Benchmarking and Security Considerations of Wi-Fi FTM for Ranging in IoT Devices

Govind Singh*, Anshul Pandey*, Monika Prakash*, Martin Andreoni*, and Michael Baddeley*

*Technology Innovation Institute, UAE

{govind.singh; anshul.pandey; monika.prakash; martin.andreoni; michael.baddeley}@tii.ae

Abstract

The IEEE 802.11mc standard introduces fine time measurement (Wi-Fi FTM), allowing high-precision synchronization between peers and round-trip time calculation (Wi-Fi RTT) for location estimation – typically with a precision of one to two meters. This has considerable advantages over received signal strength (RSS)-based trilateration, which is prone to errors due to multipath reflections. We examine different commercial radios which support Wi-Fi RTT and benchmark Wi-Fi FTM ranging over different spectrums and bandwidths. Importantly, we find that while Wi-Fi FTM supports localization accuracy to within one to two meters in ideal conditions during outdoor line-of-sight experiments, for indoor environments at short ranges similar accuracy was only achievable on chipsets supporting Wi-Fi FTM on wider (VHT80) channel bandwidths rather than narrower (HT20) channel bandwidths. Finally, we explore the security implications of Wi-Fi FTM and use an on-air sniffer to demonstrate that FTM messages are unprotected. We consequently propose a threat model with possible mitigations and directions for further research.

Keywords

Wi-Fi, IEEE 802.11mc, Ranging, Localization

1   Introduction

The fine time measurement (Wi-Fi FTM) and round-trip-time Wi-Fi RTT features of the IEEE 802.11mc amendment to the Wi-Fi standard allow supporting devices to estimate the distance to other devices supporting Wi-Fi FTM ranging. This capability is supported in various modes (*Station (STA)*, *Access Point (AP)*, and *Neighborhood Aware Networking (NAN)*) and allows applications to benefit from accurate localization and context awareness in use-cases such as asset tracking, geofencing, industrial robotics, home automation control, and location-based information for service broadcasting.

Traditionally, distance ranging based on the Received Signal Strength Indicator (RSSI), which estimates the power of the received signal as measured through the hardware, is a simple and extensively adopted means for estimating distance – often employing a straightforward long-distance path loss model [1],

$$\text{RSSI} = -10 * n \log 10(d) + A \qquad (1)$$

where A is the RSSI at the reference distance and n is a path loss exponent. While this method is easy to employ, due to multipath issues the accuracy is frequently poor as the relationship between RSSI and distance is non-linear and is adversely affected by obstacles in non line-of-sight environments. In contrast, precise time measurement provided by Wi-Fi FTM, Wi-Fi RTT calculates the distance between two devices by measuring the time a packet takes to make a round trip (i.e., the time taken for an initiating device to receive an acknowledgment from a neighbor after transmitting a packet to that neighbor). The difference between the transmit and receive time stamps denotes the flight time which, when taking into account the speed of light, indicates how far away the Wi-Fi RTT initiator device is from the Wi-Fi RTT responder device. Importantly, RTT measurement errors are linear with distance, not exponential like RSSI, allowing sub-meter accuracy. However, precise time-stamping of packets supported by Wi-Fi FTM is highly dependent on the hardware capabilities, such as the clock resolution. Additionally, path First Arrival Correction (FAC) and accurate time-stamping of the first packet symbol are also key contributors to Wi-Fi RTT accuracy. The aim of this work is to therefore evaluate the capabilities of different commercial off-the-shelf (COTS) hardware platforms supporting the Wi-Fi FTM protocol and comparing the ranging accuracy across different bandwidth configurations.

Our contributions. In this paper we identify a number of commercially available Wi-Fi chipsets which support Wi-Fi FTM ranging and benchmark the accuracy in both outdoor and indoor experimental setups.

Outline of this paper. In Section 2 we provide necessary preliminaries on the operation of Wi-Fi RTT and Wi-Fi FTM. In Section 3 we provide details of our experimental setup and perform benchmarking of three commercially available Wi-Fi FTM chipsets. We explore related localization technologies in Section 5 before concluding in Section 6.

Table 1: Parameters affecting Wi-Fi FTM ranging performance.

FTM parameters	Description
Frequency band	6GHz/5GHz has better accuracy in comparison to 2.4GHz due to available bandwidth.
Channel bandwidth	Ranging error roughly halves with double bandwidth, when comparing the 20/40/80/160 MHz frequency bands.
Antenna diversity	Multiple antennas reduce ranging error due to better diversity. 2x2 configuration has approx 30 percent better accuracy.
Multipath	Line-of-sight path is preferred for the best accuracy.
Tx power	Higher transmission power allows for minimizing the errors when used within the regulatory limit.
Timestamping	Hardware time stamping clock resolution and lower ppm errors allow better accuracy.

2   Ranging with Wi-Fi FTM

Wi-Fi FTM was introduced in the IEEE 802.11-2016 standard revision for the purpose of allowing a fine timing measurement (FTM) frame to calculate round-trip time (RTT) between two peers. Specifically, Wi-Fi RTT makes use of IEEE 802.11 frame exchange based on acknowledgment frames (as per Figure 1a) as well as FTM bursts (as per Figure 1b), which further allows delivering many FTM messages consecutively while lowering timing computation error by averaging multiple timestamps.

In both instances, an FTM request frame (FTMR) is provided by the FTM *initiator* to start the process, while the FTM responder has the option of accepting it or rejecting the FTMR. Upon acceptance, the *responder* sends an acknowledge (ACK) frame. The *responder* then sends a single FTM frame, recording the current time t_1 within the frame, to start the beginning of the round-trip measurement. As soon as the preamble is detected by the initiator, it starts recording time at time t_2. The FTM initiator then creates its own ACK frame and transmits it to the responder. The ACK frame is transmitted at the initiator, which accounts for the hardware signal processing delay of the initiator's digital baseband and radio front end. Furthermore, the responder can determine the overall round-trip time of the signal, as per Equation 2, by deducting t_1 from t_4 when it receives the initiator's ACK frame at time t_4 and adding this to the delta between t_3 and t_2.

$$\text{RTT} = (t4 - t1 + t2 - t3) \qquad (2)$$

The time a WiFi signal takes to travel over the air between the RTT initiator peer and the RTT responder peer is proportional to the actual distance between them (approximately 3.3 nanoseconds per meter). Accordingly, the distance between the peers can be estimated using Equation 3.

$$d = \text{RTT}/2 * c = (t4 - t1 + t2 - t3)/2 * c \qquad (3)$$

However, in some circumstances (e.g., due to environmental factors such as temperature [2]) the internal clock between the initiator peer with the responder peer may not be synchronized, hence direct subtraction can not be done with two timestamps to calculate RTT. The difference in timestamps when the signal travels in the reverse direction is affected in the opposite way by the clock offset between peers. As a result, the round trip time (RTT) can be obtained without having to know the clock offsets, by simple addition and subtraction of four timestamps (as per Equation 3).

Fundamentally, however, localization accuracy depends not only on the accuracy of the timestamp but also on numerous other factors. The bandwidth, antenna diversity, the

(a) Single mode RTT protocol.

(b) Burst mode RTT protocol.

Figure 1: Wi-Fi FTM protocol in *single* and *burst* modes.

transmit power of the broadcasting device, and the reception sensitivity of the receiving device are also key factors of a Wi-Fi radio that define the accuracy of its individual measurements in an RF ranging system.

Bandwidth. In a wireless system, preamble detection is used to determine the beginning of a frame. Hardware timestamping systems based on preamble detection present a resolution bound equal to the baseband sampling period, on which the FTM protocol depends. Indeed, a detection delay of as little as 1 ns could result in an error of 30 cm (3). Hence, high resolution of the time-stamping clock is required as FTM requires pico second clock resolution for time-stamping. As the sampling period is inverse of the bandwidth (either 20MHz, 40MHz, or 80MHz), better resolution can be achieved at higher bandwidths (as per the Nyquist rate $f_s = 2B$, where f_s is the sampling frequency and B is the bandwidth in MHz).

Antenna diversity. Having multiple antennas helps to extract the spatial diversity (transmitting multiple copies of the same information via multiple antennas) which provides more resilient transmissions, and also helps to save the system from undergoing deep fade events.

Multipath. Furthermore, the channel frequency response of

Table 2: Experimental Setup Configurations.

Configuration	Initiator	Responder	Specification	Channel	Bursts	FTM Ranging
Config. 1	Google Pixel 4a (WCN3990)	Google Wi-Fi Mesh AP (QCA4019)	VHT80	5745MHz	8	Native
Config. 2	FeatherS2 NEO (ESP32-S2)	FeatherS2 NEO (ESP32-S2)	HT20	2412MHz	2	Native
Config. 3	Google Pixel 4a (WCN3990)	Google Pixel 4a (WCN3990)	HT20	2412MHz	8	Wi-Fi Aware

the associated channel varies owing to the multipath propagation. Specifically, multiple copies of the same signal with different amplitudes and phases arrive at the receiver due to the interaction of the signal with the surrounding objects. Also, due to the multipath propagation, the antenna receives several copies of the transmitted signals that have been subjected to various delays and attenuation. In the frame detector, these reflections can cause a sizable amount of jitter, especially in non-line-of-sight circumstances. FTM accuracy relies on the first arrival correction algorithm due to the multipath behavior, which is generally implemented in the lower MAC of the firmware component.

Timestamping. The coherence time, which specifies the period of time during which the channel is thought to be invariant, describes the dynamic of the channel. This channel variation may cause inaccuracy in the estimation of the channel delay due to the non-stationary state and, as a result, it will affect the FTM accuracy. With mobility, the accuracy can further suffer as the involved nodes' mobility may incur more estimation errors. Finally, with chipsets such as the WCN3990 in the Google Pixel 4a including Wi-Fi FTM ranging functionality as part of the Wi-Fi Aware specification, there has been little study on Wi-Fi FTM performance when being used as part of a wider standard rather than a 'native' approach where the FTM functions are accessed directly.

3 Experimental Analysis

To date, there are few examples of commercial Wi-Fi chipsets which support Wi-Fi FTM. In Table 2 we identify three compliant chipsets and indicate the supported channel bandwidth specification, the channel frequency used in experiments, the number of Wi-Fi FTM bursts supported, and whether Wi-Fi FTM ranging is directly accessible in the firmware or is included as part of Wi-Fi Aware.

Specifically, we consider the WCN3990 on a Google Pixel 4a, the QCA4019 on a Google Wi-Fi Mesh AP, and the ESP32-S2 on the FeatherS2 NEO and benchmark these devices in both an *indoor* (short range) and *outdoor* (longer range) experimental setup (Figure 2). Both setups consider a line-of-sight (LOS) scenario with only two devices, an *initiator* device, and a *responder* device. As per Figure 2c, in the indoor experimental setup the devices were placed on the ground and separated at distances of 0.5, 1.0, and 1.5 meters, while in the outdoor experimental setup, the devices were placed on tripods in an open area and separated at 3.0, 5.0, and 10.0 meters.

Only the ESP32-S2 and WCN3990 support both *I* and *R* modes allowing us to use the same device for the initiator and responder; when using 'Native' Wi-Fi FTM ranging on the ESP32-S2 and using Wi-Fi Aware on the WCN3990. Unfortunately, in this configuration, these devices are limited to 2.4GHz and HT20 (20MHz channel bandwidth). However,

(a) Indoor setup.

(b) Outdoor setup.

(c) Distances between Wi-Fi FTM *initiator* and *responder*.

Figure 2: Experimental setup.

by employing a Google Wi-Fi Mesh AP (QCA4019) for the *responder* and the WCN3990 for the *initiator* (allowing one to use 'Native' mode rather than Wi-Fi Aware), it is possible to perform Wi-Fi FTM ranging at 5GHz on VHT80 (80MHz channel bandwidth). These configurations are summarized in Table 2, and all experimental results are presented in Figure 3.

Config 1 (VHT80 + 'native' ranging). The first configuration uses a Google Pixel 4a (WCN3990) as *initiator* STA and a Google Wi-Fi MESH AP (QCA4019) as *responder* the responder AP. The Wi-Fi baseband in both chipsets supports IEEE 802.11ac with VHT80, allowing testing of Wi-Fi FTM ranging over a wider (80MHz) channel bandwidth. From Figure 3 it can be seen that for both the indoor and outdoor setups the WCN3990 manages to estimate the distance to the responder with sub-meter accuracy at all distances, and a small standard deviation.

Config 2 (HT20 + 'native' ranging). The second configuration employs two FeatherS2 NEO (ESP32-S2) boards as both

(a) Estimated range and RSSI over time (indoors).

(b) Estimated range and RSSI over time (outdoors).

(c) Mean Wi-Fi FTM estimated range (indoors).

(d) Mean Wi-Fi FTM estimated range (outdoors).

Figure 3: Wi-Fi FTM ranging results for both indoor and outdoor experimental setups. Samples were taken every 380ms over a period of 25s. Using VHT80 allows accurate ranging even at short distances, while HT20 chipsets struggle at such close range.

initiator (STA) and *responder* (AP) devices. The `ESP32-S2` can be clocked at up to 240 MHz in 2.4 GHz HT40 mode, however Wi-Fi FTM ranging is only supported on HT20[1]. While examination of the results in Figure 3d shows that the `ESP32-S2` is fairly accurate in the outdoor scenarios at longer ranges, at short distances indoors (Figure 3c) it performs exceptionally poorly – with an error of ≈1m at a distance of 0.5m, and an error of 2-3m at a true distance of 1.0m and 1.5m. While the indoor environment suffers from external interference sources and multipath reflects, the `ESP32-S2` suffers from poor receiver sensitivity short distances[2]. It is therefore likely that the main factors which might be contributing to inaccuracy are lower bandwidth (i.e. HT20 mode), first arrival correction errors, and hardware timestamping delays in FTM packets.

Config 3 (HT20 + Wi-Fi Aware ranging). The final configuration considers Wi-Fi Aware-supported FTM ranging [3] using one NAN anchor master and one NAN slave device using two Google Pixel 4a devices (`WCN3980`). As with The `ESP32-S2`, the `WCN3980` is limited to HT20 mode as this is the only mode supported by Wi-Fi Aware for Wi-Fi FTM ranging in the Android framework. Equally, the `WCN3980` performs well in the outdoor scenario at longer distances (Figure 3d) with measurements accurate to within a meter. However, at shorter distances (Figure 3c) the ranging measurements become wholly inaccurate – deviating from the true distance with errors up to multiple meters. Again, while there is external interference and reflections in the indoor environment, the culprit for this poor accuracy is likely the lower receiver sensitivity due to the use of HT20 mode in this configuration.

4 Security Analysis

From a security perspective, Wi-Fi FTM can be useful for identifying and locating rogue devices that may be attempting to gain unauthorized access to a network. However, it also has the potential to be exploited by attackers to perform location tracking and other forms of surveillance on legitimate devices connected to the network. Specifically, Wi-Fi FTM protocol messaging is based on a request-response model, therefore relying on the integrity of the responding device.

By default, Wi-Fi FTM control frames are unprotected and no cryptography and authentication is applied on the top messaging protocol in unassociated ranging mode. Wi-Fi FTM can be used to **track the location** of devices on a network by measuring the time it takes for a signal to travel between a device and an access point. Attackers can exploit this to perform location tracking on a legitimate device. The FTM protocol is vulnerable to **replay attacks**, where an attacker can intercept and replay a valid FTM response to a requesting device in order to impersonate a legitimate device and gain access to the network. While Wi-Fi FTM can detect **rogue devices** on a network by measuring the timing of the signals they send and comparing them to the timing of signals from legitimate devices, attackers can also use this feature to bypass security measures. An attacker that can **impersonate a device** can use the FTM feature to get information about other devices in the network which can be used to perform further attacks.

To mitigate these risks, it is important to ensure that Wi-Fi FTM ranging is used in the associated mode using WPA3 or WPA2+PMF to improve FTM packet privacy protection. Moreover, a Packet Number (PN) check at LMAC firmware is expected to prevent replay attacks. At the ranging application layer, multi-factor authentication is expected to mitigate issues related to the elevation of privilege. For unassociated ranging MAC address randomization is expected to

---

[1]https://github.com/espressif/esp-idf/tree/master/examples/wifi/ftm
[2]https://tinyurl.com/yc2ca746

Table 3: Wi-Fi FTM threats and possible mitigations.

Threat	Mitigation
Location tracking	WPA3 or WPA2+PMF (802.11w)
Replay attacks	PN check (LMAC)
Rogue Device Detection	Associated ranging with rekeying
Elevation of privilege	Multifactor authentication

Figure 4: On-air Wi-Fi FTM ranging messages are unprotected and can be easily read by a nearby sniffer.

provide some basic security measures. Table 3 outlines the main Wi-Fi FTM vulnerabilities that we have identified in this paper, as well as possible mitigations.

5 Related Work

WiFi FTM protocol ranging is getting widely adopted for many use-cases related to ranging, indoor localization for industrial robots, and asset tracking use cases in the industrial IoT segment. To date, there are many examples of commercial AP manufacturers enabling FTM responder functionality to enable more precise asset tracking, time, and motion analysis [4]. This includes several of the recent "mesh" APs (e.g., google Nest Wifi, Eero Pro, Netgear Orbi, Linksys Velop, ASUS RT-ACRH13). Furthermore, FTM initiator functionality Google has worked with key wifi chip vendors(Qualcomm, Broadcom) to enable the complete AOSP ranging framework [5] to integrate multilateration algorithm to estimate the absolute location in an indoor environment. Salomon et al. [6] proposed the implementation of distance estimation approaches based on both RSSI and CSI measurements using the Nexmon CSI Extractor on Raspberry Pi 4 devices. In a multi-radio environment, the fusion-based scheme can be used to improve location in diverse ways to achieve higher precision with frequency band diversity [7].

6 Conclusions

In this paper we have presented an overview of the parameters that can affect the accuracy of the FTM protocol and performed an experimental study using three different com-

mercial Wi-Fi chipsets supporting the Wi-Fi FTM protocol. We compared the ranging accuracy achieved in the different bandwidth configurations for a short distance (up to 1.5m) indoor scenario as well as a longer distance (up to 10m) outdoor scenario, finding that while the Wi-Fi FTM chipsets that support the wider channel bandwidths available in the 5GHz spectrum are capable of providing fairly accurate ranging estimations in both the indoor (short range) and outdoor (longer range) scenarios, Wi-Fi FTM ranging at 2.4GHz on the narrower HT20 bandwidths performs poorly in the indoor setting at shorter distances, where believe that the lower receiver sensitivity of the HT20 devices is a significant factor. While we were unable to comprehensively evaluate all of the Wi-Fi cards which currently support FTM, these findings show that Wi-Fi FTM deployments should strongly consider using 5GHz VHT80 configurations for accuracy at both longer and shorter ranges. Furthermore, by sniffing the on-air packets, we have demonstrated that Wi-Fi FTM messaging is completely unprotected and could easily be tampered with. These findings suggest that as well as studying upcoming improvements to Wi-Fi FTM accuracy through the IEEE 802.11az specification, which leverages MAC and PHY-level techniques, further work is needed to explore the Wi-Fi FTM security concerns and mitigations we have outlined in our threat model.

References

[1] Kin K. Leungl Ḟaheem Zafari, Athanasios Gkelias. A Survey of Indoor Localization Systems and Technologies. *IEEE Communications Surveys & Tutorials*, 21:31, 2019.

[2] Carlo Alberto Boano, Marco Zúñiga, James Brown, Utz Roedig, Chamath Keppitiyagama, and Kay Römer. Templab: A Testbed Infrastructure to Study the Impact of Temperature on Wireless Sensor Networks. In *Proc. of the 13th IPSN Conf.*, pages 95–106. IEEE, April 2014.

[3] Govind Singh and Anshul Pandey. Reliable and Secure V2X Communications with Wi-Fi Neighbor Aware Networking. In *Proc. of the 7th WiSPNET Conf.*, pages 276–281. IEEE, 2022.

[4] Tim Vanevenhoven. A New Way to Add Indoor Location Context, October 2020. [Online] http://blogs.arubanetworks.com/corporate/a-new-way-to-add-indoor-location-context/ — Last accessed: 2023-02-13.

[5] Google AOSP. Wi-Fi location: ranging with RTT, 2021. [Online] https://developer.android.com/guide/topics/connectivity/wifi-rtt/ — Last accessed: 2023-02-13.

[6] Elisabeth Salomon, Leo Happ Botler, Konrad Diwold, Carlo Alberto Boano and Kay Römer. Comparison of Channel State Information driven and RSSI-based WiFi Distance Estimation. In *Proc. of the 18th EWSN Conf.*, pages 173–174. Junction Publishing, February 2021.

[7] Carlos S Álvarez-Merino, Hao Qiang Luo-Chen, Emil Jatib Khatib, and Raquel Barco. WiFi FTM, UWB and Cellular-based Radio Fusion for Indoor Positioning. *Sensors*, 21:7020, 2021.