

# IEEE 802.11az Indoor Positioning with mmWave

Pablo Picazo-Martínez, Carlos Barroso-Fernández, Jorge Martín-Pérez,  
Milan Groshev and Antonio de la Oliva

**Abstract**—Last years we have witnessed the uprising of location-based applications, which depend on the device’s capabilities to accurately obtain their position. IEEE 802.11, foretelling the need for such applications, started the IEEE 802.11az work on Next Generation Positioning. Although this standard provides positioning enhancements for sub-6 GHz and mmWave bands, high accuracy in the order of centimeters can only be obtained in the latter band, thanks to the high temporal resolution from the multi-GHz bandwidth. This work presents the new techniques provided by IEEE 802.11az for enhanced secured positioning in the mmWave band. Additionally, this paper assesses 802.11az mmWave accuracy using a novel trigonometry solution, compares it with advanced positioning solutions, and identifies open research challenges.

**Index Terms**—IEEE 802.11 standard, Next Generation Positioning, FTM, EDMG, mmWave

## I. INTRODUCTION

With the advance of new services requiring precise knowledge of location such as asset tracking, factory automation, or autonomous robots; precise localization and positioning are demanded from local and personal wireless technologies [1]. While the current sub-6 GHz WLANs can achieve a positioning accuracy of tens of meters to tens of centimeters [2], the 60 GHz WLAN with its high

The authors are with the Department of Telematics Engineering, Universidad Carlos III de Madrid; and Departamento de Ingeniería de Sistemas Telemáticos, Universidad Politécnica de Madrid. E-mail: {papicazo, cbarroso, mgroshev}@pa.uc3m.es, jorge.martin.perez@upm.es, aoliva@it.uc3m.es.

This work has been partially funded by the European Union’s Horizon Europe research and innovation programme under grant agreement No 101095759 (Hexa-X-II), the Spanish Ministry of Economic Affairs and Digital Transformation and the European Union-NextGenerationEU through the UNICO 5G I+D 6G-EDGEDT and Remote Driver (TSI-065100-2022-003), and the Spanish Ministry of Economy and Competitiveness & and the Spanish Ministry of Science and Innovation through ECTICS project (PID2019-105257RB-C21).

©2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new or redistribution to servers or lists, or reuse of any copyrighted component of this work in other work

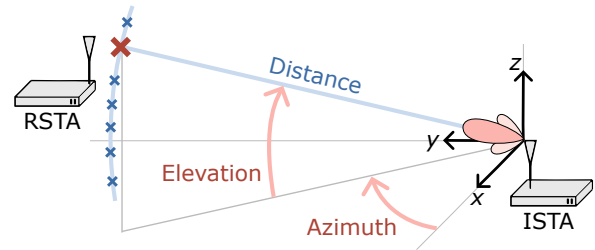


Fig. 1. Legacy positioning in 802.11 only knew the distance between devices, thus, there are many feasible locations (blue markers). 802.11az uses mmWave beamforming to obtain the azimuth and elevation between devices, hence, the exact location (red marker).

temporal resolution from the multi-GHz bandwidth can achieve centimeter positioning accuracy, not achievable in lower bands. The position accuracy can be further enhanced through the use of wider bandwidths, as currently being explored in IEEE 802.11bk task group.

Although researchers have already validated [3], [4] the centimeter accuracy achievable using mmWave beamforming – see<sup>1</sup> Fig. 1, mmWave positioning in 802.11 still faces several challenges, solved in 802.11az [5]:

- (i) mmWave is highly directive and the signal path may differ in the estimation of the distance between Station (STA)s and the angle (elevation and azimuth) of the signal (see Fig. 1). To overcome such problem, 802.11az includes angle and estimations in FTM exchanges.
- (ii) The high-frequency of mmWave signals results in increased signal attenuation, and Non Line Of Sight (NLOS) propagation complicates the positioning accuracy. To enhance NLOS positioning accuracy, 802.11az presents the Line Of Sight (LOS) assessment procedure.
- (iii) The positioning information is not ciphered and malicious stations may know the location of a user. This issue is solved in 802.11az by cipher-

<sup>1</sup>In the paper we use blue color for legacy features, purple for extended features, and red color for new 802.11az features.



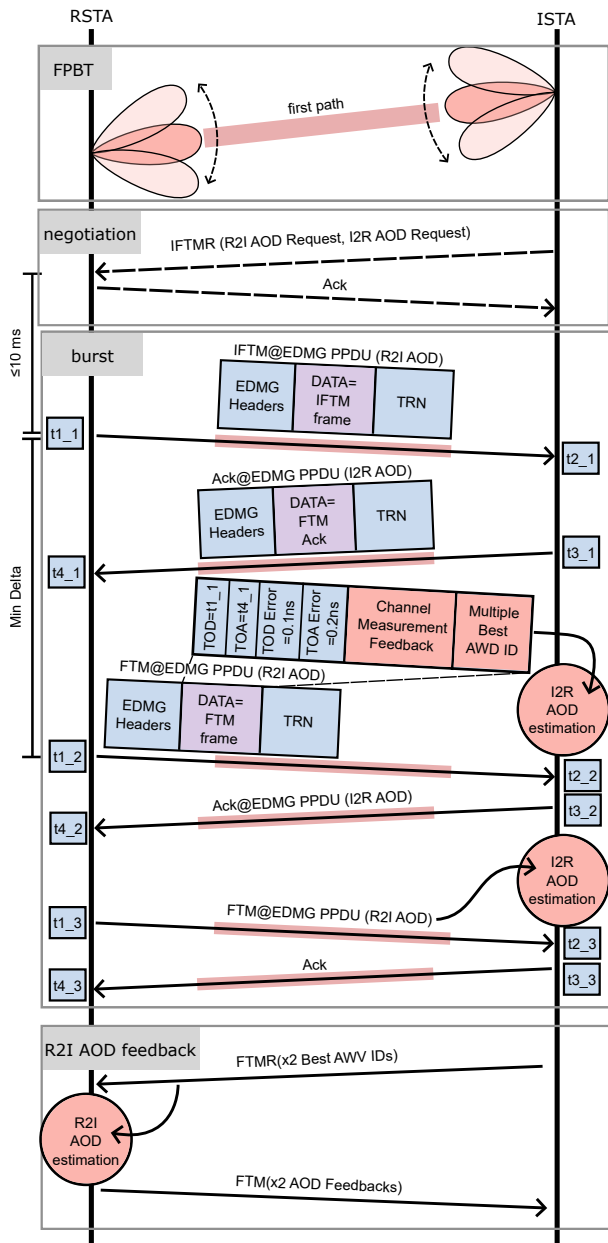


Fig. 3. FTM session over EDMG with FPBT, I2R and R2I AOD measurements. The illustration highlights legacy (blue), modified (purple), and new (red) features from 802.11az.

The EDMG PPDU contains a TRN field with Golay sequences used for channel estimations. In particular, the TRN field carries two complementary Golay sequences  $G_a$  and  $G_b$  that allow reconstructing an accurate estimation of the Channel Impulse Response (CIR). Complementary Golay sequences are binary sequences known by the ISTA and RSTA whose autocorrelations sum up a delta function – see [10] for further details. Consequently (i) correlating the sequence received by the antenna  $G_a'$  with the original sequence  $G_a$  ( $G_b$  with  $G_b'$ ,

respectively); and (ii) summing up the correlation of both sequences results into an accurate estimation of the CIR included within the Channel Measurement Feedback – see Fig. 2 (bottom right).

The channel and angle estimations obtained with TRN are carried in the FTM frames. In particular, the 802.11az amendment has extended the FTM frames to carry the TRN Channel Measurements associated to the AWD, angle estimations, and LOS likelihood – see Fig. 2 red fields. These new fields are complemented with legacy timestamps, localization and synchronization information – blue color in Fig. 2 – to obtain accurate positioning.

### C. Negotiating FTM sessions over EDMG

Before the FTM negotiation, EDMG STAs can find the first path among them through the FPBT procedure – see Fig. 3. Then, both negotiate parameters as the session duration or the number of FTM bursts within a session.

The negotiation starts with the exchange of an Initial FTM Request (IFTMR) where the ISTA proposes, e.g., an EDMG FTM session over the first path with one burst and AOD estimations – as in Fig. 3. Additionally, the ISTA may propose a secure exchange using a specific bandwidth between 2.16 and 8.64 GHz.

It is up to the RSTA to decide whether it accepts the proposed FTM parameters, or it renegotiates them. In case the RSTA accepts the parameters of the received IFTMR, it sends an Acknowledgement (ACK) followed by an Initial FTM (IFTM) frame in less than 10 ms.

The negotiation fails in case the RSTA does not reply with an ACK or the IFTM frame reports that the FTM session cannot start, i.e. RSTA is not capable of satisfying the proposed parameters.

### D. FTM measurement exchange over EDMG

After a successful negotiation, STAs start an FTM session to perform distance and angle measurements. Each session consists of bursts with multiple exchanges of FTM frames encapsulated in EDMG PPDUs. Fig. 3 illustrates an FTM session consisting of a single burst of three FTM and ACK exchanges.

In every exchange the STAs timestamp the Time of Departure (TOD) and Time of Arrival (TOA) of the sent and received frames, respectively. As a result, it is possible to estimate the distance in the

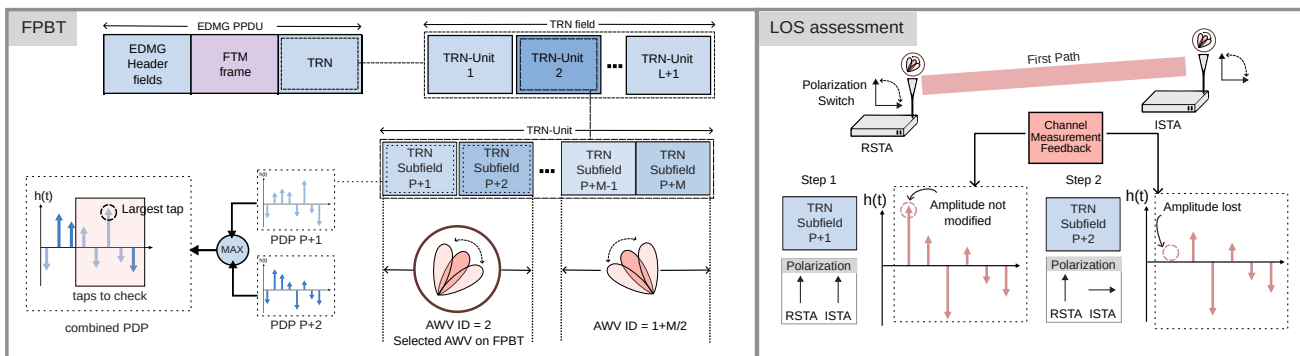


Fig. 4. 802.11az finds the first path sweeping the mmWave beam during the transmission of EDMG TRN Subfields (left). Then, STAs change their mmWave antenna polarization to tell whether they are at LOS by checking the Channel Measurements (right).

first exchange by multiplying the speed of light by the corresponding Round Trip Time (RTT) ( $RTT_1$ ). Fig. 3 illustrates in blue boxes the timestamps used in the RTT estimation.

However, the real time at which frames depart and arrive may differ with the respective timestamps. For example, an IFTM frame may have departed at nanosecond 1 ns, whilst the clock timestamp may be  $t_{1\_1} = 1.1$  ns – thus, the TOD Error of 0.1 ns shown in Fig. 2. Due to the speed of light, the timestamp error of 0.1 ns would result in a distance estimation error of 3 cm. Hence, FTM should obtain distance estimations checking the exchange whose timestamps had least error.

To derive angle estimations within a burst, the STAs compute channel measurements using the EDMG TRN fields. Additionally, STAs change their AWW, to try out multiple setups in the angle estimations. Fig. 3 exemplifies how the initiator estimates the departure angle using the channel measurements and best AWW reported by the responder in the FTM frame – see the first I2R AOD estimation in Fig. 3.

In an FTM session it is possible to drive multiple Initiator-to-Responder (I2R) AOD estimations during the burst – two estimations in Fig. 3 example. But in the case of Responder-to-Initiator (R2I) AOD, 802.11az specifies that the estimations are done once the burst finishes. Specifically, the initiator exchanges the best AWW setups perceived during the burst so the responder can estimate its AOD – see Fig. 3. Finally, the responder sends back to the initiator the two angle estimations.

### III. LOS ASSESSMENT OVER FIRST PATH

802.11az uses FPBT to determine the best path between two STAs and LOS assessment to deter-

mine if that path suffers or not from reflections. Both FPBT and LOS are essential procedures for high accuracy in mmWave.

#### A. First Path Beamforming Training (FPBT)

In the FPBT procedure, the STAs try different mmWave antenna configurations until the beam points to the first path. In particular, the STAs sweep over multiple AWW configurations and select the best one – see Fig. 4 (left). In the following, we detail the FPBT procedure presenting (i) the EDMG TRN fields; and (ii) the AWW sweep procedure.

The EDMG PPDU contains the TRN field that is used to perform channel estimations in the FPBT procedure. The TRN field contains  $L+1$  TRN-Units – see Fig. 4 (left). Every TRN-Unit contains  $P+M$  TRN Subfields that are filled with Golay sequences. The transmission of the Golay sequence results in a Power Delay Profile (PDP) that measures the in-phase, quadrature and SNR of each tap – see the PDPs of TRN Subfields  $P+1$  and  $P+2$  in Fig. 4 (left).

The AWW sweep procedure changes the AWW after the transmission of a group of TRN Subfields – e.g., after a group of two in Fig. 4 (left). Then, the STA combines the PDPs of each TRN Subfield in the group, and selects the highest amplitude taps. The quality of the combined PDP is measured by checking the taps near the one with highest amplitude – see Fig. 4 (left). Finally, the STA compares the combined PDPs in the TRN field, and selects the best AWW – which points to the first path.

#### B. Line Of Sight (LOS) Assessment

Once FPBT determines the best AWW, the ISTA initiates an FTM LOS assessment exchange. In the



exchange the STAs alternate the antenna polarization to determine whether the first path is at LOS. The change of polarization is perceived in the taps of the received signal, whose values are reported as a list of in-phase and quadrature (I/Q) components within the Channel Measurement Feedback.

The LOS assessment compares the signal taps of the received TRN Subfields P+1 and P+2. The TRN Subfield P+1 is transmitted/received by STAs using the same polarization. TRN Subfield P+2 is transmitted/received using vertical/horizontal polarization – see Fig. 4 (right). If STAs are at LOS, the main tap amplitude for TRN Subfield P+1 is non-zero, and zero for TRN Subfield P+2 due to polarization mismatch. Upon NLOS, the main tap amplitude is not zero for both TRN Subfields P+1 and P+2 because reflections change the polarization.

Once the procedure is completed, STAs elaborate a LOS likelihood report with the probability of being at LOS/NLOS. How to compute the LOS likelihood is out of the scope of 802.11az, however, works as [11] propose alternatives to distinguish between LOS/NLOS even without antenna alignment. Furthermore, if the STA is at NLOS, the position is obtained considering the reflection of walls – as in the trigonometry solution we propose in Sec. V-A.

#### IV. SECURE NEXT-GENERATION POSITIONING

The position of a STA is sensitive information that malicious STAs may sniff or corrupt [8]. With 802.11az it is possible to achieve secure FTM sessions. Specifically, STAs authenticate through PASN to later cipher the exchanged FTM frames.

##### A. Pre-Association Security Negotiation (PASN)

802.11az introduces PASN for secure exchanges among non-associated STAs. PASN reaches a Pairwise Transient Key Security Association (PTKSA) between Access Point (AP) and STA acting as a Robust Security Network Association (RSNA) protocol. However PASN can also reach the PTKSA without the Pairwise Master Key (PMK), acting as a non-RSNA protocol.

The PTKSA key is obtained exchanging three PASN elements (inside authentication frames) – see Fig. 5. First, the STA sends to the AP an ephemeral key and parameters to later derive a PMK. Second, the AP sends to the STA a protected frame with its ephemeral key and the chosen parameters to

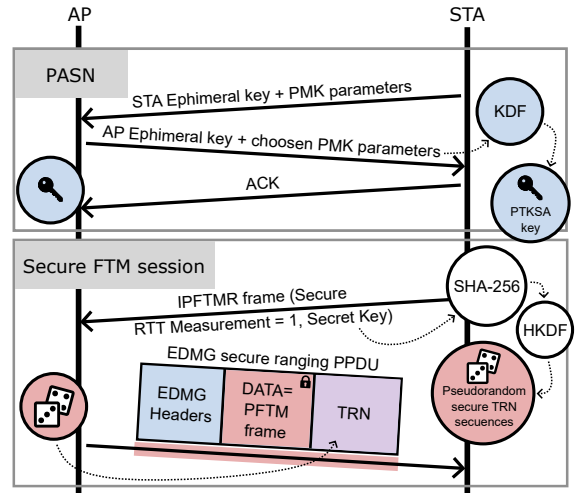


Fig. 5. The STA and AP securely pre-associate using 802.11az PASN (top). Afterward, both protect the FTM session (bottom) ciphering the FTM frame (black lock), and generating pseudorandom secure TRN sequences at PHY level (dice).

derive the PMK. Third, the STA confirms the chosen parameters sending an ACK within a protected frame.

Upon confirmation, the STA and AP use the Key Derivation Function (KDF) to generate the PTKSA key using the parameters negotiated in the exchanged PASN frames.

##### B. Secure FTM sessions

Once the PTKSA is achieved through PASN, or legacy authentication protocols [5], the STA requests a Secure FTM session issuing an Initial Protected FTM Request (IPFTMR) – see Fig. 5. Then, the STA obtains its relative position with respect to the AP through EDMG secure ranging PPDUs. The exchanged PPDUs contain Protected FTM (PFTM) frames and secure TRN Subfields for channel and positioning estimations.

The PFTM frame is ciphered using a RSNA or non-RSNA 802.11 confidentiality and integrity protocol [5]. Hence, the RSTA will notice if a malicious STA alters/corrupts the positioning information.

Secure TRN Subfields consist of padded pseudorandom bit sequences transmitted using  $\frac{\pi}{2}$ -BPSK. The pseudorandom sequences are generated as follows. First, the STA creates a Pseudo-random Key (PRK) using an SHA-256 hash function that receives the Secret Key and the identifier of the PMK previously generated, e.g., in PASN. Second, the STA produces the pseudorandom secure TRN sequence by feeding the HMAC-based Key Derivation

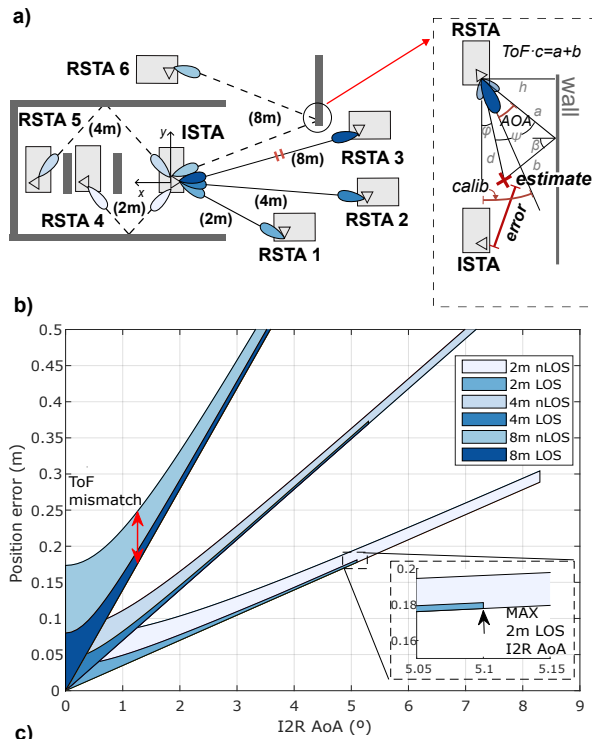


Fig. 6. Experimental scenario with trigonometry approach in NLOS (a). I2R AoA errors vs. the positioning error (b). Legacy FTM does not use FPBT, introducing positioning error variance (ToF mismatch). Comparison between SoA alternatives for indoor positioning (c).

Function (HKDF) with (i) the PRK; (ii) the string "EDMG Secure RTT"; and (iii) the length of the TRN field. A 3<sup>rd</sup> malicious STA sniffing the secure TRN Subfields cannot estimate the CIR and derive other STA position, as it does not know the original pseudorandom sequence. Moreover,  $\frac{\pi}{2}$ -BPSK is robust enough to detect if the TRN Subfield is corrupted upon channel jamming, and discard such TRN Subfield for positioning estimations.

## V. EVALUATION OF 802.11AZ MMWAVE

This section evaluates the accuracy of 802.11az implementations using a novel trigonometry solution<sup>2</sup>. Additionally, we compare 802.11az perfor-

mance with other indoor positioning solutions.

### A. Positioning accuracy

In our experimental analysis, we evaluate the precision of 802.11az implementations. For this purpose, we use MikroTik AP 60G, commercial-off-the-shelf devices with legacy 802.11-2016 FTM support and a mmWave uniform rectangular antenna array of 36 elements, using 2.16 GHz channel bandwidth, as specified in 802.11az. To obtain the ToF and I2R AoA estimations – 3<sup>rd</sup> option of [5, Table 11.11]) – we apply, respectively: (i) 802.11ad legacy FTM; and (ii) beamsweeping using a custom version of OpenWrt and mD-Track [4] to classify the obtained paths, extracting the AoA (elevation & azimuth) and received power.

The scenario consists of an ISTA and six RSTAs, half at LOS, half at NLOS, arranged in the room illustrated in Fig. 6 (a). The three RSTAs with LOS are placed 2, 4, and 8 m away from the ISTA; and the signals of NLOS RSTAs travel 2, 4 and 8 m to reach the ISTA. All the STAs are placed 1 m above the floor, thus the beam's elevation is 0°.

When STAs are at LOS, our trigonometry solution<sup>2</sup> computes the relative position leveraging the AoA and the ToF estimation. In the NLOS case (attenuation around 5 dB), our solution obtains the triangle formed by the signal bounce against the wall – with sides  $a, b$  and angle  $\psi$  in Fig. 6 (a) zoom. Sides  $a, b$  sum up the ToF times the speed of light, and angle  $\psi$  is obtained through elementary trigonometry.

Fig. 6 (b) plots the position error (y-axis) depending on the I2R AoA error (x-axis) for each RSTAs in Fig. 6 (a). As the graph shows, the RSTAs with LOS experience less AoA error (dark blue areas) than the NLOS (light blue areas) RSTAs. Fig. 6 (b) inset evidences the latter, for the RSTA at 2 m LOS has a maximum AoA error of 5.1° in while the RSTA at 2 m NLOS achieves an 8.3° AoA error.

In addition, for a fixed I2R AoA error, the RSTA reports different positioning errors – see Fig. 6 (b) red arrows. This happens because the implementation does not carry AoA estimations though the FTM frame, where ToF is carried. This leads to an ToF mismatch with the AoA estimation, which introduces variance in the position error, as the channel may not be the same during both estimations. Future implementations of 802.11az will overcome

<sup>2</sup><https://gitlab.netcom.it.uc3m.es/papicazo/802.11az/>

this problem, including the AoA estimations in the FTM frame.

### B. Comparison with existing solutions

We compare the positioning accuracy of our implementation with the following SoA indoor positioning technologies: 3GPP sub-6 GHz [12], Bluetooth 5.1 [13], and 3GPP mmWave [14]. Specifically, we compare the accuracy of our implementation in the same scenarios where the technologies were evaluated, each with the distances in Fig. 6 (c).

In the Bluetooth 5.1 scenario, with STAs 7.07 m away, 802.11az mmWave has errors below 36.49 cm, while Bluetooth 5.1 experiences larger errors of up to 80 cm due to low power and carrier.

For the 3GPP sub-6 GHz scenarios, with STAs 7 and 9 m away, we also see larger positioning errors than in 802.11az mmWave due to the smaller carrier frequency. 3GPP sub-6 GHz only outperforms our implementation in two percentiles (7 m 100% and 9 m 25%) because of bad AoA estimations.

Lastly, in the 3GPP mmWave scenarios, at 11.2 and 14.2 m, we observe that our implementation achieves higher worst-case accuracy – always below 56.30 cm error compared to the 85.50 cm error of 3GPP mmWave. Although both technologies show high accuracy, 802.11az mmWave (2.16 GHz at @60 GHz carrier) outperforms 3GPP mmWave (400 MHz at @28 GHz carrier) as it uses higher frequency and bandwidth.

## VI. CONCLUSION AND OPEN CHALLENGES

This work presents the main features of 802.11az mmWave positioning. The new amendment: (i) enhances FTM to include angle and ToF estimations; (ii) introduces a LOS assessment procedure; and (iii) secures FTM exchanges through PASN. Experimental results show cm-level accuracy using a novel trigonometry approach, and competitive errors with respect to SoA technologies.

Future evolutions of 802.11az mmWave will have to tackle the following research challenges to enhance indoor positioning: (i) how to compute the LOS likelihood in the LOS assessment; (ii) how to preserve positioning accuracy in secure FTM sessions – e.g. using Golay sequences ciphered with homeomorphisms [15]; (iii) how to coordinate 802.11az with other technologies for multi-RAT positioning; and (iv) how to optimally schedule

FTM sessions to not detriment the wireless communication;

## REFERENCES

- [1] R. Want *et al.*, “Accurate Indoor Location for the IoT,” *Computer*, vol. 51, pp. 66–70, 2018.
- [2] K. Chang *et al.*, “Technical challenges and solutions for 10cm-level positioning accuracy towards 6G,” *ICT Express*, 2022.
- [3] C. Wu *et al.*, “mmTrack: Passive Multi-Person Localization Using Commodity Millimeter Wave Radio,” in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020, pp. 2400–2409.
- [4] Y. Xie *et al.*, “mD-Track: Leveraging Multi-Dimensionality for Passive Indoor Wi-Fi Tracking,” in *The 25th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom ’19. New York, NY, USA: Association for Computing Machinery, 2019.
- [5] IEEE, “IEEE 802.11az Approved Draft Standard for Information technology – Amendment 4: Enhancements for positioning,” *IEEE P802.11az/D7.0, September 2022*, pp. 1–291, 2022.
- [6] V.A. Reddy and G.L. Stüber, “Multi-User Position Estimation and Performance Trade-offs in IEEE 802.11az WLANs,” in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, 2022, pp. 1–5.
- [7] N.G. Rihan *et al.*, “A Hybrid Deep-learning/Fingerprinting for Indoor Positioning Based on IEEE P802.11az,” in *2022 5th International Conference on Communications, Signal Processing, and their Applications (ICCSIPA)*, 2022, pp. 1–6.
- [8] J. Henry *et al.*, “Ranging and Location attacks on 802.11 FTM,” in *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2021, pp. 1481–1486.
- [9] P. Leu *et al.*, “Security of Multicarrier Time-of-Flight Ranging,” in *Annual Computer Security Applications Conference*, ser. ACSAC ’21. New York, NY, USA: Association for Computing Machinery, 2021, p. 887–899.
- [10] H. Ajorloo *et al.*, “On the Feasibility of Using IEEE 802.11ad MmWave for Accurate Object Detection,” in *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, ser. SAC ’19. New York, NY, USA: Association for Computing Machinery, 2019, p. 2406–2413.
- [11] O.L.A. López *et al.*, “Polarization Diversity-Enabled LOS/NLOS Identification via Carrier Phase Measurements,” *IEEE Transactions on Communications*, vol. 71, pp. 1678–1690, 2023.
- [12] L. Chen *et al.*, “Carrier Phase Ranging for Indoor Positioning With 5G NR Signals,” *IEEE Internet of Things Journal*, vol. 9, pp. 10908–10919, 2022.
- [13] P. Sambu and M. Won, “An Experimental Study on Direction Finding of Bluetooth 5.1: Indoor vs Outdoor,” in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, 2022, pp. 1934–1939.
- [14] G. Yammine *et al.*, “Experimental Investigation of 5G Positioning Performance Using a mmWave Measurement Setup,” in *2021 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2021, pp. 1–8.
- [15] A. Acar *et al.*, “A Survey on Homomorphic Encryption Schemes: Theory and Implementation,” *ACM Comput. Surv.*, vol. 51, jul 2018.

**Pablo Picazo-Martínez** got his M.Sc. in 2022 and is a Ph.D. student at Universidad Carlos III de Madrid.

**Carlos Barroso-Fernández** got his M.Sc. in 2022 and is a Ph.D. student at Universidad Carlos III de Madrid.

**Jorge Martín-Pérez** got his M.Sc. in 2017 and Ph.D. in 2021, is an assistant professor at Universidad Politécnica de Madrid.

**Milan Groshev** got his Ph.D. on Telematics Engineering in 2022 at Universidad Carlos III de Madrid, where he works as postdoc.

**Antonio de la Oliva** got his M.Sc. in 2004 and his Ph.D. in 2008, is an associate professor at Universidad Carlos III de Madrid.