On the Privacy of LEO Two-Way-Ranging

1st Daniele Coppola
ETH Zürich

2nd Harshad Sathaye
ETH Zürich

3rd Giovanni Camurati
ETH Zürich

4th Srdjan Capkun
ETH Zürich

***Abstract*— Low Earth Orbit (LEO) satellite-based positioning, navigation, and timing (LEO-PNT) is being investigated as an alternative to traditional broadcast-based satellite navigation systems. LEO satellites make bidirectional communication possible, and organizations like ESA, GMV, and Thales have considered Two Way Ranging (TWR) as an alternative to classical broadcast PNT systems. Previous work has shown that TWR poses a threat to the location privacy of its users and proposes countermeasures. In this work, we analyze this problem in the context of LEO-PNT. First, we quantify the location leakage in LEO-PNT. Second, we identify that due to the relative motion between high-speed satellites and users, mitigations proposed in the context of distance bounding cannot be directly used - they introduce inaccuracies with an average of 36.7 m in the computed position. Third, we propose a new TWR system which combines previously proposed countermeasures with Intertial Measurement Unit (IMU) sensing such that it provides privacy protection and eliminates ranging inaccuracies. We study the performance of our system in simulation and show that short-term error introduced by privacy-protection measures can be very well mitigated with the short-term stability of IMU output.**

***Index Terms*—Secure Positioning, Two-way ranging, Navigation, Inertial Sensor.**

I. Introduction

A. Motivation

In recent years, the LEO satellite segment has seen tremendous growth. Constellations like Starlink [18] and Iridium [8] are examples of successful commercial services based in LEO space. LEO satellites are closer to Earth, and thanks to better SNR, they enable bidirectional communication. While currently used primarily for communication, LEO satellites naturally lend themselves to positioning applications. Indeed, the mission *leo-pnt* [4] by the European Space Agency (ESA) investigates how LEO satellites can be leveraged to increase the resilience and robustness of Global Navigation Satellite Systems (GNSS) systems. A key aspect investigated in this mission is the use of Two Way Ranging (TWR) [3] between orbiting LEO satellite(s) and a User Equipment (UE) on the ground. Companies like *Thales* and *GMV* have started programs to develop a two-way ranging solution for LEO satellites [5], [7]. In the future, LEO TWR could be used to enhance existing GNSS solutions, or as a standalone system.

TWR has already been deployed for local distance measurements in key technologies such as UWB and Bluetooth [1], [6]. In this paper, we study the privacy implications of using TWR in LEO ranging and positioning. Specifically, how TWR can leak information regarding the location of the ranging parties and how previously proposed countermeasures may not work out of the box in the context of LEO. The privacy implications of TWR were already studied in 2008 by Rasmussen et al. [15] in the context of distance-bounding protocols with slow moving or static devices. The authors demonstrated that rapid message exchanges can leak information about the location of the ranging devices. The mitigation proposed by the authors was to randomize the reply times and conceal the user's location within this noise. This mitigation was designed for systems like UWB, where the objects involved are typically slow relative to the time required for the TWR process to complete.

In this work, we study the privacy implications of TWR in the context of LEO - this setting differs from prior work in two main aspects: (i) the geometry of the system changes during the message exchange due to high mobility of the ranging objects (e.g. satellites or planes; i.e., from the time that the challenge is transmitted and the reply is generated, the distance between the devices changes, and (ii) the trajectories of satellites are publicly known, providing additional information to the attackers.

This has the following implications. As discussed in section II, an adversary equipped with a single antenna can monitor the ranging process, measure message timings, and derive quadratic constraints on the user's location. However, since in the LEO context, satellites (and users such as planes) move at high speeds, the system's geometry cannot be assumed to be constant during the TWR process. Consequently, RTT measurements inherently contain errors due to the distance changing on each message trip. Randomizing the reply time as suggested in [15] - in order to protect location privacy - exacerbates the problem, as longer reply times lead to more significant geometry changes, which, if not properly addressed, result in errors in the computed range and position. On the other hand, randomized reply times are necessary to conceal the users location.

To address this issue we propose a new LEO TWR system that combines randomized reply times - in order to protect user privacy with IMUs that provide the short-term error correction. Our results show that this combination is an ideal fit, providing both privacy and error-correction.

B. Contributions

In this paper, we raise the issue of location leakage in upcoming LEO TWR systems and make the following contributions:

- We show that in LEO TWR based positioning system, a single antenna recording a positioning exchange is sufficient to reveal the user's position.

- We evaluate the impact of previously proposed mitigations on the position accuracy. Specifically, we show that the error in positioning grows linearly with the applied delay, with a coefficient of 146.8 meters error per second delay. For example, a delay of 0.25 seconds results in an error of approximately $\approx 36.7m$.
- We show that a low-cost MEMS IMU is sufficient for correcting this error. The short-term stability of such sensor fits perfecly the usecase of estimating the position changes of the user during TWR. Thanks to this correction, the positioning errors remain small and largely constant throughout, even as delays increase. We achieve position accuracies of approximately $\approx 0.12\ m$ when delaying replies by up to $maxDelay$, with an error that grows linearly in the delay, having a coefficient of 0.5 m/s.

II. Background

In this section, we introduce TWR and describe the privacy leakage with an example of how the positions leak when TWR is performed with fixed reply times.

A. Two-way Ranging

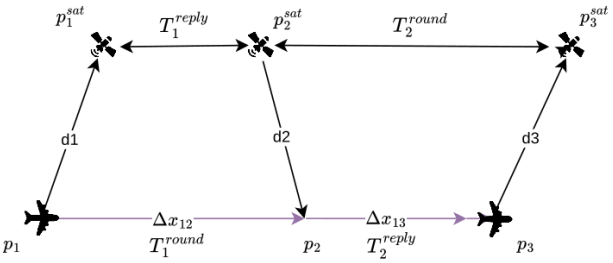


Fig. 1. Two-way ranging measurement in the dynamically moving LEO setting.

In TWR, the distance is measured based on the Round Trip Time (RTT) of the exchanged messages. Figure 1 shows a double-sided two-way ranging between a satellite and a plane. In the following section of the paper, we will refer to the device computing its position as the system's user. Given the reply times T_1^{reply}, T_2^{reply} and the round-trip times T_1^{round} and T_2^{round}, the user can compute the distance.

$$d_1 + 2d_2 + d_3 = c \cdot (T_1^{round} - T_1^{reply} + T_2^{round} - T_2^{reply}). \quad (1)$$

Where c is the speed of light and d_1, d_2, d_3 are the distances between the satellite and user when each of the three messages is sent. Equation 1 can be seen as the sum of two single-sided ranging, the first from the user to the satellite and the second in reverse. This explains why the term d_2 appears twice. For brevity, we will refer to the sum $d_1 + 2d_2 + d3$ as d_{twr}. In terrestrial applications where the objects involved are relatively slow, the distances $d_1 \approx d_2 \approx d_3$ are constant during the measurement, and therefore the distance can be computed from Equation 1.

In the context of LEO, with a non-negligible processing time, solely the satellite movement would make the distances change significantly during the exchange. Consequently, for each satellite included in the position measurement, the following equation can be derived

$$d_{twr} = \mathsf{d}(p, p_1^{sat}) + 2\mathsf{d}(p, p_2^{sat}) + \mathsf{d}(p, p_3^{sat}). \quad (2)$$

With three such equations, and under the assumption that the velocity of the user is small, the position p of the user can be accurately computed. We show in section IV that for objects moving at higher speed (e.g. planes with velocities > 200 m/s) the approximation of $d_1 \approx d_2 \approx d_3$ leads to positioning errors in the order of tens of meters.

B. Location Leakage

Assuming an adversary can listen to the conversation depicted in Figure 1, and that the satellites' positions are known, an adversary can locate the user. In this section, we adapt the work of [15] to the LEO context and provide an example of the constraint that an adversary can derive for each satellite used in the positioning. A key difference with respect to [15] is that in the context of LEO only the trajectory of the satellites is known, but not the position at which the message was transmitted. However, an adversary could still estimate the satellite's position at the transmission time based on when it received the message from the satellite and on an estimate of the message's travel time derived from the attacker's location. In the following, we assume that the satellite's positions are known and that the Time of Flight (ToF) between satellite and user is approximately constant for short reply times; this provides an over-approximation of the attacker's capabilities that shows the potential of this attack.

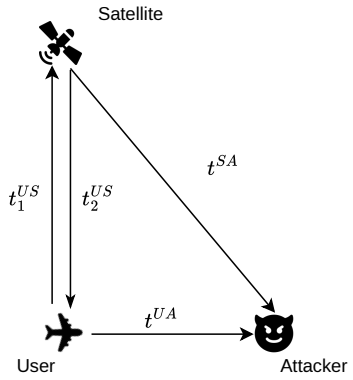


Fig. 2. Attack on position privacy against a user performing TWR with a satellite. The attacker is assumed to be close enough to the victim to overhear the conversation and register the arrival time of the messages.

As shown in Figure 2, the attacker can register the following three timings

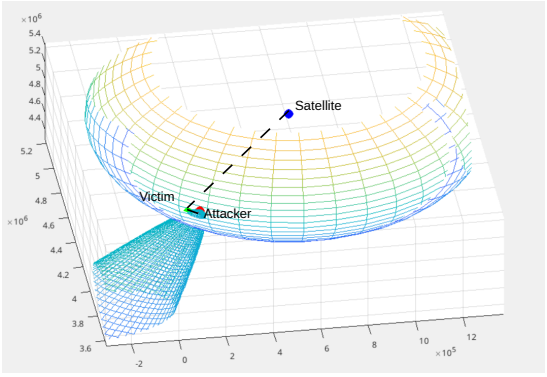
$$\begin{cases} T_0 = t_0 + t^{UA} \\ T_1 = t_0 + t^{US} + t^{SA} \\ T_2 = t_0 + 2 \cdot t^{US} + t^{UA}. \end{cases} \quad (3)$$

Here we used the assumption that without randomization $T^{reply} \approx 0$ and therefore $t_1^{US} \approx t_2^{US} = t^{US}$.

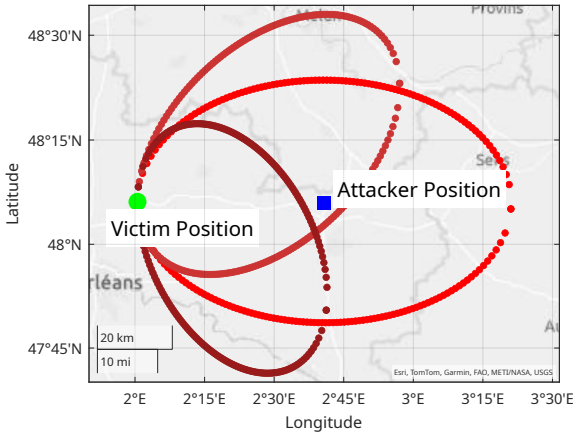
By observing the message timings, the adversary can learn

$$\begin{cases} t^{US} - t^{UA} = T_1 - T_0 - t^{SA} \\ t^{US} = (T_2 - T_0)/2 \end{cases} \quad (4)$$

The first equation generates a hyperboloid with the foci in the attacker and the satellite, and the second is a sphere around the satellite. The two shapes are visualised in Figure 3(a), where we considered a scenario with an attacker at 50 km from the victim. As shown in Figure 3(b), the attacker's constraints intersect at the victim position.



(a) For each user-satellite TWR, the attacker can position the user on the above surfaces.



(b) The intersection of the constrain derived by the attacker for two satellites intersect at the victim's position.

Fig. 3. Privacy leakage attack visualized.

C. Mitigation

We showed that LEO TWR systems are vulnerable to the attacks proposed in [15]. The user's location fully leaks in case TWR is performed with three or more satellites, which is necessary for the user to compute its position. Rasmussen et al. in [15] also propose hiding the user's position by adding random delays to the reply time. If random delays are added to the T^{reply}, then both equations in Equation 3 have an additional $delay$ term which is unknown to the adversary. Consequently, the intersection in Figure 3 becomes a distribution of possible positions that spreads wider as the random delays increase. A side effect of increasing the reply time is that the error introduced on the measured distances also increases. This creates a tradeoff in increasing the reply times. High reply times conceal the user's location and additionally reduce the requirements on the processing speed of the devices. However, this poses a problem if the ranging devices move during a TWR measurement. Changes in position during TWR cause a shift in the measured distance and increase the position error. We show in this paper that integration of an IMU sensor allows correction of errors and breaks this tension, enabling the creation of a privacy-preserving and accurate positioning system.

III. System Design

If a randomized reply scheme is adopted, the changes in user positions are non-negligible, as both devices have moved significantly between messages; hence, the final range calculated does not accurately reflect the user's true range at the time of measurement. To overcome this limitation, we propose the integration of IMU sensors to compensate and correct for the user's movements during the TWR measurement.

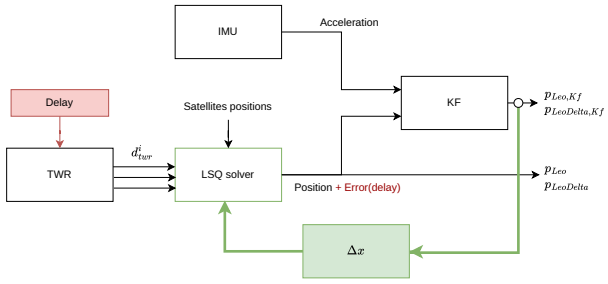


Fig. 4. The baseline *Leo* positioning system with randomized responses introduces an error proportional to the delay introduced. The system processes as inputs the IMU measurements and the TWR ones. Our proposal is highlighted in green. In *LeoDelta*, the position changes of the user's are fed back to the positioning block which uses to correct the system of equations.

A. Leo TWR with Randomized Reply Time

We consider as baseline a positioning system that gets as inputs

- the satellites' positions
- the distances d_{twr} measured with TWR
- the sensor readings of an IMU.

In the baseline solution, a Kalman Filter (KF) is used to fuse positioning measurements from the LEO block and the IMU using standard sensor fusion. This system, without the additional delta block in green, is depicted in Figure 4. We keep track of two positions computed by the system: the one at the output of the position solver p_{Leo} , and the one outputted by the KF $p_{Leo,kf}$. We chose this setup because it allows for the evaluation of both a standalone position system and a position system that utilizes sensor fusion to enhance position accuracy.

As suggested in [15], the TWR measurement adds a randomized $delay$ to protect the user's location. A side-effect of this countermeasure is that the reply times T^{reply} become longer, and the distance measured by the TWR block consists of the sum of three different distances corresponding to the distances at the moment of transmission of the three messages. This leads to an error in the position computed by *Leo*. Our results in section IV show that a naive application of sensor fusion is not enough to compensate for the error introduced by the longer reply times.

B. LeoDelta: Error Correction

We propose a different design for the integration of the IMU measurements with LEO TWR. The core idea is to leverage the IMU's short-term accuracy to compensate for the errors introduced by the user's movements.

Similarly to the baseline system, a Kalman Filter is used to fuse the position from the solver and the IMU measurements. We use the high update rate measurements of the IMU to estimate the position of the user when the TWR messages are transmitted. Our innovation consists of feeding the output of the KF back to the positioning block so that an estimate of the displacement of the user $\Delta x_{12}, \Delta x_{23}$ can be computed and used as a correction in the system of equations used for the position. The user expresses its positions $p_{1,2}$ as a function of the final position p_3 and the displacements. Equation 2 can be then corrected as follows:

$$\begin{aligned} d_{twr} = \; & \mathsf{d}(p - \Delta x_{23} - \Delta x_{12}, p_1^{sat}) + \\ & 2\mathsf{d}(p - \Delta x_{23}, p_2^{sat}) + \\ & \mathsf{d}(p, p_3^{sat}). \end{aligned} \tag{5}$$

The three positions of the user are expressed with respect to the position of the user p when the last message is exchanged. Thanks to the corrections provided by the IMU, the only unknowns are the three coordinates of the user at the end of the exchange, and the system can be solved with three satellites. As for the baseline, we track the positions $p_{LeoDelta}$ and $p_{LeoDelta,kf}$ at the output of the solver and the KF.

IV. Evaluation

In this section, we describe the simulations used to analyze the accuracy of our proposal and present the results obtained.

A. Evaluation Framework

Our simulation framework was built on top of the MATLAB sensor fusion example [10].

The simulation framework receives a list of trajectories as inputs and simulates the system in Figure 4. Given the position ground truth, the simulation creates a position problem which consists of three satellite positions, and the sum of the distances $d_{twr} = d_1 + 2d_2 + d_3$.

For each simulation, we evaluate two systems: (i) *Leo* solves the position without the Δx corrections, (ii) *LeoDelta* uses the feedback loop to compensate for the user movements. For both systems, we instantiate a separate KF [11] and report the positioning output by the KF and the position solver.

B. Simulations Description

We choose to evaluate our system on plane trajectories, as these are the objects most affected by the dynamic nature of the TWR system. The trajectories come from the *traffic* dataset [13], which contains trajectories of planes in landing areas and while cruising. We considered using ADS-B data from [16], however, we found significant noise in the unfiltered trajectories that led to unreasonable accelerations (e.g., 10G) and therefore decided to pick the already filtered dataset from *traffic*. In the simulations, trajectories are created based on waypoints and ground speed using the Matlab *waypointTrajectory* function, with the maximum jerk fixed at 3 m/s^3. We evaluate our system on 600 trajectories of ≈ 10 minutes. For 7 trajectories, due to noisy measurements, the trajectories would have required higher jerk, and were therefore excluded. The IMU is initialized with the default Matlab values, which are typical for low-cost MEMS sensors, and we make minimal changes to the fusion filter.

For the satellite constellation, we use the Starlink constellation. Given the ground truth position of the user, we provide the solver with the TWR distance to three of the Startlink satellites that are in view. We consider a satellite in view if they are above 30 degrees elevation. If more than three satellites are visible, we choose three satellites that are ≈ 120 degrees apart to ensure a good spread.

Finally, we study the positioning error for increasing fixed delay as opposed to randomized ones. This enables us to reduce the number of simulations necessary to understand the tradeoff between longer reply times and position accuracy.

C. Results

1) Average Position Errors: Our results show that the error grows linearly with respect to the reply time. However, with the IMU compensation, we are able to maintain the error low even for reply times up to 0.25 seconds. Figure 5 shows the trend of the positioning error across all simulated scenarios.

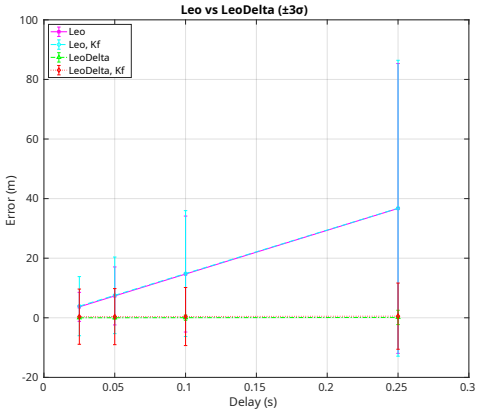
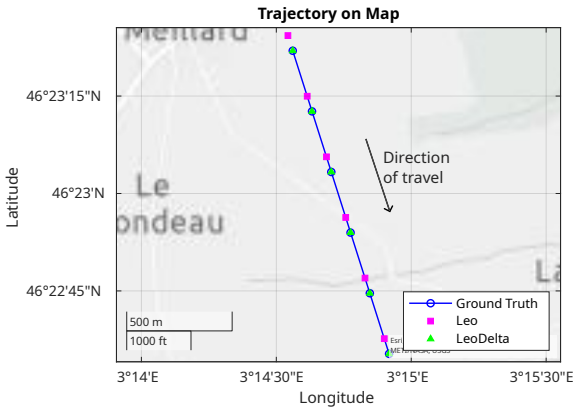


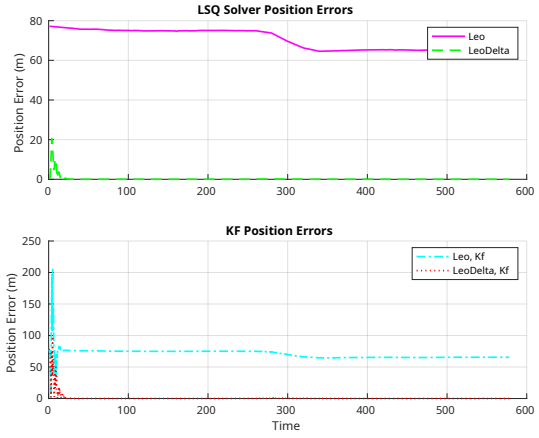
Fig. 5. Positioning errors obtained by the *Leo* and *LeoDelta* systems. The *Leo* system is not able to compensate for the errors introduced by the longer reply times, even when fusing the IMU positions. The errors are greatly compensated by *LeoDelta*.

In *Leo*, the error grows linearly with a coefficient of 146.8 meters per seconds of delay. Thanks to the correction provided by the IMU, the growth rate is significantly decreased to a value of 0.5 m/s. When applying a reply time of 0.25 seconds, the average error for *Leo* is $36.7m$, while in for *LeoDelta* it remains at $0.12\ m$.

2) Error on the Trajectory: An interesting finding that only shows when looking at the trajectories computed by the two systems is that the trajectories from the *Leo* system are still accurate, though the computed points lag behind the ground truth. This is because, without compensating for the user's movement, the distances from the satellites are an average of the three distances. Consequently, the position is an average of the three positions. An example of this is depicted in Figure 6(a). Though from the view on the map, the error may seem constant, Figure 6(b) shows that this is not the case. Future work should investigate this phenomenon with fully randomized timings and the connection between trajectory type, e.g., constant vs changing speed, and the trajectory error.



(a) Trajectory of a plane during crusing.



(b) Positioning errors incurred by *Leo* and *LeoDelta*.

Fig. 6. Trajectories computed by *Leo* and *LeoDelta*. The light blue dots representing the *Leo* trajectory lag behind the ground truth and the trajectory computed by *LeoDelta*.

V. Related Work

The issue of location privacy leakage in distance bounding protocols was first investigated by Rasmussen et al. [15] and later formalized by Mitrokotsa et al. [12]. Kotuliak et al. [9] and Schepers et al. [17] showed location leakage attacks on real systems like LTE and WiFi. In the context of LEO positioning, sensor fusion with an IMU was mainly used with signals of opportunity [2], [14] and not on TWR. TWR is currently used in short-range systems (e.g., for access control [6]) where the velocity of the devices is negligible compared to our study.

VI. Conclusions

In this paper, we have shown the problem of position leakage when performing TWR with LEO satellites. We show that existing countermeasures introduce inaccuracy in the computed positions. Our results indicate that the readings of an IMU can be used to compensate for the errors introduced by the privacy-preserving countermeasures.

References

[1] Bluetooth SIG. Channel Sounding CR-PR. https://www.bluetooth.com/specifications/specs/channel-sounding-cr-pr/. Accessed 2024-08-8.

[2] Yansong Du, Honglei Qin, and Chao Zhao. LEO satellites/ins integrated positioning framework considering orbit errors based on FKF. *IEEE Trans. Instrum. Meas.*, 73:1–14, 2024.

[3] European Space Agency. 5G NON-TERRESTRIAL NETWORK SECURE TWO-WAY RANGING FOR LEO SATELLITES. https://esastar-publication-ext.sso.esa.int/ESATenderActions/details/138768. Accessed 2025-06-24.

[4] European Space Agency. LEO-PNT. https://www.esa.int/Applications/Satellite_navigation/LEO-PNT. Accessed 2024-08-8.

[5] European Space Agency. Navisp1-fp-gmvnsl-057-0001 v1.0 final presentation slides. https://navisp.esa.int/uploads/files/documents/NAVISP1-FP-GMVNSL-057-0001_v1.0_Final%20Presentation%20Slides%201%20(1).pdf, 06 2025. Final presentation of NAVISP Element 1 project.

[6] FiRa Consortium. Fira consortium. https://www.firaconsortium.org/. Accessed: 2025-06-24.

[7] Thales Group. Proof-of-concept of a space-based position augmentation with 2way communication. https://nebula.esa.int/sites/default/files/neb_tec_studies/3195/public/ESR_Executive_Summary_Report.pdf, 2023.

[8] Iridium. Iridium. https://www.iridium.com/network/. Accessed 2024-08-8.

[9] Martin Kotuliak, Simon Erni, Patrick Leu, Marc Röschlin, and Srdjan Capkun. Ltrack: Stealthy tracking of mobile phones in LTE. In Kevin R. B. Butler and Kurt Thomas, editors, *31st USENIX Security Symposium, USENIX Security 2022, Boston, MA, USA, August 10-12, 2022*, pages 1291–1306. USENIX Association, 2022.

[10] MathWorks. Imu and gps fusion for inertial navigation. https://ch.mathworks.com/help/nav/ug/imu-and-gps-fusion-for-inertial-navigation.html. Accessed: 2025-06-24.

[11] MathWorks. insfilterMARG. https://ch.mathworks.com/help/nav/ref/insfiltermarg.html, 2025. Accessed: 2025-06-24.

[12] Aikaterini Mitrokotsa, Cristina Onete, and Serge Vaudenay. Location leakage in distance bounding: Why location privacy does not work. *Comput. Secur.*, 45:199–209, 2014.

[13] Xavier Olive. traffic, a toolbox for processing and analysing air traffic data. *Journal of Open Source Software*, 4:1518, 2019.

[14] Honglei Qin, Yansong Du, Jiatong Li, Zhenbo Xu, and Huaiyuan Liang. A dynamic initialization method for LEO/INS integrated positioning. *IEEE Trans. Instrum. Meas.*, 73:1–12, 2024.

[15] Kasper Bonne Rasmussen and Srdjan Čapkun. Location privacy of distance bounding protocols. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 149–160, 2008.

[16] Matthias Schäfer, Martin Strohmeier, Vincent Lenders, Ivan Martinovic, and Matthias Wilhelm. Bringing Up OpenSky: A Large-scale ADS-B Sensor Network for Research. In *Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*, IPSN '14, pages 83–94. IEEE Press, April 2014.

[17] Domien Schepers and Aanjhan Ranganathan. Privacy-preserving positioning in wi-fi fine timing measurement. *Proc. Priv. Enhancing Technol.*, 2022(2):325–343, 2022.

[18] Starlink. Starlink. https://www.starlink.com/technology. Accessed 2024-08-8.