Verification: Accuracy Evaluation of WiFi Fine Time Measurements on an Open Platform

Mohamed Ibrahim[1], Hansi Liu[1], Minitha Jawahar[1], Viet Nguyen[1],
Marco Gruteser[1], Richard Howard[1], Bo Yu[2], Fan Bai[2]
[1]WINLAB, Rutgers University, [2]General Motors Research

ABSTRACT

Academic and industry research has argued for supporting WiFi time-of-flight measurements to improve WiFi localization. The IEEE 802.11-2016 now includes a Fine Time Measurement (FTM) protocol for WiFi ranging, and several WiFi chipsets offer hardware support albeit without fully functional open software. This paper introduces an open platform for experimenting with fine time measurements and a general, repeatable, and accurate measurement framework for evaluating time-based ranging systems. We analyze the key factors and parameters that affect the ranging performance and revisit standard error correction techniques for WiFi time-based ranging system. The results confirm that meter-level ranging accuracy is possible as promised, but the measurements also show that this can only be consistently achieved in low-multipath environments such as open outdoor spaces or with denser access point deployments to enable ranging at or above 80 MHz bandwidth.

CCS CONCEPTS

• **Networks → Location based services**;

KEYWORDS

WiFi Localization, Fine Time Measurements, Ranging Evaluation

1 INTRODUCTION

WiFi positioning has established itself as a key positioning technology that together with GPS is widely used by mobile devices. Yet, precise indoor positioning, to obtain room-level location or to support indoor navigation has remained stubbornly challenging due to the large effort required to create and maintain WiFi surveys. Similar challenges exist in urban canyons, where GPS accuracy is degraded due to multipath and WiFi positioning cannot entirely replace it.

Among many other solutions, researchers have long advocated for RF time-of-flight positioning methods. Time-based WiFi ranging techniques have been introduced in [17, 19] and followed by several improvements [7–9, 11, 15]. More recently, IEEE 802.11-2016 standardized [5] a Fine Time Measurement (FTM) protocol that supports such ideas. According to the WiFi alliance, this ranging system offer meter-level accuracy [1]. Major WiFi chipset vendors have already released WiFi chipsets that support FTM protocol based on 802.11REVmc and Android P support has been announced [2]. Beside the 802.11 standard documents, there are few details about implementation techniques and the performance of such ranging systems [6] using the off-the-shelf WiFi chipsets.

Given the momentum building around this technology, this paper therefore sets out to verify the research and standard accuracy claims. We describe an open tool for the research community to experiment with WiFi fine-time measurements, based on the the Intel Dual Band Wireless-AC 8260 and 8265 cards and their open-source Linux driver. We also develop a systematic methodology for measuring the performance of time-based ranging systems to enhance the repeatability of such experiments by gradually introducing additional reflectors in the environment that add multipath propagation.

Generally, WiFi time-of-flight ranging estimates distance by measuring the round-trip time of a signal between a station and an access point. It promises several advantages. First,
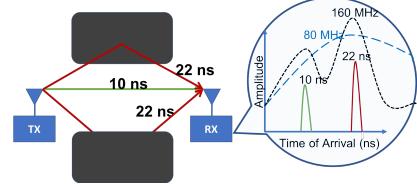
time-of-flight is linearly dependent on range (as opposed to received signal strength, for example), which should allow a ranging error nearly independent of distance. Second, the timing of the leading edge of a signal is less dependent on multipath than the signal amplitude.

Given this, one might expect that the accuracy of time-based ranging systems that have nanosecond resolution should not be affected by multipath while the line-of-sight (LoS) transmission is not blocked. We found that the accuracy of this ranging system at 2.4 GHz and up to 40 MHz bandwidth is significantly affected by the non-line-of-sight (NLoS) components of the transmitted signal in non-open space environments. At 5 GHz and 80 MHz bandwidth the results approach meter-level accuracy in the indoor LoS environment but become unreliable in a NLoS environment at distances above 20m. It therefore, requires denser access point deployments to realize these gains.

Given that speed-of-light signals cannot arrive too early, one might also expect that ranging errors are biased towards long estimates rather than short estimates. We found that some configurations of the system, in particular 2.4 GHz with 20-40 MHz bandwidth at the access point, frequently outputs short estimates and without calibration can produce negative estimated ranging distances, when the ground truth distance is less than 6 meters. This bias occurs even when the LoS component of the signal is dominant to the NLoS components. Using external antennas with different orientations can help to alleviate this problem. Also, using longer cables to connect the two antennas to the card (which increases the propagation delay) can correct this, along with filtering out measurement noise. After canceling out the offset, the estimated distances are within (± 1) m of the actual distances in an outdoor open-space setup.

In summary, the major contributions of this paper are as follows:

- Conducting an evaluation and verification of the performance claims of WiFi time-of-flight ranging and positioning in several benchmark and real-world environments.
- Introducing, analyzing, and calibrating an open platform for conducting WiFi time-of-flight experiments to the research community.
- Proposing a repeatable measurement framework for evaluating time-based ranging systems.
- Confirming the expected meter-level ranging accuracy in open-space outdoor environments, while showing that multipath environments remain a challenge at least at lower bandwidths.

Figure 1: Multipath problem.

2 BACKGROUND

A wireless ranging system estimates the distance between two devices by sending a wireless signal between them. As the signal travels between the two devices, its properties change over the distance. These properties include amplitude, frequency and phase. Moreover, given the propagation speed of the signal, a ranging system can estimate the distance by estimating the time the signal takes to travel between two devices. In this section, we illustrate time-based ranging systems and their challenges.

2.1 Multipath Challenge

A key challenge that limits ranging systems is multipath, where the transmitted signal is reflected in the environment and reaches the receiver's antenna by more than one path. These paths have different lengths resulting in different RTTs. Therefore, ranging accuracy depends directly on whether the RTT measurement is based on the direct path or a reflected path. The main challenge, in presence of multipath, is how to distinguish the direct path signal from the reflected signals. In case of non-blocked direct path, this problem seems to be solvable for time-based ranging, by simply picking the first received signal. However, dealing with signals that travel with speed of light complicates the problem.

Bandwidth and raw localization resolution. Detecting the arrival of a packet is challenging since a difference of 1 ns could result in an error of 1 foot for the RF ranging systems (speed of light ≈ 1 foot/nanosecond). Therefore, a fine resolution clock with 1 ns or higher is needed for 1 foot raw accuracy. Another factor that limits the accuracy resolution for packet detection algorithms is the channel bandwidth. For example, WiFi signal is sampled once every 50 nanoseconds for a 20 MHz channel, during this period, the signal travels 15 meters. Therefore, distinguishing between two signal spaced by a distance less than that raw resolution is challenging problem. Prior super-resolution spectral signal processing techniques [16, 26] can improve this raw resolution. Fig. 1 shows the multipath problem, and illustrates the channel bandwidth effect on the ranging error. In this figure, the transmitted signal reaches the receiver through three main paths, line of sight (LoS), and two reflections from

parallel planes (same material and same distance to transmitter). However, the LoS component of the signal reaches the receiver first, the NLoS components arrive afterwards with the same signal phases, resulting stronger received signal through constructive interference. With enough bandwidth, hence higher ADC sampling rate, the receiver will be able to sample enough to distinguish between the first arrival through direct path and the multipath reception.

2.2 Evaluation Challenges

Different environments lead to different multipath profiles, hence result in different performances for ranging systems. Therefore, it is challenging to produce repeatable and generalized results to evaluate a ranging system . Moreover, details about signal processing algorithms implemented on current off-the-shelf cards that support the FTM ranging system are not available, even for the open source drivers. These physical layer algorithms are implemented in the firmware of these cards. As a result, there is no information about how the packet arrival is being detected, how the implementation deals with multipath problem, or what is the bandwidth used for the packet arrival detection. Even details about the clock resolution of these cards are not available. In this paper, we present a measurement framework for evaluating the FTM ranging system, even without knowing beforehand the answers of the previously mentioned questions.

2.3 Fine Time Measurement

IEEE 802.11-2016 standardized a Fine Time Measurement (FTM) protocol that enables a pair of WiFi cards to estimate distance between them. Fig. 2 illustrates the details of the FTM protocol. An initiator is a station (STA) that initiates the FTM process by sending a FTM Request to a corresponding access point (AP). An AP that supports the FTM procedure as a responding device (Fig. 2) is called a responder. Based on the AP response, the protocol agrees or refuses to continue the ranging process. In the case of agreement, the AP/responder starts to send FTM message and wait for its ACK. The RTT is estimated based on the transmission timestamp of the FTM message and the reception timestamp of its ACK. The AP may send multiple FTM messages, but have to wait for acknowledgement, before sending a new message. Fig. 2 shows an example of one burst with 3 FTM messages, with ASAP mode set to 1[1]. The RTT is calculated for n FTM messages as follows:

$$RTT = \frac{1}{n}(\sum_{k=1}^{n} t_4(k) - \sum_{k=1}^{n} t_1(k)) - \frac{1}{n}(\sum_{k=1}^{n} t_3(k) - \sum_{k=1}^{n} t_2(k))$$

[1]STA is ready to receive FTM messages and hence, capable of capturing timestamps associated with an initial FTM message and sending them in the following message
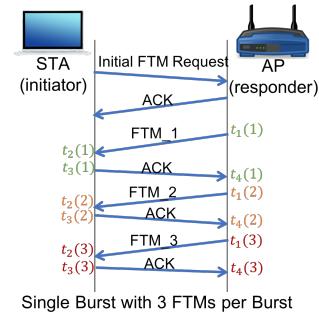

Single Burst with 3 FTMs per Burst

Figure 2: FTM Protocol Overview.

Generally, the protocol excludes the processing time on the STA by subtracting it ($t_3 - t_2$) from the total round trip time ($t_4 - t_1$), which represents the time from the moment the FTM message is being sent (t_1) to the moment the ACK is being received (t_4). This calculation is repeated for each FTM-ACK exchange and the final RTT is the average over the number of messages in the burst.

3 OPEN WIFI TIME-OF-FLIGHT PLATFORM AND BASIC RANGING CALIBRATION

3.1 Open WiFi FTM Tool

Hardware. While several vendors offer WiFi implementations with support for the FTM standard, we chose the Intel Dual Band Wireless-AC 8260 and 8265 since they are the only ones for which we were able to obtain open software support for accessing FTM measurements (an open source Linux driver with an experimental FTM implementation). In practice, we found that this driver requires further modifications to be usable for FTM measurements. We refer to these cards as WiFi card A and use them as the station to take measurements as well as the access point in some experiments. In access point mode, these cards unfortunately only support the 2.4 GHz band and 20/40MHz channels but they do support 5GHz and higher bandwidth as clients. Moreover, we found that the ASUS Wireless-AC1300 RT-ACRH13 APs is configured to respond to FTM requests out of the box. This AP uses the Qualcomm IPQ4018 chipset and also supports the 5GHz band with higher bandwidths. We refer to this AP as AP B.

Software versions for open station. In our framework, APs and STAs use Linux kernel version 3.19.0-61-lowlatency. Although, the FTM protocol is implemented in newer kernel versions, it is only supported by the backport LinuxCore releases of the IWLWIFI driver [3]. We therefore use the IWLWIFI driver from the LinuxCore30 release, along with firmware version 31. The station can be configured with

the iw (nl80211 based CLI configuration utility for wireless devices in Linux) Linux command line tool.

Configuring WiFi cards as FTM responding access points. The node can be configured as access point using hostapd (we used version 2.6). Configuring a node as AP through hostapd does not automatically enable it to respond to FTM protocol messages. We therefore modified the IWL-WIFI driver to activate the responding feature when it is configured as an access point and make this patch available. Through hostapd configuration, the AP can publish their FTM support as a responder through the beacon frames.

Initiating FTM requests. There are two options for triggering an FTM ranging request at the station. The first option is to leverage Linux Debugfs, a filesystem that enables communication between kernel and user space. The second option, which we adopt in this paper, is to use iw command line tool, along with a patch [4] that adds the FTM feature to the iw command and enables the STA to initiate the FTM process by sending FTM request. An initiating STA needs to acquire specific information about the AP in order to send the FTM request. This information includes MAC address, supported bandwidth, and frequency. Therefore, our tool starts the process by scanning the surrounding APs, in order to acquire the needed information. If a STA sends a FTM request to an AP, that doesn't support FTM, this AP will not respond and the STA has to wait for timeout to return unsuccessful ranging status. To avoid this delay, our tool send FTM requests only to the APs that supports FTM protocol. According to the standard [5], each AP that supports FTM as a responder shall publish this information in the beacon frames, (a specific bit in the extended capabilities record refers to FTM responder support.

RTT calculation. After initiating the FTM process, the AP starts to send FTM frame automatically and waits for its ACK to estimate the RTT. This process is implemented in the proprietary firmware but based on the standard we know that in order to remove the processing time for the initiating STA from the RTT, the responding AP transfers the timestamp values it captured (t_1 and t_4) to the initiating STA in the follow up FTM frame. The initiating STA is the responsible for computing the RTT, this computation is done in the firmware. By increasing the number of samples per burst, the AP sends several FTM frames in a sequence and the initiating STA estimates the RTT for each pair of FTM message/ACK. The RTT for each pair of FTM message/ACK is not available in the driver, only the averaged RTT over the burst in picoseconds along with the corresponding distance in centimeters and average received signal (RSSI) are finally returned.

Tool limitations. Extracting information including CSI, phase and measurement per antenna is currently not available due to firmware limitations. Similarly, ranging accuracy

depends on the communication bandwidth which implies having an analogue-to-digital converter (ADC) that can sample at that rate. WiFi card A can be configured as access point for up to 40MHz and should support up to 160MHz bandwidth as a station with an appropriate 802.11mc compliant access point. So far we were able to confirm support up to 80MHz.

3.2 Experimental Setup

Our experimental setup consists of two small form factor PCs (containing WiFi card A), one of them configured as AP and the other one as STA. We refer to this setup as WiFi card A setup. In a second setup, we use AP B, while still using the same small form factor PC as station. We refer to this setup as AP B setup. In these two main setups, we evaluate the FTM protocol supported by WiFi card A and AP B. These WiFi chipsets require two antennas. We use omnidirectional antennas with 6 dBi gain. To extend the height of the antennas, we use 6-feet CNT-240 cables, in which the velocity of the signal is 83% the speed of light in a vacuum and the attenuation for 2.4GHz is 12.9 dB/100 feet. Along with the cables, we use PVC pipes to fix the antennas on specific height while avoiding disturbing the signal. For measuring the ground truth distance, we use 400-Feet measuring tape, along with BOSCH GLM 80 laser distance and angle measurer. In experiments involving vehicles, we use GPS readings as ground truth.

3.3 Basic Ranging Accuracy Calibration

We start with an open space outdoor area, in which the surrounding environment is stationary. The multipath problem is minimized in this setup, in which only the ground bounce affects the measurement of the direct path. In such setup, we study two environments: 1. open green field 2. open rocks paved field.

Surprisingly, for the WiFi card A setup, Fig.3(a), and Fig.5(c) show that the system underestimates distance and returns negative round-trip-time estimations for short distances. Multipath effects can lead to longer paths but we are not aware of any effects that would allow the signal to arrive earlier than expected. We believe that this is due to internal calibration of the WiFi cards or multipath compensation algorithms that process the measurements in firmware before they are delivered to the driver. Our open-space stationary measurements at different distances, shown in Fig. 5(c), as an example, illustrate that in an open space stationary environment the mean error is constant over distance but variance increases at longer distances. The mean fixed offset is 5.7 m, which we confirmed by measuring the offset with multiple different pairs of cards.

AP label	20 MHz (2.4 GHz)	40 MHz (2.4 GHz)	20 MHz (5 GHz)	40 MHz (5 GHz)	80 MHz (5 GHz)
WiFi card A	-6.8 m	-6.8 m	Not available	Not available	Not available
AP B	Not accurate (-1000 m)	Not accurate (-998 m)	-15 m	-5 m	1.8 m

Table 1: Comparing the average ranging accuracy for using different WiFi chipsets as the AP, while fixing the STA using WiFi card A, under different bandwidth and band configurations. The average ranging accuracy is reported in meters for 1 meter actual distance.

(a) Grass ground (0.7 m height).   (b) Rocks ground (1.4 m height, offset corrected.)   (c) Maximum range (1.4 m height, offset corrected.)
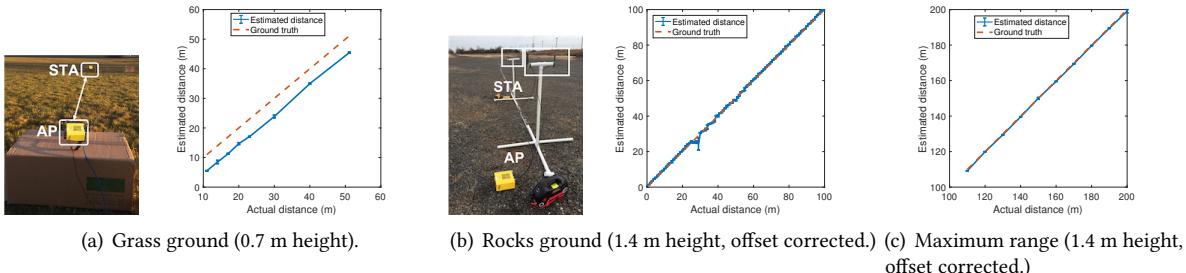
Figure 3: Outdoor open space. This setup uses the WiFi card A for both STA and AP sides.
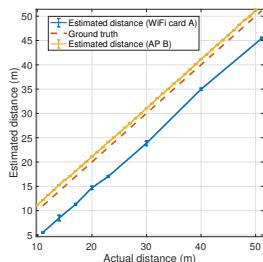

Figure 4: Outdoor open space grass ground (0.7 m height). Comparing ranging results for using WiFi card A as AP compared to AP B while using WiFi card A as STA in both scenarios.

On the other hand, ranging to AP B using WiFi card A, as in Fig.4 in open space, does not show underestimation of the distances compared to ranging to WiFi card A. In this new setup, STA and AP have different chipsets (belonging to different vendors), while using 80 MHz bandwidth at 5 GHz band.
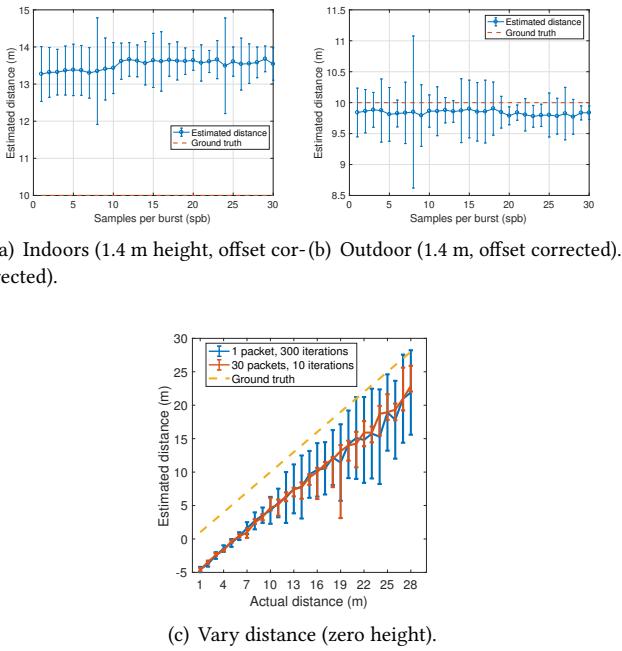
Offset correction. Filtering the fixed offset can be done by either subtracting that measured offset from the readings or by cancelling this offset through the delay of long enough cables. In this paper, we correct for the subtracted offset using 6 feet cables connecting the WiFi card to the two needed antennas. We use 6 feet cables, as it adds 1.83 meters on both sides resulting into 4.4 meters added delay after taking into account the speed of the signal in the used cables. This also enables us to put the antennas on reasonable height (1.4 m) and helps separate the antennas from the noise produced

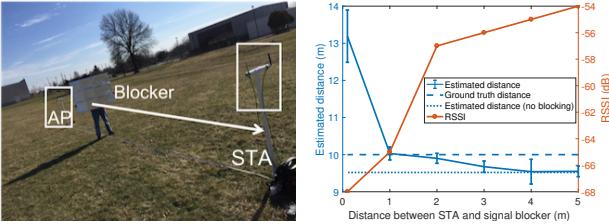by the metal box containing our form factor small personal computer.

After correcting the fixed offset, Fig.3(b) show that in these kind of open space environment, the ranging system works accurately (within 1 meter error). However, it sometimes underestimates the actual distance, even after correcting for the offset, as shown in Fig. 3(b) (between 27 m and 37 m). Therefore, we shifted both the STA and AP, while preserving the same separation distance, in order to confirm that this problem is because of the environment. After shifting the STA and AP, we observed that the estimated distance returns to the normal behaviour in such open space setup. We also tested the maximum range of this ranging system in open space environment, while putting the AP and the STA on 1.4 m height. Fig.3(c) shows that this ranging system can still estimate distances up to 200 m. We did not test the ranging system for distances more than 200 m.

Bandwidth effect. Generally, increasing the signal bandwidth is expected to improve the accuracy of time-of-flight ranging systems, especially in a multipath environment, but it is unclear whether the data communication bandwidth setting affects this process. For these WiFi cards A, it is only permitted by the firmware to work as AP in 2.4 GHz band, while only passive reception is permitted in 5 GHz band. Therefore, only 20 and 40 MHz channel bandwidth settings were available to us. We experimented with both bandwidth settings and did not observe any effect on ranging accuracy.

On the other hand, AP B, that we use, supports FTM with 80 MHz bandwidth at the 5 GHz band. The results at this higher bandwidth (higher ADC sampling rate) show a significant improvement (in Fig. 4 and Fig. 10(a)), although the

(a) Indoors (1.4 m height, offset cor- (b) Outdoor (1.4 m, offset corrected).
rected).

(c) Vary distance (zero height).

Figure 5: Effect of varying number of samples per burst.

Figure 6: Blocking LoS reception (1.4 m height, offset corrected).

different band and different chipset could have also been a factor. A more detailed comparison is presented in Table 1. Note that in the AP B configuration with 2.4GHz, the returned ranging estimates are very unreliable which could be due to compatibility or calibration issues since the FTM feature in the open source driver used for the client is not officially supported by the chipset vendor.

4 EXPERIMENTAL FRAMEWORK

In this section, we characterize the performance of the FTM ranging system through our experimental framework. We study the effect of different software and environmental parameters that affect the performance of such system. Our experimental framework consists of several experiments, indoors and outdoors to quantify the accuracy of the ranging
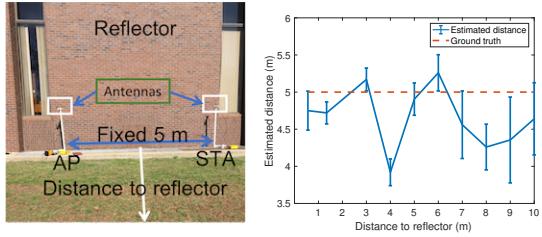
system, and most importantly, the repeatability of these results. Therefore, we start with outdoor open space stationary environments, in which we aim to understand the basic accuracy in an ideal simplified environment (single reflection by the ground). In outdoor open-space setups, we have control on the multipath problem. For example, we can control the length of the ground bounce by changing the antenna height. We can either add second bounce or block the direct path by adding reflector parallel or perpendicular to the direct path, respectively. As these ideal environments are not common, we move after that to evaluate common and more challenging situations. For example, outdoor dynamic environments with vehicles moving and causing different kinds of reflections to the transmitted signal. Indoor setups are another example for such common environments in which the multipath problem is complicated by reflections from walls, load bearing columns, doors, and furniture.
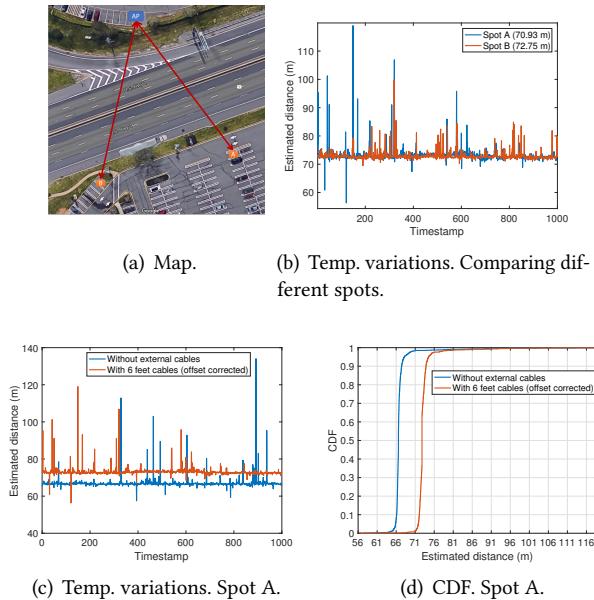
4.1 Sampling Effect

Samples per burst (spb). First, we study the effect of varying the number of FTM packets per burst, i.e. burst size, on the performance of the system. Fig. 5(a), and Fig. 5(b) show the effect of varying number of samples per burst over the estimated distance, while fixing the distance to 10 m indoors and outdoors. As the number of samples increases, the variance of the measurements decreases. Fig. 5(c) shows the estimated distance while varying the actual distance between the transmitter (AP) and the receiver (STA) while fixing their heights (on the ground, 0 m), in open space environment. In this ranging procedure, we change the burst size (1, and 30), while repeatedly calling the command multiple times (300, and 10). In the rest of the paper, we stick with the highest burst size (30) that minimizes the measurement noise.

4.2 Multipath Effect

Outdoor, blocking direct path. Even with high clock resolution and high bandwidth, ranging systems suffer from overestimating the distance while blocking the LoS reception. While this situation can practically happen, we move on to study the effect of blocking the LoS reception on the estimated distance in the same open space environment. In this setup, we use a 1.2 m × 0.9 m sheet covered with aluminum foil to block the signal between the AP and the STA. We move the blocking sheet along the line connecting the STA and the AP. Fig. 6 presents the effect of blocking the signal on the estimated distance along with the received signal. As the blocking sheet moves towards the STA, the estimated distance increases. The reason behind this is due to the partial blocking of the LoS. Since the 1.2 m × 0.9 m aluminum sheet cannot block the whole propagation channel in the open space, placing the blocker closer to the transmitter/receiver

Figure 7: Outdoor parallel to 7-floor building (1.4 m height, offset corrected).

(a) Map.

(b) Temp. variations. Comparing different spots.

(c) Temp. variations. Spot A.

(d) CDF. Spot A.

Figure 8: Mobile environment effect for static sender and receiver.

would essentially result in longer multipath propagation, which leads to longer distance estimation.

Outdoor, two reflectors. We start to add another reflector to the ground reflector in outdoor environment and study how the system reacts to simple multipath problem. In this setup, we fix the distance between the AP and the STA to 5 m, while aligning the line connecting the two nodes to be parallel to a side of 7-floor building. This side is 22 m long. Fig. 7 shows that the ranging system over the same separating distance swings between underestimating and overestimating the distance while varying the distance to the major reflector.
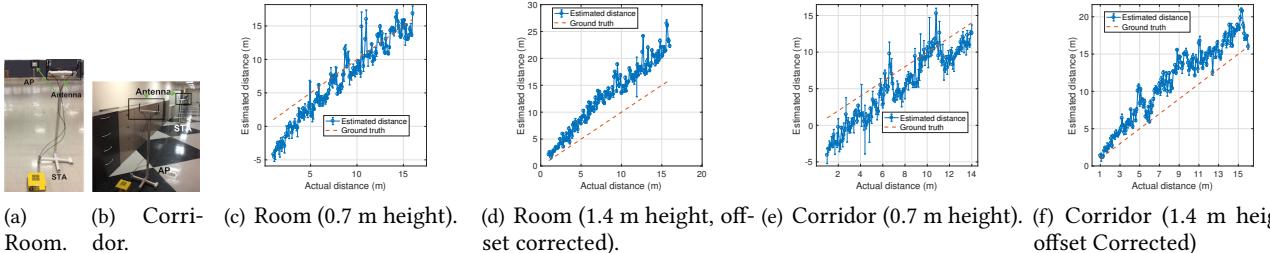
Outdoor, highway, mobile environment. In this setup, we study how a highly dynamic environment could affect the estimated distance between static transmitter and receiver. We fix the AP location, and use two different spots for the STA (Fig. 8(a)). We notice a medium traffic on the highway during the experiment. We use 30 packets per burst and

repeat the procedure 1000 times, lasting for 6 minutes. The ground truth distances between the AP and the STA are 72.5 m, and 72.3 m, and the median estimated distances are 72.79 m (66.56 m before correction), and 72.61 m, respectively for spot A and B. The median estimated distance converges over time to the actual distance, as more samples being measured while the LoS propagation is not blocked. Moreover, this ranging system underestimates the actual distance even after correcting for the fixed offset by using 6-feet cables. On the other hand, the spikes occur when big trucks pass by and block the direct LoS propagation between the AP and the STA.

Indoor. Indoor environments are challenging for ranging systems because of the multipath problem. Few steps could produce high variant measurements, even for time-based ranging systems. In order to capture this behaviour, we conduct two indoor experiments, in which we fix the AP and the STA on the same height (0.76 m), and move the STA with a step of 10 cm (less than a wavelength of 2.4 GHz frequency). We use 30 samples per burst, while repeating this FTM measurements 10 times. These two experiments are conducted in the same single-floor building, with the ceiling height 5.3 m. Fig. 9(c) shows the relation between the actual and estimated distance, while varying the distance in a large experimentation room (24.2 m × 19.4 m). We repeat the same experiment in a long corridor (30.7 m × 2.5 m), as shown in Fig. 9(e). These experiments show that even for 10 cm step, the measurements could vary up to 5 meters in these settings. These results highlight how the multipath problem could affect such ranging systems, specially indoors. This is clearly emphasized in Fig. 10(b), in which we vary the distance from 10 to 10.5 m with 1 cm step. We can see that by varying with only 1 cm, the signal gets completely blocked at 10.06 m. Therefore, the user should not expect getting the same output while moving small steps, even 1 cm matters significantly.
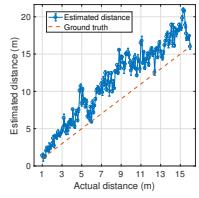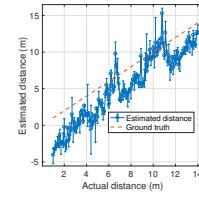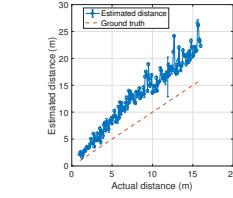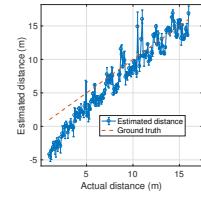
Even in this more challenging indoor environment (Fig. 10(a)), ranging with AP B with the higher 80 MHz bandwidth at 5GHz show meter-level accuracy, while confirming no underestimation of the distance compared to ranging with WiFi card A.

Indoor AP, outdoor STA. Indoor access points are frequently used by stations (e.g., smartphones) outdoors for positioning. To evaluate such a scenario, we start with fixing the AP location in an office inside single floor building (the office has window facing the road) while moving the STA outdoor. We test two setups: 1. moving the STA parallel to the road, 2. moving the STA across the road. Fig. 11(b) shows the estimated distance after correcting the offset using 6 feet cables. In such a common setup, the ranging system can estimate the distance while still being affected by multipath issues showing up to 3 m variations in the estimated distance
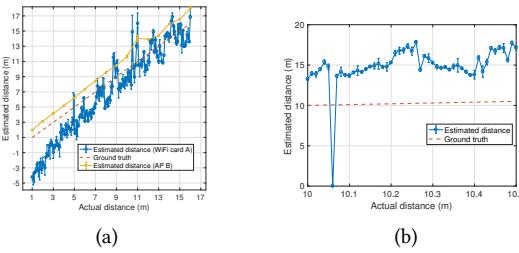
| (a) Room. | (b) Corridor. | (c) Room (0.7 m height). | (d) Room (1.4 m height, offset corrected). | (e) Corridor (0.7 m height). | (f) Corridor (1.4 m height, offset Corrected) |

Figure 9: Indoor scenarios. This setup uses WiFi card A for both STA and AP sides.

(a)

(b)

Figure 10: (a) Indoor scenario (room (0.7 m height)) for comparing ranging results for using WiFi card A as AP compared to AP B while using WiFi card A as STA in both scenarios. (b) 1 cm step in indoor room (1.4 m height, offset corrected). Zero distance represents no signal.

for 1 m step. This is shown in Fig. 11(c), as the STA moves between the cars, the signal is affected heavily by multipath, and eventually encounter a total signal blockage while the STA is 28 m, and 36 m from the AP.

For indoor AP B and an outdoor WiFi card A station (Fig. 12), the signal is weaker than with WiFi card A as AP, likely due to the higher bandwidth and carrier frequency and hence distances above 20m, the distance estimates become unreliable. According to these results, it seems that the underestimation is an undesirable result of the algorithms in the proprietary firmware.

In the next setup, we change the environment of the AP from the single-floor building to a 7-floor building while keeping the STA in nearby locations. In specific, we fix the AP in the third floor of the building near the window, with locations of the STA varying from the ground floor inside the building (right below the AP) to the outdoor field around the building. Among these setups, we also vary the orientations of antennas between vertical (antennas of each node pointing up) and horizontal (antennas pointing horizontally to the same direction). Fig. 11(d) shows how the orientations of the antennas can affect the estimated distance. For example, the deployment of AP and STA in different floors requires the antennas to be horizontally oriented, so that signals can

propagate vertically between the floors. The bars in blue and yellow showed in Fig. 11(d) indicates the effect of antenna orientation on distance estimation.
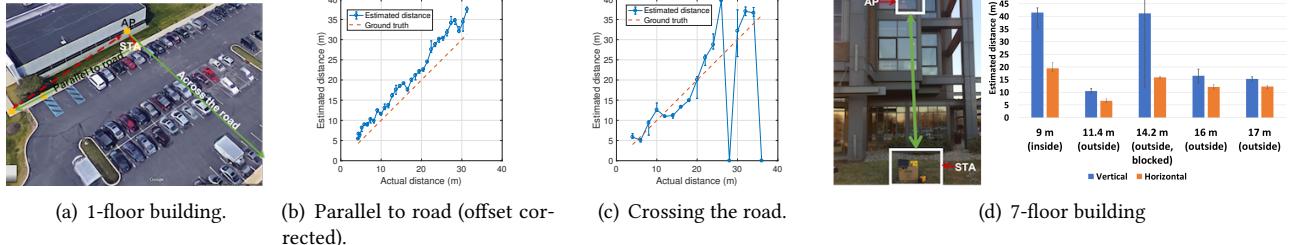
5 CORRECTING RANGING ERRORS

Based on our findings, we discuss in this section how to correct the ranging error using standard localization error correction techniques.
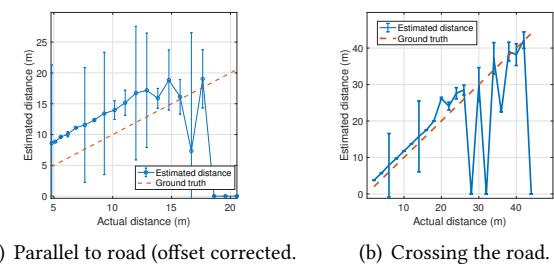
5.1 Temporal Filtering

In standard ranging systems, simply averaging multiple measurements of the same location could help to filter out hardware/software noises, but cannot eliminate the multipath effect which leads to distance overestimation. For example, previous work [21] has shown that using 50-percentile as an estimator leads to overestimating the distance. Thus, percentile bellow 50% is suggested. However, for this FTM ranging system deployed in environments showed in Fig. 6 and Fig. 7, we observe both underestimation and overestimation of the distances for the same location. Moreover, the overestimated distances presents significantly higher errors compared to underestimated counterpart. (Fig. 8).

In dynamic environments, such as highways as we shown in Fig. 8, moving objects could temporary block the direct path of the transmitted signals or add more reflectors that results in higher the ranging errors. Here we illustrate how standard temporal filtering techniques could improve the results for this setup.

We take a window of 10 bursts which each being 30 packets long, and analyze the data over this window. We estimate the most probable distance by building histogram for each window. It is worth mentioning that the most probable estimation is affected by the duration of the object/vehicle's affecting the ranging the system. Another approach[29] is to use clustering, assuming that the direct path results in closest estimations of the ground truth compared to the overestimated/underestimated data resulted from multipath. We sort the clusters centers and estimate the average of lowest half of the centers, while rejecting the lowest center. The clustering technique has median error of 0.2 m and 0.6 90-percentile

(a) 1-floor building.

(b) Parallel to road (offset corrected).

(c) Crossing the road.

(d) 7-floor building

Figure 11: Indoor AP outdoor STA. Both AP and STA use WiFi card A. Zero distance represents no signal

(a) Parallel to road (offset corrected.

(b) Crossing the road.

Figure 12: Indoor AP (AP B), outdoor STA (WiFi card A). Zero distance represents no signal.

compared to median error of 0.7 m and 2.2 m for the averaging technique. The most probable estimation has 0.3 m median error and 0.78 90-percentile while the minimum estimator has 0.4 m median error and 1 m 90-percentile.

5.2 Spatial Filtering

Given a fixed AP, we can leverage the mobility of a STA to collect multiple measurements over different locations. The estimated distances for these multiple locations may vary significantly as we have shown before because of multipath. These outliers can be filtered by validating the estimated distances using basic laws of geometry.

Known STA Displacement. As a STA moves from one location to another, the ranging algorithm estimates the distances from these two points to the AP. Because of multipath, synchronization, and bandwidth issues, these distances could be overestimated or underestimated. To filter out inconsistent estimations with the displacements, extra constraints need to be applied to them. The displacement of the STA can be estimated indoor using smart phones' inertial sensors [28] and outdoor using on board vehicle sensors [14].

Following this idea, as the station moves with a distance d_s, then there is a limit on the new estimated distance compared to the previously estimated distance. We formulate this limit in the following inequality:
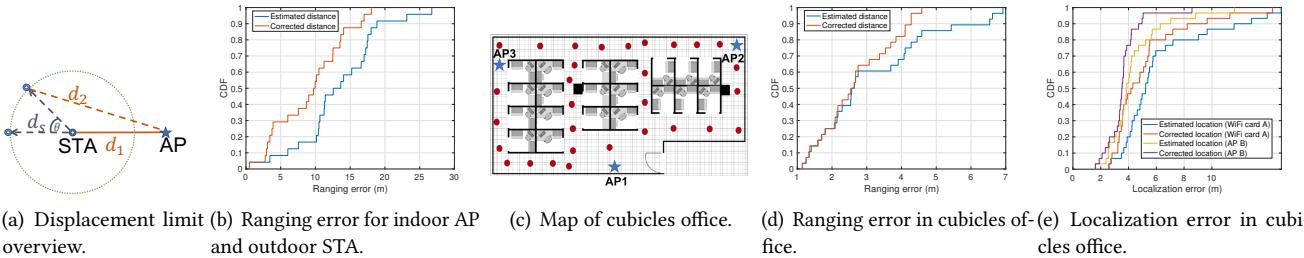
$$|d_1 - d_s| \le d_2 \le d_1 + d_s \tag{1}$$

Fig. 13(a) illustrates this displacement inequality, in which, whenever the STA moves with an angle $\theta > 0$, then $d_2 < d_1 + d_s$. This limit can be proved using the triangular inequality [29]. Equality holds in this inequality when the STA moves on the line towards the AP or backwards away from the AP. Using this method, we filter and correct the estimated distances that violates the displacement inequality: If $d_2 > d_1 + d_s$, we assign $d_2 = d_1 + d_s$; if $d_2 < |d_1 - d_s|$, we assign $d_2 = d_1 - d_s$. These assignments are based on the assumption that the direction of STA is not known.

5.3 Evaluation

Evaluating the correction technique with different movement patterns is important. Therefore, we focus on the evaluation dataset on having common setups with different movement patterns, not only moving in the same direction along a straight line. We start with indoor scenario, in which we conduct an experiment in a cubicles office (10 m x 20 m with height 2.7 m). In this indoor setup, we fix the AP in the middle of the area and move the STA trying to cover the whole area. Fig. 13(d) compares the CDF of the error of the estimated distance to the corrected distance. The corrected distance achieves 2.5 m median error, and 4.78 m 90-percentile, compared to 2.6 m median error, and 6.5 m 90-percentile for the estimated distance without correction. For the second setup, we fix the AP indoors, in the third floor of a seven floors building (near the window facing the parking lot), and we put the STA on the roof of a moving car. The car traverses the whole parking lot while logging the ranging readings along with GPS readings as ground truth location. Fig. 13(b) presents the CDF for the error of the estimated distance and the corrected distance using the displacement inequality. The corrected distance achieves 9.8 m median error, and 16.5 m 90-percentile compared to 13.1 m median error, and 18.8 m 90-percentile for the estimated distance without correction.

Localization error. Beside the ranging performance, we evaluate the localization accuracy indoors. Using at least three APs, a STA is able to estimate its location by trilateration using the locations of these APs, and the estimated ranges to them. We use the standard iterative nonlinear least

(a) Displacement limit overview.
(b) Ranging error for indoor AP and outdoor STA.
(c) Map of cubicles office.
(d) Ranging error in cubicles office.
(e) Localization error in cubicles office.

Figure 13: Illustration for the displacement limit and its effect of on the ranging and localization error along with a map for the indoor testbed. Red dots represents STA locations.

squares trilateration algorithm [13, 25]. We fix three APs in the cubicles office (the same area used for evaluating the ranging accuracy), trying to cover the whole area with APs. In this cubicles area, there are two load bearing columns (0.8 m x 0.7 m wide), which are able to block the signal. We compare the localization error between using WiFi card A or AP B as APs, while using the WiFi card A station. Fig. 13(e) shows that the ranging system, using WiFi card A APs, is able to localize a STA with 5.2 m median error and 11.6 m 90-percentile, while achieving 3.8 m median error and 6.2 m 90-percentile for using APs B. On the other hand, after correcting the ranging estimations for each AP, and using these ranging estimations for locating the STA, the localization error improves to 4.2 m median error and 8.2 m 90-percentile for WiFi card A setup, and to 3.5 m median error and 4.7 m 90-percentile for AP B setup.

6 RELATED WORK

Evaluating multipath. Work in [23] evaluate indoor LoS scenarios, verifying the directional and polarization characteristics estimated by the the RiMax algorithm [22], subtracting the Specular Multipath Component from the observed power spectrum. In [20], they quantitatively analyze the effect of angle of inclination between the STA and AP in tracking using RADAR. Markov modelling of spatial variations seen in multipath is done in [10], and is verified by taking measurements at 60GHz in a reverberation chamber. Another line of work [12] take a geometry based approach to simulate the multipath using a nonlinear multipath filter.

Evaluation of time-based ranging systems. RADAR systems were evaluated by Derham et al. in [24], calculating the FFT of various received signals to determine the characteristics of coherent RADAR ranging signals in real conditions. GPS has been evaluated by the Naval Air Development Center in [18], where they create a setup to test every possible noise-contributing factor independent of the other.

Localization correction techniques. Tonetrack [29] implements a frequency combining algorithm (to increase the

bandwidth) on the WARP hardware radio platform to track WiFi-based devices indoors. In this system, they propose a triangular inequality and clustering-based outlier detection to filter the NLoS APs. Chronos [27] proposes an indoor tracking algorithm that stitches the transmitted information over multiple bands, while leveraging a single MIMO AP. Work in [21] presents a firmware-customized time-based indoors ranging system running with a filter based on statistical learning to filter out multipath measurements.

This related work either leverage specialized hardware, or customized firmware to support nanosecond ranging time measurements. In this paper, we evaluate the FTM protocol that is already standardized in IEEE 802.11-2016 [5] and being commercialized in recent WiFi chipsets [1].

7 CONCLUSION

This paper presents a measurement study that evaluates a WiFi time-of-flight ranging system and verifies performance expectations. Moreover, it introduces the use and calibration of an open platform for WiFi time-of-flight ranging that future research can build on. We learned from our measurements that this ranging system is indeed capable of accurate meter-level ranging in open-space outdoor environments once calibrated. In indoor lab and office environments with multipath, both ranging and positioning (trilateration) errors increase to about 5m unless the deployment is dense enough to operate at higher bandwidths (80MHz in our experiments). This occurs even in settings where LoS reception is not blocked. We also, unexpectedly, found cases where the ranging system significantly underestimates the distance. Overall, at low bandwidth, accuracy in rich multipath environments does not seem higher than demonstrated by other positioning systems but the technology promises to deliver this accuracy with relatively few access points and less site survey overhead. With a dense deployment of access points so that multiple access points can be reached by high bandwidth signals, accuracy improves.

REFERENCES

[1] https://goo.gl/BSUCdG. Wi-Fi CERTIFIED Location.

[2] https://goo.gl/1z1LhE. Android P Indoor Positioning.

[3] https://goo.gl/hQUyfo. Linux Core Releases.

[4] https://goo.gl/TzJRGG. FTM Patch for iw.

[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 802.11-2016 (Revision of IEEE Std 802.11-2012)"*, pages 1–3534, Dec 2016.

[6] Leor Banin, Uri Schatzberg, and Yuval Amizur. Wifi ftm and map information fusion for accurate positioning. In *2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2016.

[7] M Ciurana, F Barcelo-Arroyo, and F Izquierdo. A ranging system with ieee 802.11 data frames. In *Radio and Wireless Symposium, 2007 IEEE*, pages 133–136. IEEE, 2007.

[8] Domenico Giustiniano and Stefan Mangold. Caesar: carrier sense-based ranging in off-the-shelf 802.11 wireless lan. In *Proceedings of the Seventh COnference on emerging Networking EXperiments and Technologies*, page 10. ACM, 2011.

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

[10] Marcia Golmohamadi, Sakil Chowdhury, and Jeff Frolik. Markov modeling of spatial variations in multipath. In *Antennas and Propagation & USNC/URSI National Radio Science Meeting, 2017 IEEE International Symposium on*, pages 611–612. IEEE, 2017.

[11] André Günther and Christian Hoene. Measuring round trip times to determine the distance between wlan nodes. In *International Conference on Research in Networking*, pages 768–779. Springer, 2005.

[12] Donald E Gustafson, John R Dowdle, John M Elwell, and Karl W Flueckiger. A nonlinear code tracking filter for gps-based navigation. *IEEE Journal of Selected Topics in Signal Processing*, 3(4):627–638, 2009.

[13] Fernán Izquierdo, Marc Ciurana, Francisco Barceló, Josep Paradells, and Enrico Zola. Performance evaluation of a toa-based trilateration method to locate terminals in wlan. In *Wireless Pervasive Computing, 2006 1st International Symposium on*, pages 1–6. IEEE, 2006.

[14] Yurong Jiang, Hang Qiu, Matthew McCartney, Gaurav Sukhatme, Marco Gruteser, Fan Bai, Donald Grimm, and Ramesh Govindan. Carloc: Precise positioning of automobiles. In *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, pages 253–265. ACM, 2015.

[15] Steven Lanzisera, David T Lin, and Kristofer SJ Pister. Rf time of flight ranging for wireless sensor network localization. In *Intelligent Solutions in Embedded Systems, 2006 International Workshop on*, pages 1–12. IEEE, 2006.

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

[17] Xinrong Li, K. Pahlavan, M. Latva-aho, and M. Ylianttila. Comparison of indoor geolocation methods in dsss and ofdm wireless lan systems. In *Vehicular Technology Conference Fall 2000. IEEE VTS Fall VTC2000. 52nd Vehicular Technology Conference (Cat. No.00CH37152)*, volume 6, pages 3015–3020 vol.6, 2000.

[18] Marvin May, Eric Kreisher, Tonino Nasuti, and Carla Sives. Evaluation of gps receiver ranging accuracy. In *Position Location and Navigation Symposium, 1990. Record. The 1990's-A Decade of Excellence in the Navigation Sciences. IEEE PLANS'90., IEEE*, pages 314–321. IEEE, 1990.

[19] Dennis D McCrady, Lawrence Doyle, Howard Forstrom, Timothy Dempsey, and Marc Martorana. Mobile ranging using low-accuracy clocks. *IEEE Transactions on Microwave Theory and Techniques*, 48(6):951–958, 2000.

[20] AV Mrstik and PG Smith. Multipath limitations on low-angle radar tracking. *IEEE transactions on aerospace and electronic systems*, (1):85–102, 1978.

[21] M. Rea, A. Fakhreddine, D. Giustiniano, and V. Lenders. Filtering noisy 802.11 time-of-flight ranging measurements from commoditized wifi radios. *IEEE/ACM Transactions on Networking*, 25(4):2514–2527, Aug 2017.

[22] Andreas Richter. Estimation of radio channel parameters: Models and algorithms. ISLE, 2005.

[23] Kentaro Saito, Jun-Ichi Takada, and Minseok Kim. Characteristics evaluation of dense multipath component in 11ghz-band indoor environment. In *Antennas and Propagation (EuCAP), 2016 10th European Conference on*, pages 1–3. IEEE, 2016.

[24] James A Scheer. Coherent radar system performance estimation. In *Radar Conference, 1990., Record of the IEEE 1990 International*, pages 125–128. IEEE, 1990.

[25] R. Schmidt. Least squares range difference location. *IEEE Transactions on Aerospace and Electronic Systems*, 32(1):234–242, Jan 1996.

[26] Ralph Schmidt. Multiple emitter location and signal parameter estimation. *IEEE transactions on antennas and propagation*, 34(3):276–280, 1986.

[27] Deepak Vasisht, Swarun Kumar, and Dina Katabi. Decimeter-level localization with a single wifi access point. In *NSDI*, volume 16, pages 165–178, 2016.

[28] He Wang, Souvik Sen, Alexander Mariakakis, Romit Roy Choudhury, Ahmed Elgohary, Moustafa Farid, and Moustafa Youssef. Unsupervised indoor localization. In *Proceedings of the 10th international conference on Mobile systems, applications, and services*, pages 499–500. ACM, 2012.

[29] Jie Xiong, Karthikeyan Sundaresan, and Kyle Jamieson. Tonetrack: Leveraging frequency-agile radios for time-based indoor wireless localization. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, MobiCom '15, pages 537–549, New York, NY, USA, 2015. ACM.