Experimental Evaluation of Ranging Error in COTS Devices Using One-Sided Wi-Fi RTT

Enrica Zola
Dept. of Network Engineering
Universitat Politècnica de Catalunya
BarcelonaTECH (*UPC*)
Barcelona, Spain
enrica.zola@upc.edu

Israel Martin-Escalona
Dept. of Network Engineering
Universitat Politècnica de Catalunya
BarcelonaTECH (*UPC*)
Barcelona, Spain
israel.martin@upc.edu

***Abstract*—IEEE 802.11mc Fine Timing Measurement (FTM) enables distance estimation between wireless devices and represents a promising technology for indoor positioning. However, conventional Wi-Fi RTT relies on FTM-capable access points (APs), limiting its deployment in existing networks. One-sided Wi-Fi RTT overcomes this limitation by enabling ranging without requiring modifications to the AP infrastructure. Despite its practical relevance, the impact of commercial hardware implementations and protocol parameters on one-sided Wi-Fi RTT performance remains largely unexplored. This paper presents an experimental characterization of one-sided Wi-Fi RTT ranging in commercial off-the-shelf (COTS) hardware under line-of-sight. Rather than evaluating downstream positioning algorithms or synthetic filtering, this study exposes the unfiltered ranging errors, sample completion dynamics, and hardware biases across different devices. Results show that raw one-sided Wi-Fi RTT performance is strongly hardware-dependent. Google Pixel devices operating in the 5 GHz band achieve post-calibration residual RMSE of $\approx$ 3 m, whereas other device/AP combinations exhibit substantially larger variability, heavy-tailed error distributions, and frequent out-of-range estimates. Increasing burst size generally reduces measurement variability but does not eliminate hardware-dependent effects. These findings demonstrate both the potential and the current limitations of infrastructure-independent Wi-Fi RTT ranging, providing practical insights for the design of indoor positioning systems in networks lacking FTM-capable APs.**

***Index Terms*—IEEE 802.11mc; One-sided Wi-Fi RTT; Indoor Localization; Wireless Ranging; Infrastructure-Independent Ranging; Performance Evaluation.**

I. Introduction

Accurate indoor positioning systems (IPSs) have become increasingly important for a wide range of applications, including asset tracking, indoor navigation, smart-building automation, and emergency response services [1]. Traditionally, many indoor localization solutions have relied on the received signal strength indicator (RSSI) due to its widespread availability in commercial off-the-shelf (COTS) wireless devices. Moreover, its passive nature supports the design and development of scalable indoor location systems. However, RSSI measurements are highly sensitive to propagation conditions and can be significantly affected by small-scale fading, multipath propagation, environmental changes, and body shadowing [2]. Although fingerprinting techniques can mitigate some of these effects by exploiting the spatial characteristics of the radio environment, the deployment and maintenance of dense radio maps remain labor-intensive and challenging, particularly in large-scale environments [3].

In this context, the introduction of the IEEE 802.11mc standard [4] marked a paradigm shift by defining the fine timing measurement (FTM) protocol, which enables accurate ranging estimation by measuring the round-trip time (RTT) between two Wi-Fi devices [5]. Under stable line of sight (LOS) conditions, standard two-sided Wi-Fi RTT can achieve meter-level or even sub-meter positioning accuracy when combined with techniques such as multilateration, deep learning, or advanced Kalman filtering [6]. Despite these advantages, FTM-based RTT faces a significant infrastructure-dependent scalability bottleneck, as it requires explicit FTM support on both the initiating user equipment (UE) and the responding access point (AP) infrastructure. . Upgrading large-scale legacy corporate or public networks to FTM-capable AP hardware remains labor- and cost-prohibitive. Moreover, small-scale private Wi-Fi deployments, typically managed by home users, are unlikely to be widely upgraded. Overall, these factors limit the widespread adoption of this positioning technology.

To overcome this infrastructure dependency, Google introduced an updated localization API in Android 12 that enables a key capability: one-sided Wi-Fi RTT. This approach allows an FTM-capable UE to perform ranging measurements with legacy APs, i.e., those that do not support Wi-Fi RTT. In a standard two-sided FTM procedure, accurate timestamps are taken at both the AP and the UE, allowing the processing time to be effectively removed. In contrast, one-sided RTT estimation relies on high-resolution timestamps only at the UE side. While this approach significantly extends the availability of ranging estimates, it introduces an additional systematic bias in the estimated distance because legacy APs do not provide information about their internal processing delay, i.e., the time elapsed between the reception of a frame and the transmission of the corresponding acknowledgment (ACK). As a result, the raw RTT estimates exhibit device-dependent biases influenced by the hardware and firmware implementations of both the UE and the AP.

979-8-3195-0167-7/26/$31.00 ©2026 IEEE

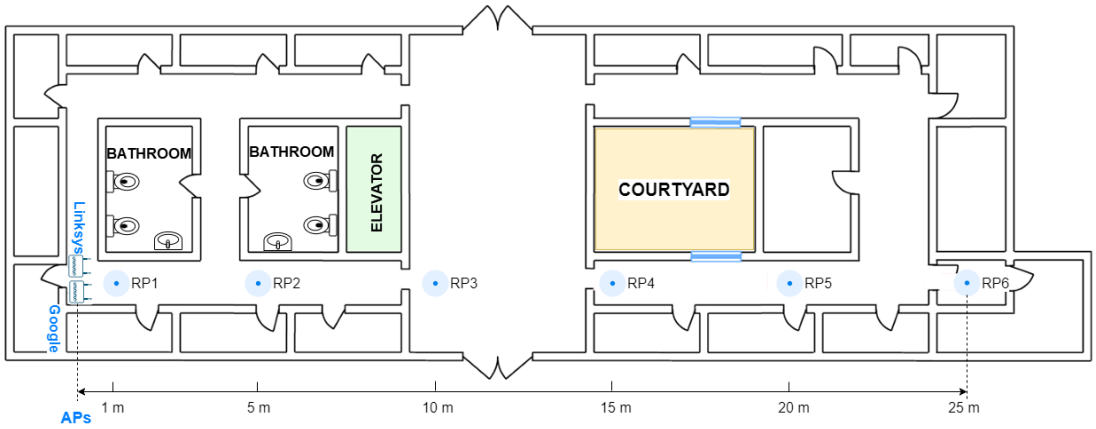


Fig. 1. Scenario of the measurement campaign

While the state of the art has extensively characterized the systematic biases and noise properties of conventional two-sided RTT measurements [2], [7], only a limited number of studies have investigated the one-sided counterpart [8]. Furthermore, the joint impact of burst size, operating frequency, and heterogeneous commercial hardware on one-sided Wi-Fi RTT remains unexplored. This paper addresses this gap through an extensive experimental campaign under controlled LOS conditions. The primary scope of this work is to establish an unvarnished empirical baseline of raw one-sided Wi-Fi RTT measurements. By explicitly isolating the effects of hardware, frequency band, and burst size without applying downstream filtering or tracking algorithms, this paper provides the foundational error models required to design future outlier-resilient indoor positioning system.

To summarize, the main contributions of this paper are:

- **Heterogeneous COTS Characterization**: To the best of our knowledge, we provide the first systematic characterization of one-sided Wi-Fi RTT ranging across heterogeneous COTS smartphones and AP, considering both 2.4 and 5 GHz operation and a wide range of burst sizes.
- **Impact of Protocol Parameters**: We systematically analyze the effect of the burst size ($BS \in [2, 29]$) on measurement completion rate, sample variability, and error distributions.
- **Empirical Error and Bias Profiling**: We demonstrate that, while raw one-sided RTT contains massive hardware-dependent systematic biases, median-offset compensation yields meter-level accuracy ($RMSE \approx 3$ m) under 5 GHz LOS conditions.

The remainder of this paper is organized as follows. Section II describes the measurement collection procedure. Section III evaluates the ranging performance and analyzes the resulting error characteristics after offset compensation. Finally, Section IV concludes the paper and discusses the implications of the findings for future indoor positioning systems.

II. Measurement Collection

Since the new localization API was implemented in Android 12, Google has enabled the use of two features defined in the IEEE 802.11mc standard [4]. The first one is the **one-sided Wi-Fi RTT**. This procedure allows an FTM-capable device (the UE in our setting) to estimate its RTT with a non-FTM-capable device (the AP in our setup). Null Function data (NFD) frames are used instead of the standard FTM exchange, allowing any legacy AP to respond with a standard ACK frame. The UE records two high-resolution timestamps: the departure time of the NFD request (t_1) and the arrival time of the corresponding ACK (t_4) in nanoseconds. The raw RTT is then calculated at the UE with high-resolution (ns) as:

$$rtt = (t_4 - t_1). \tag{1}$$

Because legacy APs do not report the arrival time of the NFD request (t_2) and the departure time of the ACK (t_3), the internal processing delay cannot be subtracted from the one-sided estimate, introducing a heavy, hardware-dependent systematic offset into the calculated distance.

To mitigate the noise introduced by the processing time, Android 12 enabled a second feature: the **ability to configure the burst size (BS)**. The Android application used in [9], which is based on Google's Android WifiRttScan [10], has been modified to make this possibility available for our experiments. In this paper, all the BS values between 2 and 29 have been used to assess their impact on the ranging performance of one-sided RTT in COTS devices. The Android application provides ranging estimates computed as the mean of the one-sided RTTs obtained during a single range-estimation burst (e.g., 8 RTT measurements when BS=8). In the following, we will refer to each ranging estimation as a sample. It is worth noting that a sample is considered successful whenever at least one RTT measurement within the burst is received.

TABLE I
AP CONFIGURATION PARAMETERS

Parameter	Google	Linksys Velop	
Frequency band	5 GHz	2.4 GHz	5 GHz
Channel bandwidth	80 MHz	20 MHz	80 MHz
Channel number	42	4	42
Wi-Fi standard	802.11ac	802.11n	802.11ac
Frequency channel	5,210 MHz	2,427 MHz	5,210 MHz
AP Name	Google 5	Linksys 2.4	Linksys 5

A. Experimental Settings

The one-sided RTT measurements were collected along a 30-meter-long corridor of the Network Engineering Department at the UPC in Barcelona (Spain). The measurement campaign was conducted using two APs placed at one end of the corridor on a 0.5m-high bench, and the UE positioned on a 0.5m-high tripod at each of six reference points (RPs) (shown as blue circles in Fig. 1.) The RPs are aligned along a straight line with the APs, at increasing distances: *RP1* is located 1 m from the APs, *RP2* at 5 m, and so on, up to *RP6*, which is located 25 m from the APs. LOS conditions between the UE and the APs were ensured to establish a baseline for one-sided RTT measurements. This controlled setup minimizes propagation-related impairments, enabling subsequent deviations observed under obstructed conditions to be assessed relative to a well-defined reference case.

The two APs already used in our previous experiments with regular Wi-Fi RTT [7] were considered for these experiments: the Google Nest Wi-Fi router [11], and the Linksys Velop AP [12]. One-sided RTT experiments have been carried out in the channels and frequency bands reported in Table I. From now on, we refer to the Google Nest AP working at 5,210 MHz as *Google 5*, and to the Linksys Velop AP working at 2,427 MHz and 5,210 MHz as *Linksys 2.4* and *Linksys 5*, respectively.

Four UEs were tested [7], [13], all updated to the latest supported Android release (i.e. at least Android 12). One smartphone from Xiaomi (Mi 10T) and three models from Google were considered: the Pixel 3a, the Pixel 4a, and the newer Pixel 6 Pro. By including devices from different vendors and hardware generations, the study can assess the extent to which one-sided RTT measurements are influenced by hardware-specific characteristics, thereby increasing confidence in the general applicability of the findings.

B. Methodology

In this study, several experiments are conducted using COTS devices from two brands and multiple models, evaluating the one-sided RTT procedure with the two APs under different burst size (BS) values.

The measurement campaign begins by placing one of the four phones (e.g. Pixel 3a) at a given RP (e.g. *RP1*). The ranging application is configured with a specific BS value (e.g. BS=2), and then the sample collection is initiated. 200 ranging estimations are gathered for each of the available frequency bands of the two APs (see Table I). The experiment is then repeated for each BS value.

Once samples from all the BSs have been collected at *RP1*, the phone is moved to the next RP and the experiments are repeated. Once all RPs have been covered, the measurement campaign is repeated for each of the other UEs. Thus, considering 200 samples per BS and RP, each UE is expected to collect 33,600 samples for each AP/frequency configuration.

C. Analysis of the Collected Samples

In this section, the percentage of requested samples that were successfully collected is analyzed to establish a performance threshold for each UE model and, where applicable, each AP. As shown in Fig. 2, the Pixel 3a collects all requested samples regardless of the BS, AP and frequency band. Also, the other UEs are able to gather almost all requested samples (99.84% on average) when operating with Google 5 (blue) and Linksys 2.4 (green), for any BS. Similar results (99.96%) for Pixel 4a and Mi 10T with Linksys 5 (orange).

In contrast, the Pixel 6 Pro exhibits several limitations when evaluating one-sided RTT with Linksys 5. First of all, the maximum supported BS is limited to 25; then, for BSs between 8 and 10, at distances up to 10 m, it successfully collected an average of 98.22% samples; also, at distance 1 m, it collected 97.67% of the samples, regardless of the BS; finally, for all the other combinations of BS and distance, the average ratio of collected samples to the requested number drops to 3.94%. This erratic behavior may be related to hardware (e.g., driver-level timeouts) limitations of this Pixel model.

We now focus on the number of RTT estimates used to compute a single ranging sample. Fig. 3 shows the average number of NFD/ACK frame exchanges successfully completed (i.e., yielding a ranging estimate), relative to the requested number of NFD frames, for each burst size. For example, when BS=8, the number of requested NFDs frames for one-sided RTT is 8. Note that all the samples collected across the different RPs are included in the analysis. All the UE models, except the Pixel 6 Pro, are able to achieve the user-configured BS, regardless of the AP and frequency band used. Again, the Pixel 6 Pro appears to exhibit limitations when operating with Linksys 5 (orange) AP. For the remaining APs, the average number of successfully completed NFD/ACK exchanges by the Pixel 6 Pro is approximately one lower than the requested.

III. RANGING PERFORMANCE OF THE ONE-SIDED RTT

This section analyses the ranging error observed from the measurements collected using the one-sided Wi-Fi RTT procedure. First, the raw ranging error is assessed to identify the offset associated with the raw measurements (Section III-A). The distribution of the residual ranging error is therefore analyzed in Section III-B.

A. Raw Ranging Estimations

Fig. 4 shows the mean ranging error observed for different APs (different colors) and for different BSs (x-axis); each subplot shows a different UE. In general, the mean ranging

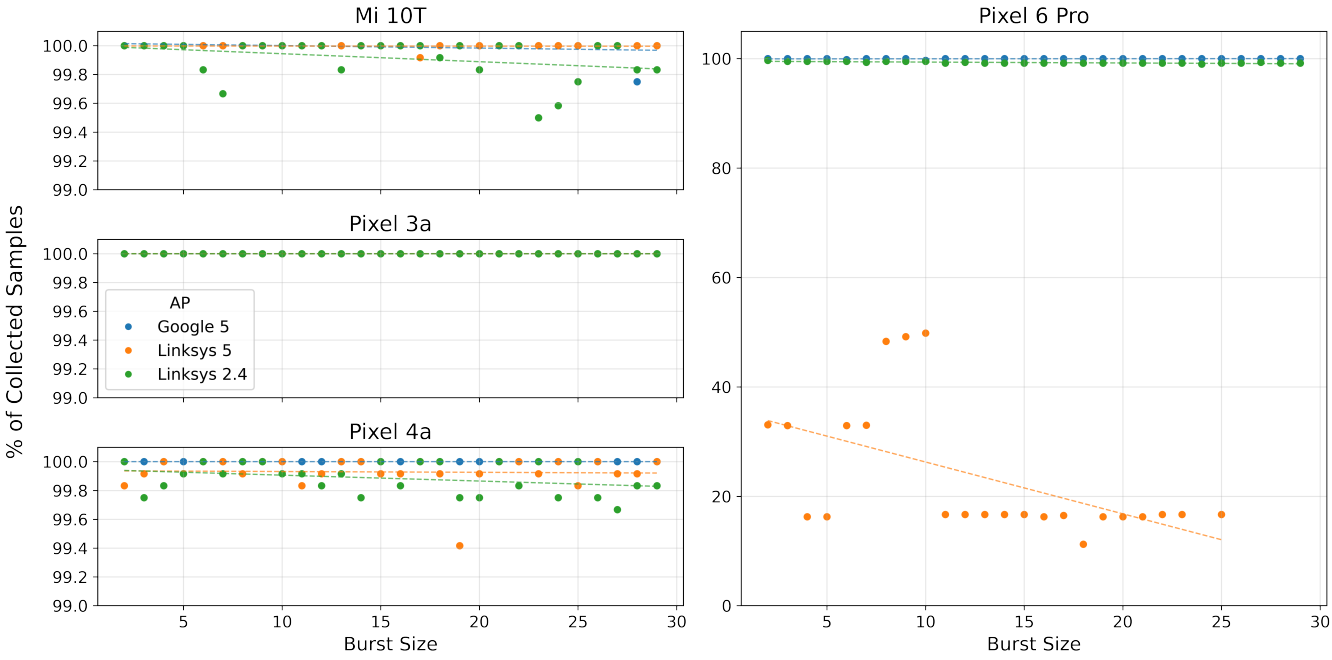


Fig. 2. Average percentage of collected one-sided RTT samples per BS and AP, for different UE models. A sample is considered collected when at least one RTT measurement within the burst is successfully completed. Trend lines are also shown.

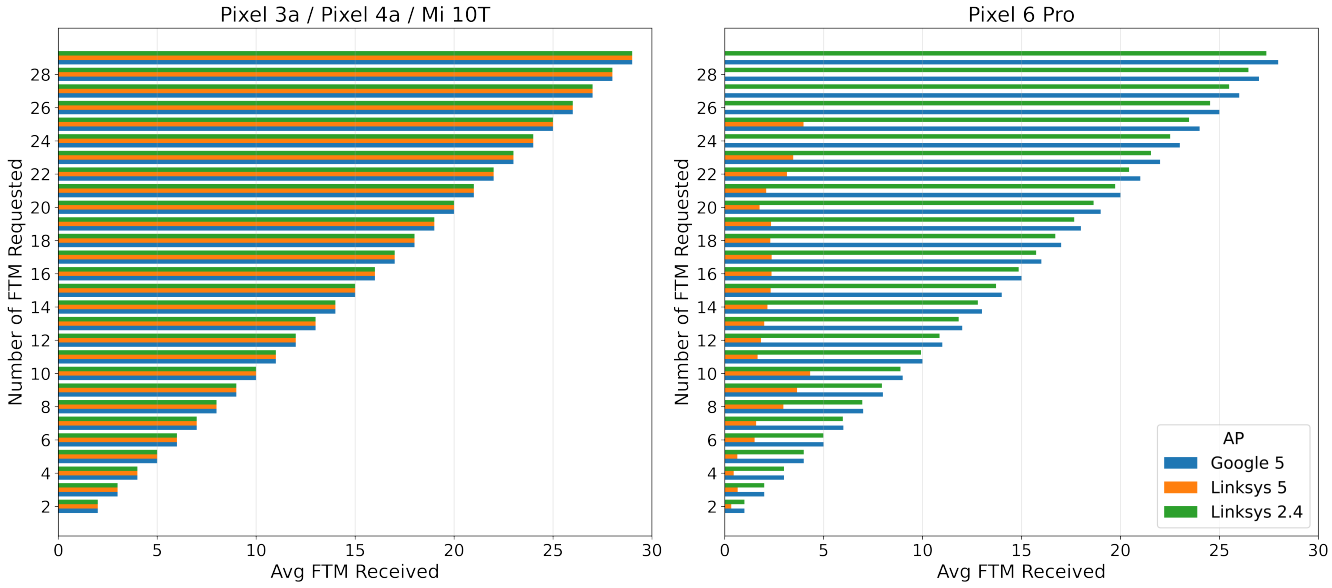


Fig. 3. Number of received ACK vs NFD frames sent per BS and AP, for different UE models.

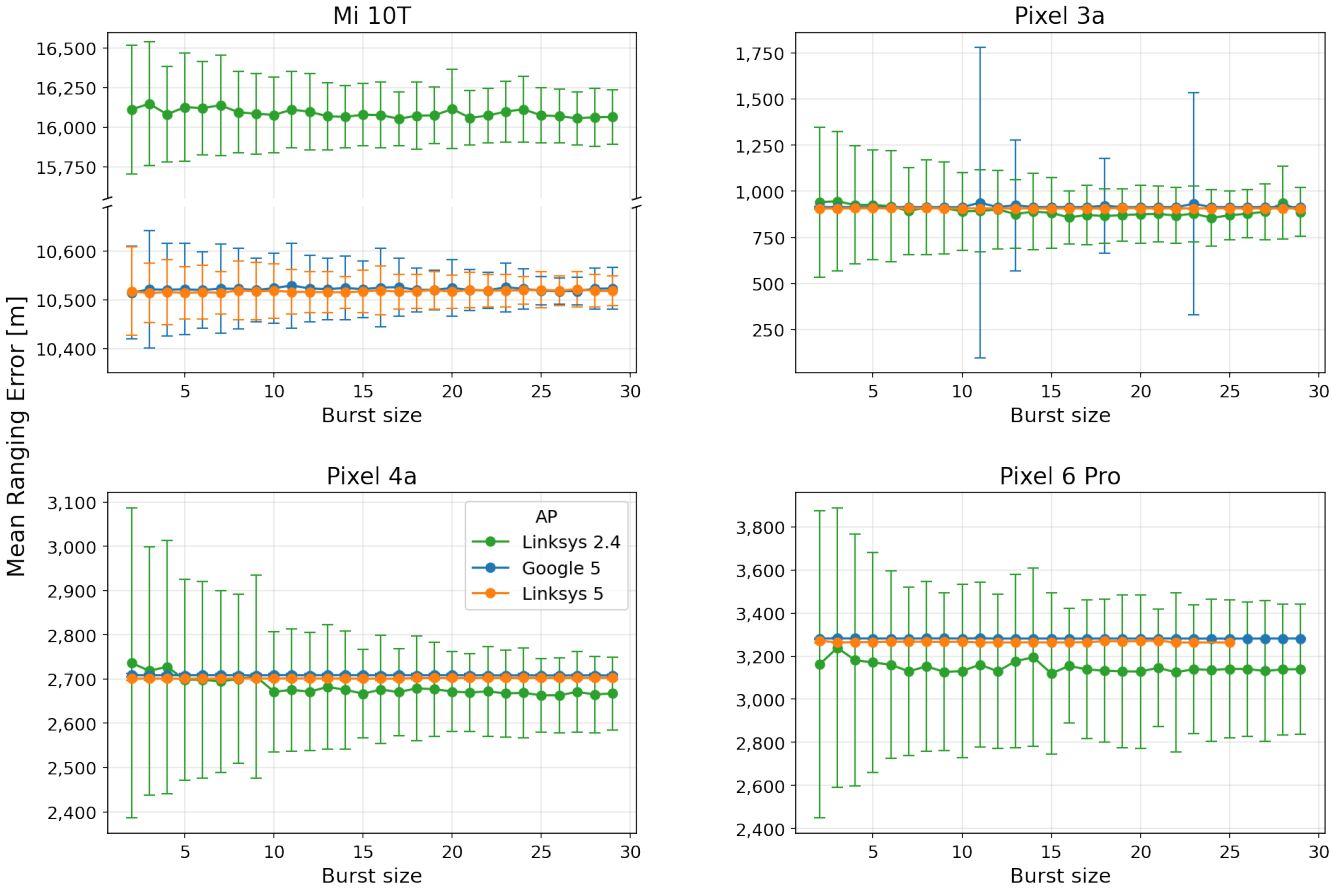


Fig. 4. Mean Ranging error (before offset removal) per each AP and BS, and for different UE models. Vertical error bars represent the STD.

TABLE II
STANDARD DEVIATION [M] OF THE RANGING ERROR (BEFORE OFFSET REMOVAL), AVERAGED OVER ALL BSS

AP	Pixel 3a	Pixel 4a	Pixel 6 Pro	Mi 10T
Linksys 2.4	206.27	147.43	387.36	232.91
Google 5	75.7	3.59	2.18	62.57
Linksys 5	4.58	3.97	2.42	44.28

error remains relatively stable regardless of the BS for measurements in the 5 GHz band (blue and orange); in the 2.4 GHz band (green), it tends to decrease as the BS increases for all the Pixel models. Pixel 3a shows the lowest mean ranging error (less than 1,000 m) regardless of the AP; on the other hand, the mean ranging error for Mi 10T is always the highest (over 10,500 m).

The STD is depicted as vertical error bars in the plots. In general, it decreases as the BS increases, for all the UE models (except Pixel 3a) with any AP and frequency band. Also, the STD is typically low when any Pixel UE model operates in the 5 GHz band of any AP (blue and orange), while Mi 10T always shows higher deviations. The highest STD appears when operating with Linksys at 2.4 GHz (green), whatever the UE and BS, as also shown in Table II. This table summarizes the STD, averaged over the burst sizes, for each combination of UE and AP.

It is worth mentioning that Pixel 3a generally shows low variability when operating with Google 5, except for specific BSs: for instance, at BS=11, the maximum raw ranging estimation is 30.0 km (i.e., an order of magnitude higher than the average), which explains the big error bar in Fig. 4. Similarly, at BS=13, 18, and 23, the maximum raw ranging estimations are 13.2, 9.8 and 21.8 km, respectively. These out-of-range values represent unfiltered ranging outliers. Rather than filtering them out, they are preserved in this study to accurately report the raw error distribution of COTS hardware. Developing adaptive filtering algorithms to mitigate these anomalies remains a natural next step for downstream positioning engine design.

From Fig. 4, it is evident that the **mean ranging error is hardware dependent** (both UE and AP), **frequency dependent** (2.4 or 5 GHz), **and varies depending on the burst size**, as already observed in the standard two-sided Wi-Fi RTT [7]. Also, all the measurements carry a heavy bias; in order to ensure comparability of the results obtained across different hardware, it must be eliminated before further analysis. A simplified approach, as the one used in [7], [8], is employed for its calibration. Considering that the burst size is a parameter

TABLE III
MEDIAN RANGING ERROR OFFSET [M] FOR EACH UE/AP/FREQUENCY/BS CONFIGURATION. N/A DENOTES NON-AVAILABLE DATA.

BS	Linksys 2.4				Linksys 5				Google 5			
	Mi 10T	Pixel 3a	Pixel 4a	Pixel 6 Pro	Mi 10T	Pixel 3a	Pixel 4a	Pixel 6 Pro	Mi 10T	Pixel 3a	Pixel 4a	Pixel 6 Pro
2	15,882.81	759.63	2,625.05	3,179.85	10,508.45	906.69	2,701.24	3,264.85	10,508.70	914.19	2,708.12	3,281.00
3	15,882.81	760.25	2,625.05	3,180.52	10,507.20	905.44	2,701.24	3,263.45	10,509.33	913.56	2,707.49	3,281.57
4	15,882.81	760.56	2,626.30	3,180.00	10,508.08	905.44	2,701.24	3,264.35	10,510.33	913.56	2,708.12	3,281.90
5	15,883.81	761.00	2,625.05	3,180.86	10,508.08	905.56	2,701.12	3,265.63	10,509.95	913.44	2,708.12	3,281.47
6	16,075.94	760.25	2,625.05	3,180.63	10,508.45	906.69	2,701.24	3,264.89	10,509.70	913.37	2,708.12	3,281.08
7	16,057.10	761.32	2,625.05	3,179.90	10,508.81	905.44	2,701.33	3,265.81	10,509.70	913.38	2,708.12	3,280.93
8	16,038.44	761.81	2,625.36	3,179.11	10,508.45	906.22	2,701.40	3,265.57	10,510.33	913.25	2,707.96	3,281.31
9	16,022.65	762.33	2,625.83	3,179.57	10,508.45	905.85	2,701.45	3,264.91	10,509.91	913.14	2,707.70	3,282.07
10	16,011.31	762.25	2,625.05	3,181.53	10,509.20	905.81	2,701.37	3,265.08	10,509.70	913.19	2,707.74	3,281.91
11	16,021.90	762.07	2,625.39	3,180.38	10,508.79	906.69	2,701.47	3,263.85	10,510.33	913.28	2,708.17	3,282.56
12	16,010.31	763.69	2,625.05	3,180.92	10,507.83	905.44	2,701.55	3,263.72	10,509.08	913.56	2,708.12	3,281.45
13	15,999.26	763.19	2,624.97	3,180.84	10,508.21	905.44	2,701.58	3,263.75	10,509.56	913.57	2,708.07	3,281.20
14	15,996.38	762.66	2,625.05	3,181.01	10,508.70	905.97	2,701.69	3,264.14	10,509.70	913.63	2,708.29	3,281.13
15	16,057.31	839.75	2,624.55	3,181.25	10,508.20	905.44	2,701.37	3,263.71	10,509.33	913.56	2,707.99	3,281.38
16	16,036.88	835.21	2,625.05	3,181.32	10,508.14	905.44	2,701.55	3,264.02	10,509.70	913.48	2,708.12	3,281.40
17	16,033.99	832.75	2,624.56	3,181.34	10,508.23	905.32	2,701.50	3,264.76	10,509.78	913.55	2,708.12	3,281.47
18	16,026.35	829.83	2,624.39	3,181.30	10,509.75	905.43	2,702.28	3,269.00	10,509.91	913.77	2,707.91	3,281.18
19	16,041.29	827.47	2,624.13	3,181.11	10,510.30	905.02	2,702.27	3,267.63	10,509.88	913.79	2,707.98	3,280.82
20	16,033.94	824.38	2,624.43	3,181.09	10,508.45	905.81	2,702.30	3,269.94	10,509.70	913.69	2,707.83	3,280.70
21	16,026.74	822.39	2,624.58	3,179.60	10,510.78	905.88	2,702.49	3,272.68	10,509.79	913.92	2,707.67	3,281.30
22	16,029.29	819.28	2,624.54	3,180.30	10,510.22	906.51	2,702.49	3,263.62	10,510.16	913.84	2,708.65	3,281.27
23	16,066.07	818.40	2,624.63	3,179.78	10,510.25	905.84	2,702.37	3,263.44	10,510.98	913.86	2,707.65	3,280.82
24	16,071.50	812.06	2,625.05	3,179.92	10,511.27	906.78	2,702.33	N/A	10,510.64	913.97	2,707.65	3,280.81
25	16,034.21	820.45	2,625.05	3,180.48	10,510.45	905.66	2,702.40	3,263.67	10,510.05	913.91	2,707.29	3,280.73
26	16,042.24	821.43	2,625.05	3,179.52	10,510.09	905.58	2,702.35	N/A	10,509.70	913.86	2,707.63	3,281.23
27	16,026.70	828.79	2,624.90	3,178.82	10,510.40	905.61	2,702.42	N/A	10,509.70	913.74	2,707.70	3,281.19
28	16,003.29	853.04	2,625.05	3,179.76	10,508.90	905.70	2,702.60	N/A	10,509.52	914.04	2,708.01	3,281.27
29	16,026.87	847.43	2,625.18	3,179.48	10,509.23	905.97	2,702.49	N/A	10,509.59	913.97	2,708.05	3,281.25

that the user must adjust when running ranging measurements, it is straightforward to consider a different offset for each UE/AP/frequency/BS combination [7], [14]. Also, due to the typical heavy-tailed distribution of the RTT error, the median is expected to be a more robust estimator for the offset of the RTT error than the mean.

Thus, from the following section, for each combination of UE/AP/frequency/BS, the median is subtracted from the one-sided RTT measurements. It is important to emphasize that, after an offline calibration phase using reference distances, real-world measurements do not require prior knowledge of the user's distance. Because the processing delay and hardware latency are tied to specific hardware and protocol configurations rather than the user's position, the median offsets compiled in Table III per each combination serve as a static lookup table. The measured offsets can therefore be used as configuration-specific calibration values under conditions similar to those of the calibration campaign.

As reported in Table III, the raw offset (median ranging error) exhibits a strong vendor dependency. While Google Pixel devices maintain median offsets between 760 m and 3,280 m across both frequency bands, the Xiaomi Mi 10T exhibits an extreme systematic offset exceeding 15,800 m exclusively when operating in the 2.4 GHz band. This anomaly may be related to vendor-specific hardware abstraction layer (HAL), driver, or firmware behavior. The 15.8 km bias (≈ 105 μs of equivalent round-trip delay) is consistent with a substantial timestamping delay and may suggest that timestamp generation occur at a higher layer than the PHY. However, the present measurements cannot identify the precise source of this delay. Despite this massive initial bias, applying median-offset compensation successfully centers the residual error distribution for all devices, though 2.4 GHz measurements still exhibit substantially higher variance compared to 5 GHz.

B. Residual Ranging Error Jitter

In this section, we analyze the residual ranging error, that is the error after the offset has been removed from the measurements. Because a different offset and a different behavior is observed depending on the burst size, for space reasons we only show the results obtained when BS=8. This is the default setting for any Android device, thus the most probable configuration in real deployments. Also, it is worth mentioning that, for BS=8, for all the Pixel UE models when working in the 5 GHz band, the median of the raw ranging error is very close to the mean, with differences of less than 1.70 m.

Figure 5 shows the probability density functions (PDFs) of the residual ranging error for different UE models (different colors). Although only results for a burst size of 8 are presented, the conclusions drawn from this analysis are generally applicable to all burst sizes. The vertical black line serves as a reference for zero-error. Since the offset was removed as

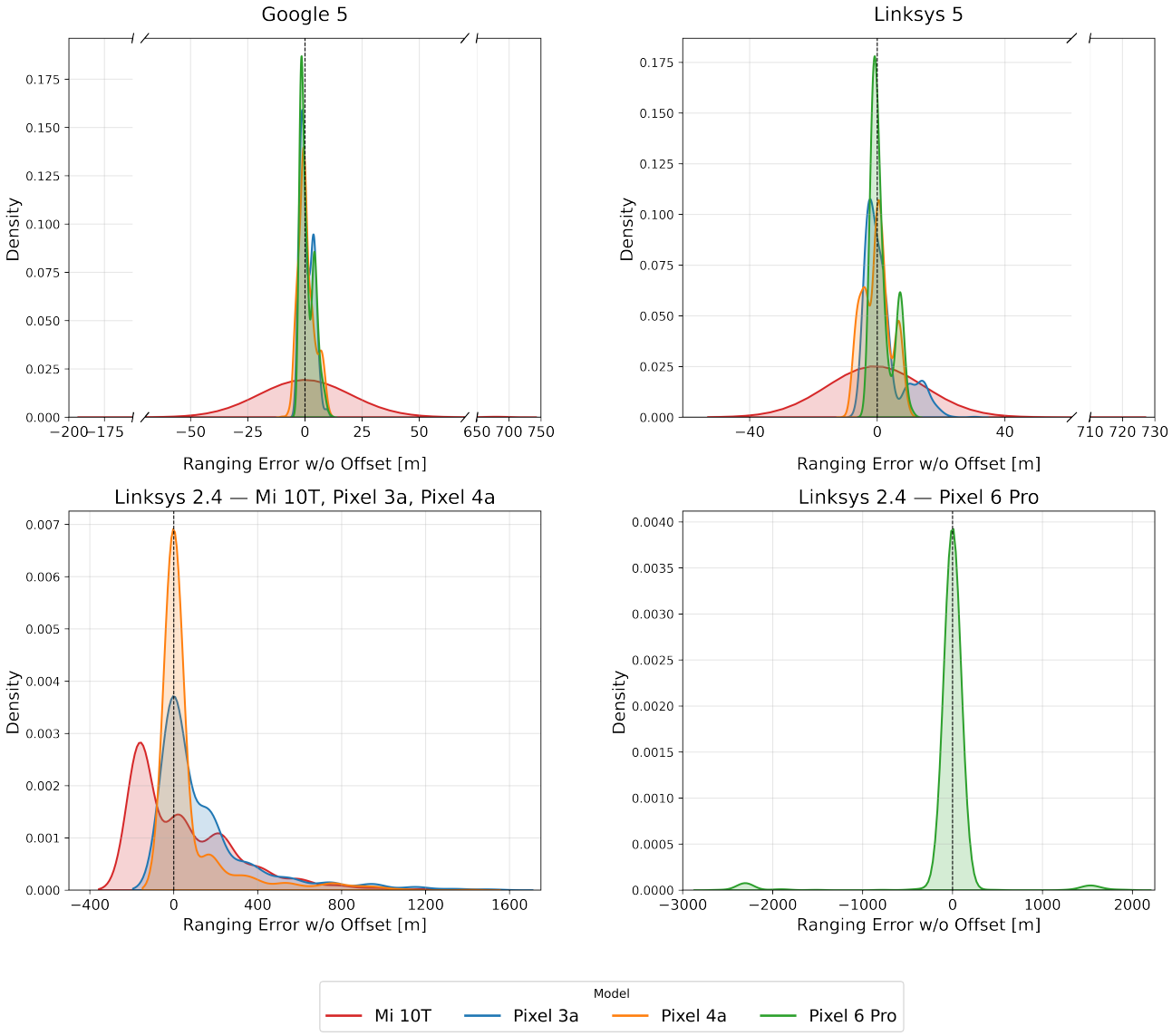


Fig. 5. Probability density function of the residual ranging error (BS=8) for each AP and different UE models.

the median raw ranging error at BS=8, the median residual ranging error is expected to be zero.

The residual error distribution in the 5 GHz band (top-row subplots: Google 5 on the left and Linksys 5 on the right) exhibits a multimodal behavior across all Pixel models. A narrow main mode is present in all Pixels, whereas the Mi 10T (in red) shows a strongly right-skewed, broad Gaussian-like distribution, covering a much wider range of ranging errors. These behaviors align with observations from the regular two-sided procedure [7]. On the other hand, the error distribution when operating with Linksys 2.4 (bottom-row subplots) differs significantly: the Pixel 6 Pro (green, right subplot) exhibits a quasi-symmetric multimodal distribution with a dominant mode and secondary modes that create pronounced right and left tails. The remaining UEs (bottom-left subplot) follow a heavy right-tailed multimodal distribution.

For all Pixel UEs in the 2.4 GHz band, the principal mode (most common value) of the residual ranging error is zero. Similarly, in the 5 GHz channel of any AP, the most common value is very close to zero. For the Mi 10T working with Linksys 2.4, the principal mode lies to the left of the median, while the second mode is near zero, reflecting a heavily right-skewed distribution not observed in the Pixel models.

Overall, the multimodal density curves observed in Fig. 5 may be explained by two primary physical phenomena. First, internal clock synchronization jitter between the MAC and PHY layers on COTS chipsets may cause timestamping lock-ins at integer multiples of the baseband sampling clock tick (e.g., $\Delta t = 12.5$ ns ≈ 3.75 m at 80 MHz), potentially producing discrete, tightly clustered error modes [8]. Second, in corridor environments, slight LOS fading causes the receiver's threshold detector to lock onto early wall or floor reflections,

TABLE IV
STATISTICS OF THE RESIDUAL RANGING ERROR [IN METERS] FOR EACH UE AND AP, WITH BS 8. THE NUMBER OF AVAILABLE SAMPLES IS ALSO GIVEN

AP	UE	Min.	5th Perc	Mean	95th Perc	Max.	STD	RMSE	N. Samples
Linksys 2.4	Mi 10T	-170.38	8.42	52.20	590.03	1,461.56	257.13	262.27	1,200
	Pixel 3a	-8.59	0.38	150.81	756.42	1,525.41	255.56	296.65	1,200
	Pixel 4a	-9.38	0.00	74.07	519.27	1,416.88	191.36	205.12	1,200
	Pixel 6 Pro	-2,587.47	0.17	-26.39	115.57	1,918.90	395.42	396.14	1,194
Linksys 5	Mi 10T	-9.06	0.31	10.37	8.45	683.12	60.63	61.49	1,200
	Pixel 3a	-5.47	0.31	1.69	14.63	30.45	5.93	6.16	1,200
	Pixel 4a	-9.53	0.16	-0.10	7.66	9.84	4.35	4.34	1,199
	Pixel 6 Pro	-3.23	0.13	1.34	8.00	11.04	3.45	3.70	580
Google 5	Mi 10T	-133.75	0.00	12.14	5.07	683.05	82.31	83.17	1,200
	Pixel 3a	-4.44	0.22	0.83	5.63	10.31	2.93	3.04	1,200
	Pixel 4a	-9.75	0.16	0.61	7.97	11.25	3.61	3.66	1,200
	Pixel 6 Pro	-3.95	0.28	1.03	6.71	11.68	3.09	3.25	1,200

shifting t_4 by discrete path-delay increments [2]. Conversely, the continuous, unimodal distribution observed in the Xiaomi Mi 10T suggests that timestamp collection occurs higher up in the MAC/driver layer; software queueing and OS interrupt jitter seem to naturally smooth out discrete physical clock quantization into a continuous, broad error distribution [15].

Table IV complements Fig. 5 by summarizing the main statistics of the residual ranging error for a burst size of 8. The mean residual error is very small compared to the range of errors for all Pixel models when working in the 5 GHz band, which suggests that, after offset correction, there is little systematic bias. Interestingly, although the mean is close to zero for some UE models, the root mean squared error (RMSE) and STD exhibit substantial variability. This confirms that median-centering (i.e., offset correction) effectively compensates for systematic offsets, while **residual errors remain highly dependent on the UE/AP hardware combination**.

The 2.4 GHz measurements reveal a much lower stability than the 5 GHz measurements, with almost two orders of magnitude difference between the STD values observed at 2.4 GHz and 5 GHz for the Pixel models. In some cases, such as the Pixel 6 Pro operating in the 5 GHz band, 90% of samples (from the 5th to the 95th percentile) lie approximately within the same interval as the complete sample range (i.e., the min-max interval). However, in most cases, the maximum residual error is substantially higher than the 95th percentile (e.g., all the UE models with Linksys 2.4), or the minimum residual error is substantially lower than the 5th percentile (e.g., Mi 10T and Pixel 6 Pro with Linksys 2.4). These extreme values represent unfiltered ranging outliers; because the objective of this work is to establish a straightforward empirical baseline, these heavy-tailed artifacts are intentionally retained to expose full operational variability rather than masked via post-processing.

Beyond statistical variance, the complete burst-level failure between specific device pairs, such as the Pixel 6 Pro and the Linksys AP, highlights a **critical vulnerability** in infrastructure-independent RTT: **unstandardized driver-level handling of one-sided ACK frames**. While standard FTM relies on explicit two-sided protocol handshakes, one-sided RTT relies on implicit frame timing at the MAC/PHY boundary. Differences in COTS firmware, such as aggressive power-save state transitions or vendor-specific frame response timeouts, can cause total burst rejection between specific chipset pairs [16]. For real-world IPS deployments, this implies that positioning engines cannot assume universal AP compatibility and must implement opportunistic AP selection or dynamic fallback mechanisms when a target AP repeatedly drops one-sided measurement bursts.

Table IV also shows aberrant RMSE values in the 2.4 GHz band, while RMSE tends to be lower for all Pixel UE models, particularly when working with Google 5 (e.g., RMSE between 3.04 and 3.66 m).

Finally, the last column reports the number of samples obtained for each combination: 1,200 samples corresponds to the case in which all NFD frames are acknowledged (i.e., 200 samples $\times$ 6 RPs). As already shown in Section II-C, the Pixel 6 Pro struggles to operate with Linksys 5. Overall, Google 5 shows the best performance, with the smallest spread and a dominant mode likely close to zero; secondary modes are also near zero.

IV. CONCLUSION

This paper presents an experimental evaluation of one-sided Wi-Fi RTT ranging under controlled LOS conditions, using four commercial Android smartphones and two off-the-shelf APs operating in both the 2.4 GHz and 5 GHz bands. To the best of our knowledge, this is the first study to jointly investigate the impact of burst size, heterogeneous UE/AP hardware combinations, and operating frequency on one-sided Wi-Fi RTT performance.

The collected measurements reveal that one-sided Wi-Fi RTT performance strongly depends on the underlying hardware and software implementations. Significant performance disparities were observed among the tested devices: Google Pixel UEs provided remarkably stable and accurate measurements, whereas the Xiaomi Mi 10T exhibited massive offsets

and continuous variance. **The results are consistent with the hypothesis that the timestamping architecture contributes substantially to ranging stability**. In particular, lower-level timestamping potentially provides more stable ranges, whereas higher-level processing may introduce substantial jitter and large systematic offsets. Furthermore, the operating frequency plays a decisive role. Even for Pixel devices, which avoid extreme offset anomalies, 2.4 GHz operation showed high residual variability (STD $>$ 140 m) due to 20 MHz channel bandwidth constraints. Consequently, this yields a **critical design recommendation**: **5 GHz configurations should be preferred for one-sided Wi-Fi RTT ranging**.

The analysis of burst size (BS) shows that increasing the number of RTT exchanges generally reduces measurement variability, although its impact on the average ranging error is limited. Furthermore, most devices successfully achieve the configured BS, while the Pixel 6 Pro exhibits interoperability issues with one of the tested APs, highlighting the **importance of vendor-specific implementations**.

The raw ranging estimates were found to contain large systematic offsets, whose magnitude depends on the UE/AP/frequency/BS combination. After offset compensation, the residual ranging error exhibits multimodal and heavy-tailed distributions, similar to behaviors previously reported for conventional two-sided Wi-Fi RTT. Nevertheless, Pixel devices operating in the 5 GHz band achieved meter-level ranging accuracy, with RMSE values around 3 m, demonstrating that **one-sided Wi-Fi RTT can provide useful ranging information even in networks lacking FTM-enabled infrastructure**.

Overall, the results confirm the feasibility of infrastructure-independent Wi-Fi RTT ranging while highlighting important operational boundaries related to device interoperability, frequency selection, and residual error variability that must be addressed before large-scale deployment in IPSs.

Future work will focus on developing adaptive, low-complexity outlier detection and mitigation algorithms tailored to heavy-tailed one-sided RTT distributions. Additional experiments involving a broader range of UEs, APs, and propagation conditions, including non-line-of-sight (NLOS) scenarios, will be conducted to further characterize interoperability and multipath degradation. Finally, one-sided Wi-Fi RTT measurements will be integrated into a full indoor positioning engine to evaluate the achievable positioning accuracy and robustness in comparison with conventional two-sided Wi-Fi RTT solutions.

ACKNOWLEDGMENTS

The Article Processing Charges were sponsored by Grant PID2025-173046OB-I00 funded by MICIU/AEI/ 10.13039/501100011033 and by ERDF/EU. This research was partially supported by Grant PID2025-173046OB-I00 and by the Generalitat de Catalunya under Grant 2021-SGR-00594.

REFERENCES

[1] R. Jurdi, H. Chen, Y. Zhu, B. Loong Ng, N. Dawar, C. Zhang, and J. K.-H. Han, "WhereArtThou: A WiFi-RTT-Based Indoor Positioning System," *IEEE Access*, vol. 12, pp. 41 084–41 101, 2024.

[2] C. Ma, B. Wu, S. Poslad, and D. R. Selviah, "Wi-Fi RTT Ranging Performance Characterization and Positioning System Design," *IEEE Transactions on Mobile Computing*, vol. 21, no. 2, pp. 740–756, 2022.

[3] S. Martín-Frechina, E. Dura, I. Miralles, and J. Torres-Sospedra, "From Fingerprinting to Advanced Machine Learning: A Systematic Review of Wi-Fi and BLE-Based Indoor Positioning Systems," *Sensors*, vol. 25, no. 22, 2025. [Online]. Available: https://www.mdpi.com/1424-8220/25/22/6946

[4] IEEE, "IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - 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," 2016, last accessed on June 2024.

[5] M. Orfanos, H. Perakis, V. Gikas, G. Retscher, T. Mpimis, I. Spyropoulou, and V. Papathanasopoulou, "Testing and Evaluation of Wi-Fi RTT Ranging Technology for Personal Mobility Applications," *Sensors*, vol. 23, no. 5, 2023.

[6] K. Kosek-Szott, S. Szott, W. Ciezobka, M. Wojnar, K. Rusek, and J. Segev, "Indoor positioning with Wi-Fi Location: A survey of IEEE 802.11mc/az/bk fine timing measurement research," *Computer Communications*, vol. 247, p. 108400, 2026. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366425003573

[7] E. Zola and I. Martin-Escalona, "Assessing the Impact of the Burst Size in the FTM Ranging Procedure in COTS Wi-Fi Devices," *Computer Communications*, vol. 229, p. 107980, 2025.

[8] B. K. P. Horn, "Indoor Localization Using Uncooperative Wi-Fi Access Points," *Sensors*, vol. 22, no. 8, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/8/3091

[9] I. Martin-Escalona and E. Zola, "Ranging Estimation Error in WiFi Devices Running IEEE 802.11mc," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*. IEEE, Dec. 2020, p. 1–7.

[10] Google, "Android WifiRttScan Sample," Available online: github.com/android/connectivity-samples/tree/main/WifiRttScan, this repository was archived by the owner on Jul 10, 2025. It is now read-only.

[11] Google-LLC, "Google WiFi AP," Available online: store.google.com/product/google_wifi, (accessed on May 11, 2023).

[12] Linksys, "Linksys Velop Intelligent Mesh WiFi System, Tri-Band," Available online: www.linksys.com/us/p/P-WHW0303, (accessed on May 11, 2023).

[13] Android-Developers, "Wi-Fi location: ranging with RTT," Available online: developer.android.com/guide/topics/connectivity/wifi-rtt#supported-phones, (Last updated 2026-05-12).

[14] B. K. Horn, "Doubling the Accuracy of Indoor Positioning: Frequency Diversity," *Sensors*, vol. 20, no. 5, p. 1489, 2020.

[15] A. Mahmood, R. Exel, and T. Sauter, "Delay and Jitter Characterization for Software-Based Clock Synchronization Over WLAN Using PTP," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1198–1206, 2014.

[16] C. Gentner, M. Ulmschneider, I. Kuehner, and A. Dammann, "WiFi-RTT Indoor Positioning," in *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2020, pp. 1029–1035.