists, Vol. 1, 2009, pp. 378–383.

[61] A. Gholoobi, S. Stavrou, A hybrid TDoA-ToA localization method, in: 20th Int. Conf. on Telecommunications, 2013, pp. 1–4.

[62] D. J. Geiger, High resolution time difference of arrival using timestamps for localization in 802.11 b/g wireless networks, in: IEEE Wireless Communications and Networking Conference, 2010, pp. 1–6.

[63] H. Reddy, M. Girish Chandra, P. Balamuralidhar, S. Harihara, K. Bhattacharya, E. Joseph, An improved Time-of-Arrival estimation for WLAN-based local positioning, in: 2nd Int. Conf. on Communication Systems Software and Middleware, 2007, pp. 1–5.

[64] H. Reddy, M. G. Chandra, S. Harihara, P. Balamuralidhar, J. Sen, D. Arora, WLAN-based local positioning using distorted template, in: Int. Symp. on Communications and Information Tech., 2007, pp. 1043–1048.

[65] M. Youssef, A. Youssef, C. Rieger, U. Shankar, A. Agrawala, Pinpoint: An asynchronous time-based location determination system, in: Proceedings of the 4th Int. Conf. on Mobile Systems, Applications and Services, 2006, pp. 165–176.

[66] P. J. Voltz, D. Hernandez, Maximum likelihood time of arrival estimation for real-time physical location tracking of 802.11 a/g mobile stations in indoor environments, in: Position Location and Navigation Symposium, PLANS, 2004, pp. 585–591.

[67] Z. He, Y. Ma, R. Tafazolli, Improved high resolution TOA estimation for OFDM-WLAN based indoor ranging, IEEE Wireless Communications Letters 2 (2013) 163–166.

[68] R. Exel, J. Mad, G. Gaderer, P. Loschmidt, A novel, high-precision timestamping platform for wireless networks, in: IEEE Conference on Emerging Technologies & Factory Automation, 2009, pp. 1–8.

[69] R. Exel, G. Gaderer, P. Loschmidt, Localisation of wireless LAN nodes using accurate TDoA measurements, in: IEEE Wireless Communications and Networking Conference, 2010, pp. 1–6.

[70] K. Nur, S. Feng, C. Ling, W. Ochieng, A new time estimation technique for high accuracy indoor WLAN positioning, in: The European Navigation Conference, 2011, pp. 1–14.

[71] A. Makki, A. Siddig, M. M. Saad, J. R. Cavallaro, C. J. Bleakley, High-resolution time of arrival estimation for OFDM-based transceivers, Electronics Letters 51 (2015) 294–296.

[72] X. Li, K. Pahlavan, Super-resolution TOA estimation with diversity for indoor geolocation, IEEE Transactions on Wireless Communications 3 (2004) 224–234.

[73] J. Li, L. Pei, M. Cao, D. Yu, Super-resolution time delay estimation algorithm based on the frequency domain channel model in OFDM systems, in: The Sixth World Congress on Intelligent Control and Automation, Vol. 1, 2006, pp. 5144–5148.

[74] F. Zhao, W. Yao, C. C. Logothetis, Y. Song, Super-resolution TOA estimation in OFDM systems for indoor environments, in: IEEE Int. Conf. on Networking, Sensing and Control, 2007, pp. 723–728.

[75] L. Jing, P. Liang, C. Maoyong, S. Nongliang, Super-resolution time of arrival estimation for indoor geolocation based on IEEE 802.11 a/g, in: 7th World Congress on Intelligent Control and Automation, IEEE, 2008, pp. 6612–6615.

[76] F. Zhao, W. Yao, C. C. Logothetis, Y. Song, Comparison of super-resolution algorithms for TOA estimation in indoor IEEE 802.11 wireless LANs, in: Int. Conf. on Wireless Communications, Networking and Mobile Computing, IEEE, 2006, pp. 1–5.

[77] A. Gaber, A. Omar, Sub-nanosecond accuracy of TDOA estimation using Matrix Pencil algorithms and IEEE 802.11, in: Int. Symp. on Wireless Communication Systems, 2012, pp. 646–650.

[78] A. A. Ali, A. 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, Vol. 5, 2005, pp. 11–20.

[79] S. Napoleon, A. Omar, S. Elramly, S. Khamis, M. E. Nasr, C5. time difference of arrival by IEEE 802.11a, g based on practical estimation, in: 29th National Radio Science Conference, 2012, pp. 185–190.

[80] M. Ciurana, F. Barceló-Arroyo, I. Martín-Escalona, Comparative performance evaluation of IEEE 802.11v for positioning with time of arrival, Computer Standards & Interfaces 33 (2011) 344–349.

[81] A. Tayebi, J. Gomez, F. M. Saez de Adana, O. Gutierrez, The application of ray-tracing to mobile localization using the direction of arrival and received signal strength in multipath indoor environments, Progress In Electromagnetics Research 91 (2009) 1–15.

[82] J. Xiong, K. Jamieson, ArrayTrack: A Fine-Grained Indoor Location System., in: Usenix NSDI, 2013, pp. 71–84.