Is hardware preventing Wi-Fi RTT success?

1. Positioning by means of the Wi-Fi technology

The IEEE 802.11 standard, also known as Wi-Fi, defines communication networks and does not account for specific location purposes. However, due to its widespread deployment and use, exploiting this technology to get a position has always raised so much attention. For many years, it seemed that the only possible way went through the observation of the received signal strength (RSSI): why? Because such a metric is available in any off the shelf device. However, the high variability of the RSSI makes it pretty sensitive to environmental changes, thus leading to inaccurate estimations of the device's position. On the other hand, the use of other metrics, such the angle of arrival (AoA) or the round trip time (RTT) for positioning, often required custom hardware

In 2016, a procedure was introduced in the IEEE 802.11 standard [IEEE, 2016] to estimate the RTT between two devices. This new feature (known as IEEE 802.11mc) paves the way for enabling location services over Wi-Fi networks, further than their foundational communication purposes.

2. What is Wi-Fi RTT?

The Wi-Fi RTT procedure, as defined in the IEEE 802.11mc feature, is depicted in Figure 1.

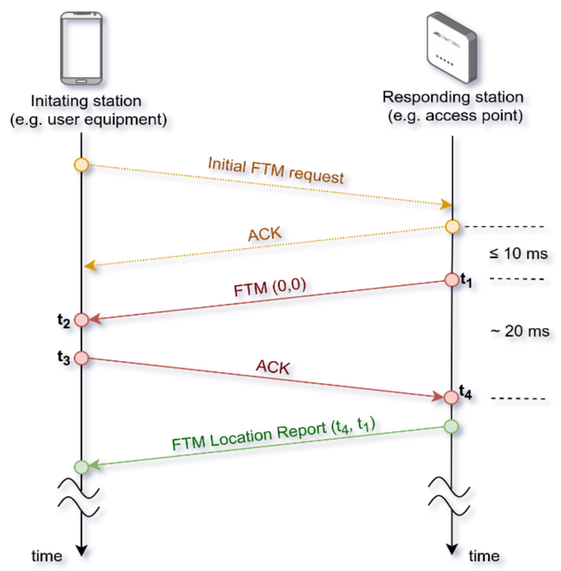

Figure 1. RTT estimation with IEEE 802.11mc (Wi-Fi RTT)

The device on the left (e.g., the initiating station) needs to estimate its position. For that, it sends a Fine Time Measurement (FTM) request to the responding station (e.g., typically an access point (AP) that advertises the 802.11mc feature); the latter needs to acknowledge the request before starting the FTM procedure. The time of departure (t_1) and arrival (t_2) of the FTM frame are stored at the responding and initiating stations, respectively. When the initiating station sends an acknowledgement back, again the departure (t_3) and arrival (t_4) times of this frame are recorded at the initiating and responding stations, respectively. A last step is needed in order to deliver the measurements taken at the responding station (e.g., timestamps t_1 and t_4) to the initiating station, where the RTT is computed as

$$RTT = (t_4 - t_1) - (t_3 - t_2).$$

Finally, the initiating station can derive its distance from the responding station by multiplying the RTT by the speed of light and dividing by 2, that is: $d = \frac{RTT \cdot speed}{2}$.

Despite this procedure allowing precise time measurements and hence accurate position estimation, there are still open issues the Wi-Fi RTT technology has to address, such as the **hardware availability**.

3. How does BANSHEE use Wi-Fi RTT?

The BANSHEE location solution aims at coupling GNSS with Wi-Fi RTT to provide the best indoor positioning experience. Such an approach has been used repeatedly in the past to assist GNSS in scenarios where these technologies can hardly fix a position due to poor signal reception conditions.

What makes BANSHEE a novel solution, then? Firstly, the use of the Wi-Fi RTT technology for ranging estimation, which provides better accuracy indoors; and secondly, the use of GNSS to fix the APs position. Thus, the BANSHEE solution does not rely on APs announcing their own position, which requires network operators to fill the data properly. Instead, BANSHEE aims to fix the positions where such APs are by using GNSS. Two scenarios may be drawn:

1. Wardriving. In case the BANSHEE client knows its own position (e.g., by means of GNSS), the procedure in Figure 1 can be used to fix the position of every Wi-Fi RTT AP at sight.
2. Positioning. Whenever the BANSHEE client knows where the Wi-Fi RTT APs are, it can fix its own position by using the procedure in Figure 1 and GNSS data (if available).

This dual role of the BANSHEE clients makes them able to take advantage from accurate positions from the GNSS whenever available (e.g. outdoors) and, at the same time, it paves the way to a robust indoor positioning based on Wi-Fi RTT where the GNSS signals are either degraded or simply not available.

4. What devices support IEEE 802.11mc?

Although the technology has been ready for use over the last 5 years, compatible hardware is still scarce if compared with the ubiquity of Wi-Fi technology. The following sections explore the support received by the industry for both the user equipment and the network infrastructure.

4.1 User equipment

Brand	**Models**
Google	Pixel 1, 2, 2XL, 3, 3XL, 3a, 4, 4XL, 4a, 5, 5a
Xiaomi	Mi 10 (T, Pro), Mi Note 10 (lite), Mi 9 (T), Redmi Note 9 (S, Pro), Redmi Mi 9T Pro, Redmi Note 8 (T), Redmi Note 5 Pro, Redmi K20 (Pro), Redmi K30
Samsung	Galaxy Note 10 (+, 5G, +5G), Galaxy S20 (+, 5G, +5G, Ultra 5G)
LG	G8X ThinQ, V50S ThinQ, V60 ThinQ, V30
Poco	X2, F3 (Pro)
Sharp	Aquos R3 SH-04L
Zebra	PS20, TC52/TC52HC, TC57, TC72, TC77, MC93, TC8300, VC8300, EC30, ET51, ET56, L10, CC600/CC6000, MC3300x, MC330x, TC52x, TC57x, EC50 (LAN, HC), EC55 (WAN), WT6300

Table 1. List of mobile phones officially compatible with the IEEE 802.11mc technology as for November 2021.

Some of the largest hardware and software manufacturers, such as Intel or Google, announced their support for the technology. In 2018, Google decided to make the IEEE 802.11mc accessible to the mass market, by supporting the standard into the Android O.S., from version 9 (Pie) onwards. Thus, over the last two years, the list of compatible mobile devices supporting the Wi-Fi RTT has drastically increased. Google continuously tracks the devices that have been confirmed to work with IEEE 802.11mc and keep up to date a list in [Android, 2021], which is summarized in Table 1.

However, even though Google has boosted the use of the IEEE 802.11mc by supporting it in the Android O.S., the actual support of the technology depends on the brand/device being used. Thus, **there are several devices that, even though running Android 9 or higher, do not support the IEEE 802.11mc technology due to a manufacturer's decision**. Hence, no general statement can be set in terms of compatibility for a specific brand.

4.2 Network Infrastructure (Access points)

For the time being, only a low percentage of the APs in private networks support the IEEE 802.11mc technology. Although this condition is expected to change in the near future, it currently limits both the infrastructure availability and the users that can employ the location system.

Nowadays, only few APs officially support the technology [Android, 2021]: Compulabs WILD, Google Wi-Fi, Google Next Wi-Fi Point and Google Next Wi-Fi Router, as displayed in Figure 2. The former is about to be discontinued and the company discourages its use in new projects, so only three APs can be effectively used.

Currently, another manufacturer (HPE/Aruba) plays a key role when supporting the IEEE 802.11mc technology. Together with CISCO, it is one of the most important providers of "enterprise level" Wi-Fi systems. In the case of HPE/Aruba, all Wi-Fi 6 APs (e.g. 500/H series, 510 series, 530 series, 550 series, 560 series, 570 series and AP-630 series) support IEEE 802.11mc, either by running ArubaOS (from version 8.7 released in July 2020, onwards) or InstantOS (from version 8.8 onwards).

Despite providing indoor positioning features, the other key actor in this segment, CISCO with Meraki solutions, does not still support IEEE 802.11mc at the time this paper is written.

Figure 2. APs officially supporting the IEEE 802.11mc technology

Although the mass market devices officially supporting the technology seems to be quite short, there are several APs that, even not actively promoting the technology, are able to deal with the Wi-Fi RTT. Figure 3, displays some of the ones that have been reported to work in this way. Such devices are mostly mesh APs. It is expected that mesh Wi-Fi networks will be the predominant solution for home Wi-Fi deployment in the near future, as they make the whole Wi-Fi network setup accessible to every user profile.

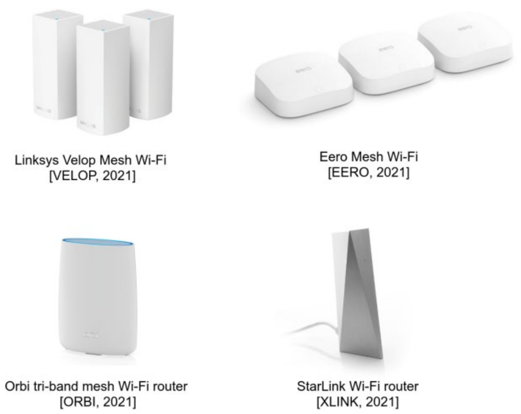

Figure 3. APs supporting, but not advertising, the IEEE 802.11mc technology

Most of the solutions shown in Figure 3 are based on a Qualcomm chipset, so it is likely that any device bundling this pair of chips should work, too. Apart from Qualcomm, there are other chipsets able to deal with Wi-Fi RTT; some of them are listed in Table 2. The capability of handling FTM frames, however, may depend on the specific device integrating these hardware solutions.

Manufacturer	**Model**
Intel	Dual Band Wireless-AC 8260, 8265 and 9260
Marvell	AP-8964 802.11ac 4x4 Wave2
MediaTek	MT663X 802.11abgn/ac
Qualcomm	IPQ4017, IPQ4018, IPQ4019, IPQ4028, IPQ4029, IPQ8065, QCA9984, QCA9986
Realtek	RTL8812BU

Table 2. List of chipsets that are able to attend FTM requests

It must be noted that many Wi-Fi adapters are unable to work as APs because of regulatory restrictions. Channels on these Wi-Fi adapters may be marked as *no IR* (i.e. passive scan only) and hence prevent the device from running the Wi-Fi RTT procedure. Solutions based on Intel 8260, Intel 8265 and Intel 9260 Wi-Fi cards are just some examples of this: they support IEEE 802.11mc when they work as initiating stations, but are not allowed to act as APs. There are some exceptions, such as the Compulabs WILD, which is based on an Intel 8260 card and it can play the role of AP.

5. Conclusion

IEEE 802.11mc is considered a noticeable step forward in the field of indoor positioning. The ubiquity of the Wi-Fi technology makes it especially suitable for location purposes and the support for fine time measurements in Wi-Fi hardware opens a large range of opportunities.

For the time being, the number of devices officially compatible with the technology is pretty short. However, unofficially, there are lots of devices, both stations and APs, able to run the IEEE 802.11mc procedure, which alleviates the apparent lack of support of the manufacturers to the technology. This is mainly due to the fact that IEEE 802.11mc can be often enabled by software, with no hardware customization requirements. Therefore, it is expected that a large number of devices will support this technology in the near future.

Acknowledgements

This research was supported by the European GNSS Agency under grant GSA/GRANT/04/2019/BANSHEE.

References

[IEEE, 2016] IEEE Standard for Information technology. Telecommunications and information exchange between systems Local and metropolitan area networks. Specific requirements," in IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012), pp.1-3534, 14 Dec. 2016.

[Android, 2021] IEEE 802.11mc compatibility list by Google, https://developer.android.com/guide/topics/connectivity/wifi-rtt#supported-devices (accessed in November, 2021).