

Fundamental Evaluation of IEEE 802.11az Wi-Fi RTT-based Ranging and Positioning

Haruki Naiki

Dept. Electrical and Electronic Engineering
Meijo University
Nagoya, Japan
263427037@ccmailg.meijo-u.ac.jp

Kentaro Kobayashi

Dept. Electrical and Electronic Engineering
Meijo University
Nagoya, Japan
kkobaysh@meijo-u.ac.jp

Abstract—With the advancement of navigation technologies, highly accurate and versatile indoor positioning technologies are increasingly required. Since GNSS, which is widely used outdoors, has difficulty providing accurate positioning indoors, IEEE 802.11az has emerged as an alternative Wi-Fi-based ranging protocol. However, the number of compatible devices remains limited, and the positioning performance of actual devices has not been sufficiently evaluated. In this study, ranging experiments of the conventional IEEE 802.11mc and the new IEEE 802.11az protocols were conducted using a stationary terminal and a Wi-Fi access point in a line-of-sight (LOS) environment to clarify the impact of these protocol revisions on ranging performance. Furthermore, positioning experiments were conducted using four access points and a single terminal to evaluate the positioning accuracy of IEEE 802.11az Wi-Fi RTT.

Keywords—Wi-Fi RTT, IEEE 802.11az, IEEE 802.11mc, Ranging, Positioning

I. INTRODUCTION

Accurate positioning is essential for autonomous navigation and control of robots and drones. While GNSS-based positioning is widely used in outdoor environments, achieving stable positioning indoors is difficult due to the blocking of radio waves by obstacles such as walls and ceilings. To address this issue, various indoor positioning methods have been proposed, including those based on geomagnetism, Bluetooth Low Energy (BLE) beacons, and Wi-Fi access points (APs). However, geomagnetic positioning requires prior mapping of the magnetic field in the target environment and is susceptible to interference from metallic objects such as vehicles and railways. In addition, methods based on the Received Signal Strength Indicator (RSSI) of BLE beacons or Wi-Fi signals are highly sensitive to environmental factors. Obstacles can cause signal attenuation, reflection, and absorption, resulting in fluctuations in RSSI and making highly accurate positioning difficult.

In contrast, Wi-Fi Round Trip Time (RTT)-based positioning estimates distances from the propagation time of radio signals and is expected to provide higher ranging accuracy than RSSI-based positioning, which is vulnerable to

amplitude fluctuations. Furthermore, since existing Wi-Fi APs can be utilized for positioning, deployment costs can be reduced without requiring additional infrastructure.

IEEE 802.11az [1] is a standard developed to enhance Wi-Fi RTT to improve ranging accuracy and security. It revises IEEE 802.11mc [2], a Wi-Fi RTT standard established in 2016, and improves ranging performance by redesigning the PHY and MAC layer specifications while maintaining its fundamental principles.

Several studies have reported the positioning performance of IEEE 802.11az in simulation environments [3], [4]. However, evaluations in real environments have been limited to point-to-point ranging experiments [5], and the lack of detailed descriptions of the devices used makes reproduction difficult. Moreover, experimental evaluations of positioning accuracy using multiple APs have not been sufficiently investigated.

In this study, toward the development of an IEEE 802.11az positioning system, we evaluate the accuracy of point-to-point ranging between a smartphone and an AP, as well as the positioning accuracy achieved using four APs. Furthermore, by comparing IEEE 802.11az with IEEE 802.11mc under identical conditions, we clarify the fundamental characteristics and challenges of IEEE 802.11az in ranging and positioning.

II. POSITIONING SYSTEM

A. Wi-Fi RTT-based Ranging

Wi-Fi RTT is a ranging method that estimates the distance between a terminal and an AP using the RTT of Wi-Fi signals and their propagation speed. The timing chart of Wi-Fi RTT is shown in Fig. 1.

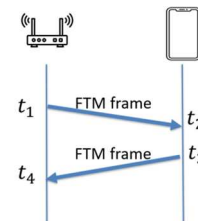


Fig. 1. Timing chart of Wi-Fi RTT.

A part of this research was supported by the Hibi Science Foundation, Japan.

The ranging procedure is as follows. First, the terminal sends a ranging request to the AP, after which the AP transmits an Acknowledgement (ACK) frame to the terminal. Subsequently, the AP transmits a Fine Time Measurement (FTM) frame containing the timestamp t_1 to the terminal at time t_1 . After receiving the FTM frame at time t_2 , the terminal sends an ACK frame to the AP at time t_3 . The AP then receives the ACK frame at time t_4 . Finally, the AP transmits another FTM frame containing the transmission timestamp t_1 of the initial FTM frame and the reception timestamp t_4 of the ACK frame to the terminal.

Based on these timestamps, the RTT between the AP and the terminal can be obtained. By multiplying half of the RTT by the propagation speed of radio waves (the speed of light, c), the distance d between the terminal and the AP is calculated as follows:

$$d = \frac{1}{2}((t_4 - t_1) - (t_3 - t_2)) \times c. \quad (1)$$

When the burst size is set to N_B , the sequence of FTM frame exchanges is repeated N_B times. For each FTM exchange, the transmission timestamps $(t_1, t_3)^{(n)}$, and the reception timestamps $(t_2, t_4)^{(n)}$, are substituted into (1) to calculate the ranging value $d^{(n)}$. Statistical processing is then applied to the set of ranging values $\{d^{(1)}, d^{(2)}, d^{(N_B)}\}$ to produce the final ranging result.

B. IEEE 802.11mc

IEEE 802.11mc does not employ a dedicated frame structure for FTM frames; instead, it uses frame structures that are largely identical to those used for data transmission. As a result, timestamps are acquired not at the actual signal arrival time at the PHY layer, but at the time when the frame is recognized by the MAC layer. Since frame recognition at the MAC layer requires processing such as frame synchronization, header decoding, and error detection, the exact signal arrival time cannot be accurately determined due to the associated processing delay.

In addition, IEEE 802.11mc cannot fully exploit the available wireless channel resources and is susceptible to multipath effects. When a device transmitting FTM frames is equipped with multiple transmit antennas, FTM transmission is performed using only a single antenna because IEEE 802.11mc does not support MIMO. Consequently, the ranging performance becomes more vulnerable to channel blockage caused by obstacles and signal reflections. Regarding the operating frequency bands, IEEE 802.11mc supports only the 2.4 GHz and 5 GHz bands. Therefore, the maximum available channel bandwidth is limited to 80 MHz.

C. IEEE 802.11az

IEEE 802.11az is a protocol that revises IEEE 802.11mc. Two ranging methods, namely Non-Trigger-Based (NTB) ranging and Trigger-Based (TB) ranging, are newly defined in IEEE 802.11az. Since TB ranging is not employed in this study, the following description focuses exclusively on the specifications of NTB ranging.

Unlike IEEE 802.11mc, the FTM frame in IEEE 802.11az is redefined as a Null Data Packet (NDP) rather than using the conventional frame structure employed for data communication. The NDP frame is derived from the frame used in IEEE 802.11mc by removing the data portion including the MAC header, thereby reducing unnecessary MAC-layer processing that is not required for ranging.

In addition, IEEE 802.11az supports MIMO to fully utilize the antennas equipped on a device. Therefore, the NDP frame is designed to include Long Training Fields (LTFs), which are used for channel estimation, and the number of LTFs is determined according to the number of transmit antennas. Furthermore, the supported operating frequency range has been extended to include the 6 GHz band, enabling the utilization of channel bandwidths up to 160 MHz. Note that the 6 GHz band is not evaluated in this study.

D. Positioning Based on Maximum Likelihood Estimation

Four APs and a single terminal are deployed, and the ranging values obtained using the Wi-Fi RTT ranging described in II-A are utilized for the self-position estimation of the terminal. In this study, maximum likelihood estimation is employed as the positioning method.

Let the known coordinates of the i -th AP be denoted by $\mathbf{a}_i = (a_{xi}, a_{yi}, a_{zi})$, and let the unknown coordinates of the terminal be denoted by $\mathbf{X} = (x, y, z)$. The ranging value obtained from the i -th AP is represented by d_i . Based on the Pythagorean theorem, the distance D_i between the terminal and the i -th AP is given by

$$D_i^2 = \|\mathbf{a}_i - \mathbf{X}\|^2 = (a_{xi} - x)^2 + (a_{yi} - y)^2 + (a_{zi} - z)^2. \quad (2)$$

Let the ranging error between the terminal and the i -th AP be denoted by ϵ_i .

$$\epsilon_i = d_i - \sqrt{(a_{xi} - x)^2 + (a_{yi} - y)^2 + (a_{zi} - z)^2} \quad (3)$$

Under the assumption that the ranging error follow a Gaussian distribution $\mathcal{N}(0, \sigma^2)$, the probability density function corresponding to the i -th ranging value is considered. For a terminal located at (x, y, z) , the probability density function $p(d_i|x, y, z)$ is expressed as

$$p(d_i|x, y, z) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{\left(d_i - \sqrt{(a_{xi} - x)^2 + (a_{yi} - y)^2 + (a_{zi} - z)^2}\right)^2}{2\sigma^2}\right). \quad (4)$$

The overall likelihood function $L(x, y, z)$ is given by the product of the N probability density functions as

$$L(x, y, z) = \prod_{i=1}^N p(d_i|x, y, z). \quad (5)$$

To maximize (5), (6) must be minimized.

$$f(x, y, z) = \sum_{i=1}^N \left(d_i - \sqrt{(a_{xi} - x)^2 + (a_{yi} - y)^2 + (a_{zi} - z)^2}\right)^2 \quad (6)$$

Therefore, the values of x , y , and z that minimize (6) are obtained as the estimated coordinates of the terminal.

III. EXPERIMENTAL EVALUATION OF RANGING

A. Experimental Ranging Method

An HPE Aruba Networking AP-735 was used as the AP, and a Google Pixel 10 Pro XL (OS: Android 16) was used as the terminal. The antenna configurations of both the AP and the terminal were 2×2 MIMO.

First, ranging measurements were conducted for various terminal-AP distances using the IEEE 802.11az and IEEE 802.11mc protocols. The experiments were performed in an unoccupied corridor of the university under line-of-sight (LOS) conditions. The AP and the terminal were placed on tripods at a height of 1.1 m, as shown in Fig. 2. The operating frequency band was set to 5 GHz, the channel bandwidth was 80 MHz, and the burst size was set to 8. For each distance, ranging requests were continuously transmitted from the terminal using the IEEE 802.11az protocol until 100 successful ranging results were obtained. The protocol was then automatically switched to IEEE 802.11mc, and the same procedure was repeated. The terminal-AP distance was varied from 2.0 m to 20.0 m in increments of 2.0 m.

Next, the experimental environment was changed to a laboratory under LOS conditions, as shown in Fig. 3. Following the same procedure as in the previous experiment, ranging measurements were conducted for each protocol while varying the channel bandwidth. The operating frequency band was set to 5 GHz, the terminal-AP distance was fixed at 6.0 m, and the burst size was set to 8. The channel bandwidth was varied among 20 MHz, 40 MHz, and 80 MHz in the 5 GHz band.

In addition, to evaluate the impact of the burst size, the processing time required for ranging was measured for each protocol. Here, the processing time is defined as the duration from the initiation of the ranging request to the acquisition of the final measurement result. These measurements were conducted in the same laboratory environment. The operating frequency band was 5 GHz, the channel bandwidth was 80 MHz, and the terminal-AP distance was fixed at 6.0 m. The burst size was varied as 2, 4, 8, 16, and 31.

B. Evaluation of Terminal-AP Distance Impact

The results of distance measurements obtained by varying the terminal-AP distance are shown in Fig. 4. The ranging values for each protocol are plotted for distances from 2.0 m to 20.0 m, along with a reference line indicating the true distance. To improve visibility, Fig. 4 is divided into two parts: one covering distances from 2.0 m to 10.0 m, and the other covering distances from 12.0 m to 20.0 m. The violin plots visualize the probability density of the measured distances.

Focusing on the distribution shapes, IEEE 802.11mc exhibits bimodal distributions at 2.0 m, 10.0 m, 14.0 m, and 16.0 m, and several outliers are also observed. In contrast, IEEE 802.11az shows unimodal distributions at all measured distances. This suggests that IEEE 802.11az is less susceptible to the effects of reflected signals due to its MIMO-based signal processing.



Fig. 2. Ranging environment. (corridor)



Fig. 3. Ranging environment. (laboratory)

Consequently, the ranging stability of IEEE 802.11az outperforms that of IEEE 802.11mc. The maximum standard deviation for IEEE 802.11az is 0.099 m (at 12.0 m), which is less than half of the 0.258 m observed for IEEE 802.11mc (at 16.0 m). Similarly, the maximum root mean squared error (RMSE) for IEEE 802.11az is 0.847 m (at 16.0 m), compared to 2.294 m for IEEE 802.11mc (at 6.0 m).

C. Evaluation of Channel Bandwidth Impact

The results of distance measurements obtained by varying the channel bandwidth are shown in Fig. 5, where the ranging values obtained for each protocol are presented as violin plots.

Focusing on the distribution shapes, the ranging values are broadly dispersed at 20 MHz, whereas the distributions become more concentrated as the channel bandwidth increases. This improvement is attributed to the enhanced time resolution in the arrival time estimation.

In terms of protocol comparison, the distribution of IEEE 802.11az is consistently closer to the true distance compared to that of IEEE 802.11mc. IEEE 802.11az exhibits a smaller positive bias, with the gap between the two protocols ranging from approximately 0.3 m to 2.2 m across all bandwidth settings. This trend suggests that differences in the protocol structure affect the measured values.

One possible reason is the difference in the FTM frame structure described in II-C. In IEEE 802.11az, the data frame portion processed at the MAC layer is removed from the FTM frame format defined in IEEE 802.11mc. Consequently, frame processing is handled at the PHY layer, and the uncertainty caused by the MAC-layer processing delay is eliminated. This structural optimization reduces the error from the true reception time in IEEE 802.11az.

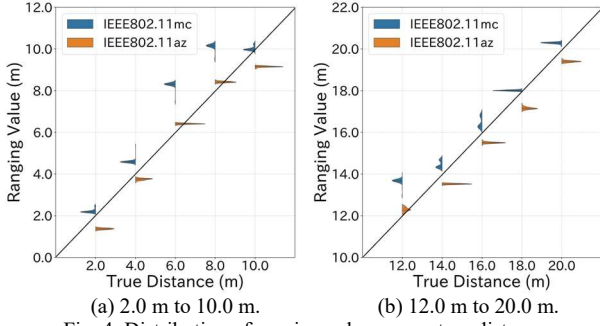


Fig. 4. Distribution of ranging value versus true distance.

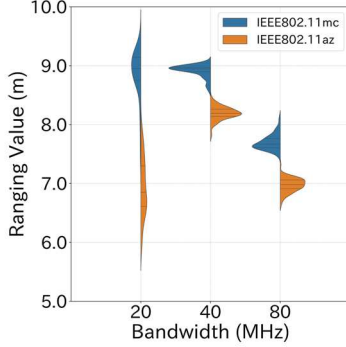


Fig. 5. Distribution of ranging value versus channel bandwidth.

D. Evaluation of Burst Size Impact

The results of distance measurements obtained by varying the burst size are shown in Fig. 6, where the processing time and the ranging values obtained for each protocol are presented as violin plots.

Focusing on the distribution of processing time shown in Fig. 6(a), IEEE 802.11az shows an increasing trend for burst sizes of 2, 4, and 8, while no significant change is observed beyond a burst size of 8. In contrast, IEEE 802.11mc exhibits a nearly constant processing time across all burst sizes. In terms of average processing time, IEEE 802.11az and IEEE 802.11mc are approximately 1.3 s and 0.3 s, respectively.

Regarding the distribution of ranging values shown in Fig. 6(b), no clear dependency on the burst size is observed. To investigate this further, the maximum number of successful FTM frame exchanges among 100 samples for each burst size was evaluated, as shown in Table I, where the FTM frame exchange success rate is defined as the ratio of successful exchanges to the total number of attempted exchanges.

As a result, for IEEE 802.11az, even when the burst size was set to 8 or higher, the maximum number of successful FTM frame exchanges remained constant at four, and no cases with five or more successful exchanges were observed in any of the experiments. Since the burst size is configured by the terminal, this suggests that the actual number of FTM frame exchanges was limited by the AP implementation.

IV. EXPERIMENTAL EVALUATION OF POSITIONING

A. Experimental Positioning Method

Four HPE Aruba Networking AP-735 units were used as APs, and a single terminal (Google Pixel 10 Pro XL) was

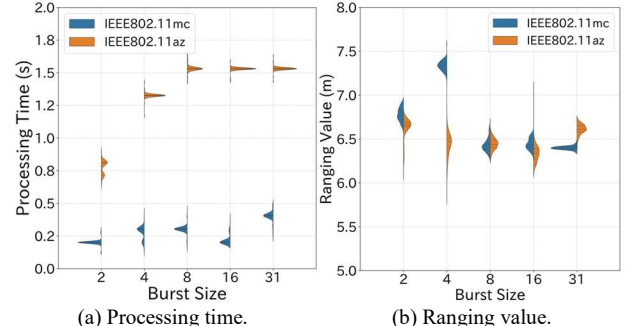


Fig. 6. Performance evaluation with varying burst size.

TABLE I. FTM FRAME EXCHANGE SUCCESS RATE

Burst Size	2	4	8	16	31
802.11az	2/2	4/4	4/8	4/16	4/31
802.11mc	2/2	4/4	8/8	16/16	25/31

placed as shown in Fig. 7. The terminal sequentially transmitted ranging requests to each of the four APs. The burst size was set to 8, and the procedure was repeated until 100 ranging results were collected for each AP. After that, the same measurements were repeated 100 times for each protocol. The positioning procedure was performed by estimating the terminal position using the distances to the four APs, and this process was repeated for each measurement. The ranging values were used as inputs in (6), and the terminal position was estimated using the maximum likelihood estimation described in II-D.

The experiments were conducted for 20 MHz, 40 MHz, and 80 MHz in the 5 GHz band, and ranging values were obtained under each condition.

B. Evaluation of Positioning Accuracy

Fig. 8 shows the resulting ranging distributions, where the red markers indicate the ground-truth distances from the terminal to each AP. As shown in Fig. 9, the positioning errors are represented as violin plots. Here, the positioning error is defined as the Euclidean distance between the estimated position (x, y, z) and the ground-truth position $(0.000, 0.000, 1.070)$.

Comparing the distribution shapes of the protocols in Fig. 9, IEEE 802.11mc exhibits two peaks in the range of 7 m to 9 m and 9 m to 10 m (at 40 MHz), whereas IEEE 802.11az shows one peak in the range of 5 m to 6 m (at 40 MHz). IEEE 802.11mc exhibits a multimodal distribution, whereas IEEE 802.11az shows a unimodal distribution. Regarding the positioning error across channel bandwidths, IEEE 802.11az achieves a maximum standard deviation of 0.291 m (at 20 MHz), whereas IEEE 802.11mc reaches 1.05 m (at 40 MHz). In terms of RMSE, IEEE 802.11az attains a maximum of 5.26 m (at 40 MHz), while IEEE 802.11mc reaches 8.18 m (at 20 MHz).

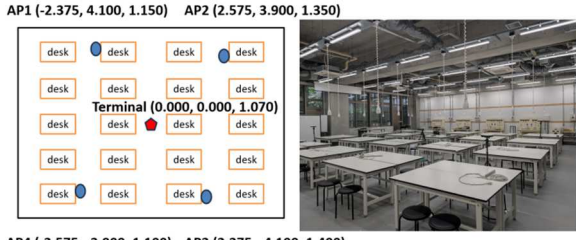


Fig. 7. Positioning environment.

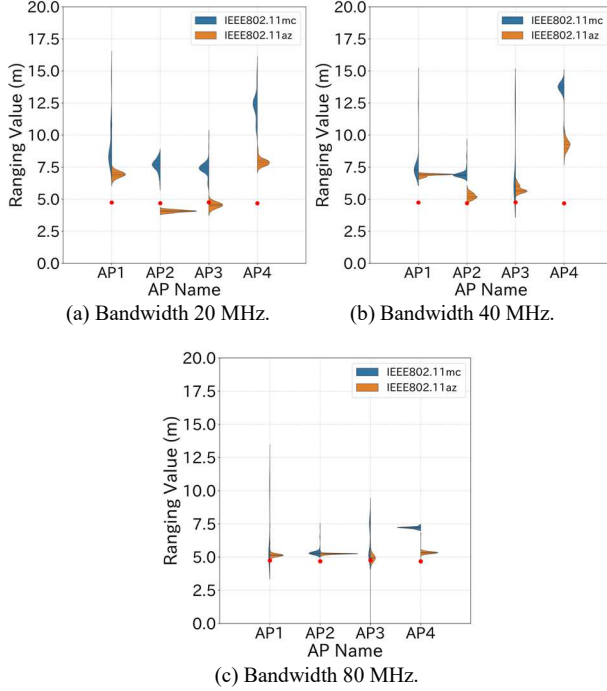


Fig. 8. Ranging value data used for positioning estimation.

The narrower distribution of positioning errors observed in IEEE 802.11az can be attributed to the smaller variability in its ranging values. As shown in Fig. 8, IEEE 802.11az measurements are concentrated within 3 m, indicating a smaller standard deviation compared to IEEE 802.11mc. Since the objective function used in the maximum likelihood estimation is defined as the sum of squared ranging errors, the estimator is sensitive to outliers. For this reason, the presence of a larger number of outliers in IEEE 802.11mc leads to a wider distribution of positioning errors.

V. CONCLUSION

In this study, we conducted experimental evaluations of IEEE 802.11az and IEEE 802.11mc under single-link (1-to-1) ranging and multi-link (1-to-4) positioning scenarios.

In the single-link ranging experiments under LOS static conditions, IEEE 802.11az demonstrated superior ranging accuracy to IEEE 802.11mc. With a channel bandwidth of 80 MHz, IEEE 802.11az achieved a maximum standard deviation of 0.099 m and a maximum RMSE of 0.847 m, whereas IEEE 802.11mc reached 0.258 m and 2.294 m,

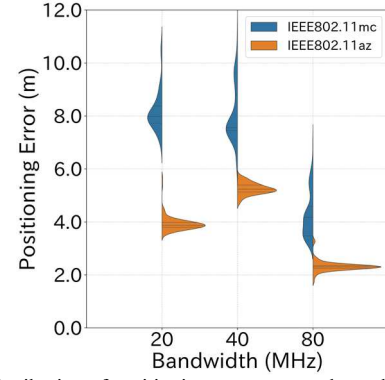


Fig. 9. Distribution of positioning error versus channel bandwidth.

respectively. While increasing the channel bandwidth improved the standard deviation of both protocols, the ranging distribution of IEEE 802.11mc tended to become widely dispersed depending on the measurement conditions.

Similarly, in the positioning experiments, IEEE 802.11az achieved superior accuracy compared to IEEE 802.11mc. Specifically, the standard deviation of the positioning error was 0.291 m for IEEE 802.11az and 1.05 m for IEEE 802.11mc, while the RMSE was 5.26 m for IEEE 802.11az and 8.18 m for IEEE 802.11mc.

However, IEEE 802.11az faces a challenge regarding the processing time. For burst sizes of 4 and above, the processing time per ranging operation was more than 1 s longer than that of IEEE 802.11mc. Furthermore, when the burst size was increased from 2 to 31, the peak of the processing time distribution increased from approximately 0.8 s to 1.5 s, without any noticeable improvement in ranging accuracy. These results confirm that while IEEE 802.11az provides higher ranging and positioning accuracy, its average processing time increases by more than 1 s compared to IEEE 802.11mc, representing a nearly fourfold increase that degrades system responsiveness.

REFERENCES

- [1] IEEE Std 802.11az-2022: Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Enhancements for Positioning, 2022.
- [2] IEEE Std 802.11-2016 Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, pp. 636–638, 2016.
- [3] A. Famili, T. Atalay, and A. Stavrou, “Unlocking the Potential of IEEE 802.11az: A Deep Dive into Ranging Capabilities,” *Proc. 2025 Computing, Networking and Communications: Wireless Communications*, pp. 764–769, Feb. 2025.
- [4] N. N. Tung, T. Huynh-The, and Q.-N. T. Tran, “Optimized Deep Networks for Indoor Position and Localization Based on IEEE P802.11az,” *Proc. 2024 Int. Conf. Advance Technologies for Communications*, pp. 672–677, Oct. 2024.
- [5] G. Rajendran, K. Sharma, V. Chetlapalli, and J. Parekh, “Performance comparison of 802.11mc and 802.11az Wi-Fi Fine Time Measurement protocols,” *Proc. 2026 18th Int. Conf. COMMUNICATION SYSTEMS AND NETWORKS*, pp. 871–876, Jan. 2026.