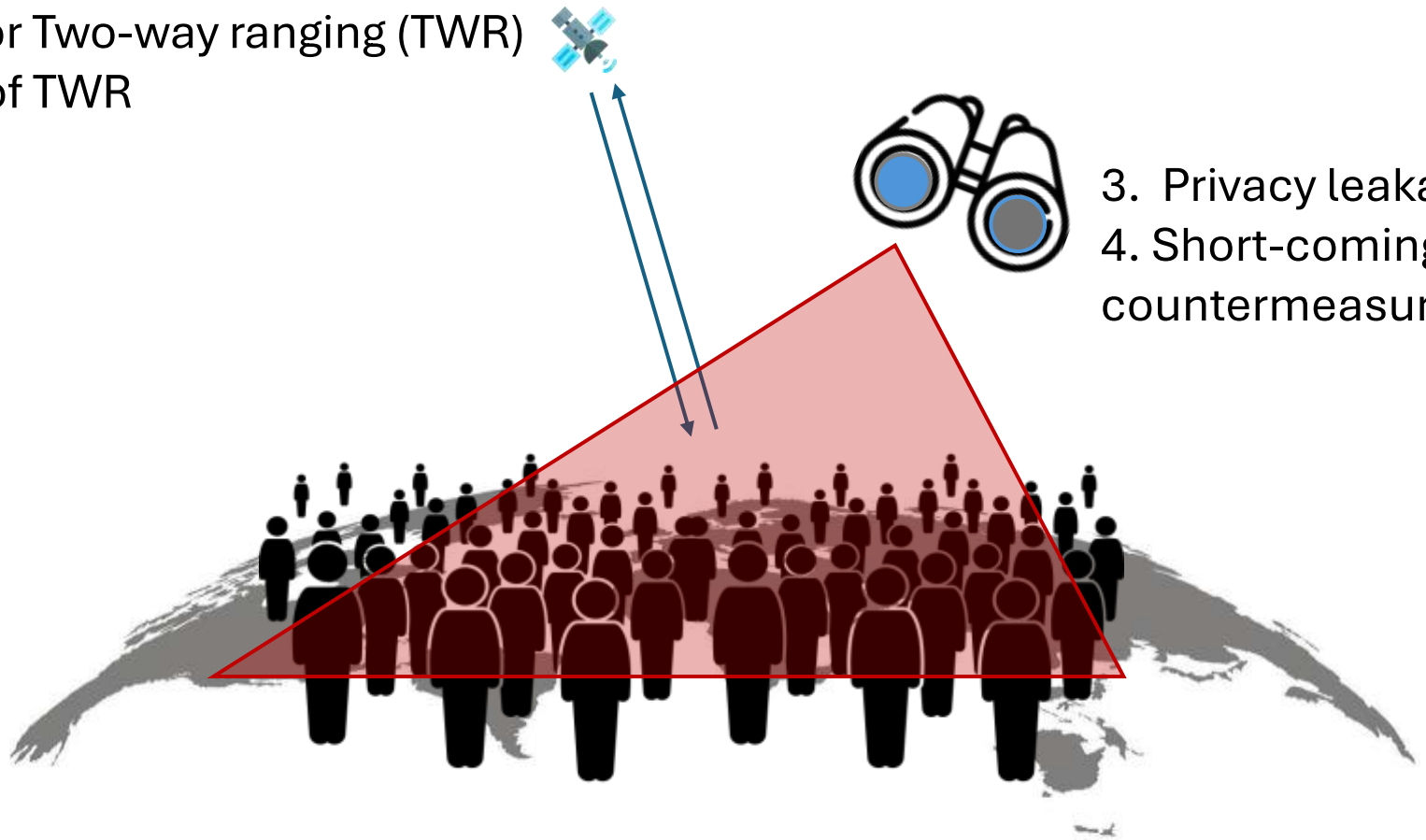
On the Privacy of LEO Two-Way Ranging

Daniele Coppola, Harshad Sathaye, Giovanni Camurati, Srdjan Capkun

ETH Zürich

Summary

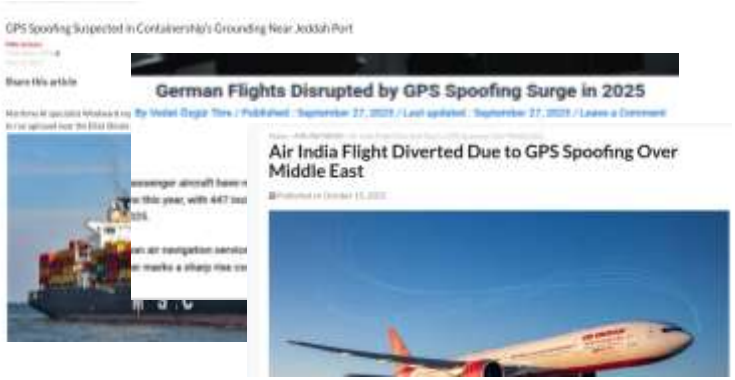
1. Motivation for Two-way ranging (TWR)
2. Challenges of TWR

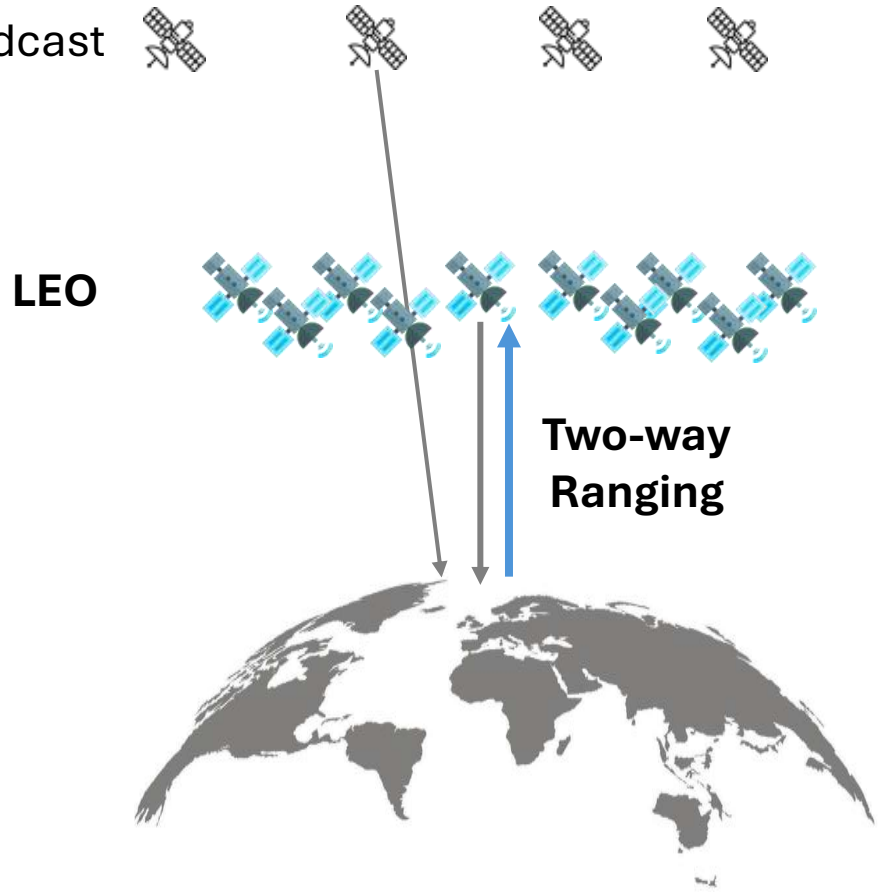


3. Privacy leakage
4. Short-coming of existing countermeasures

5. Our Proposal: LeoDelta
6. Results and Conclusions

Secure Positioning Landscape

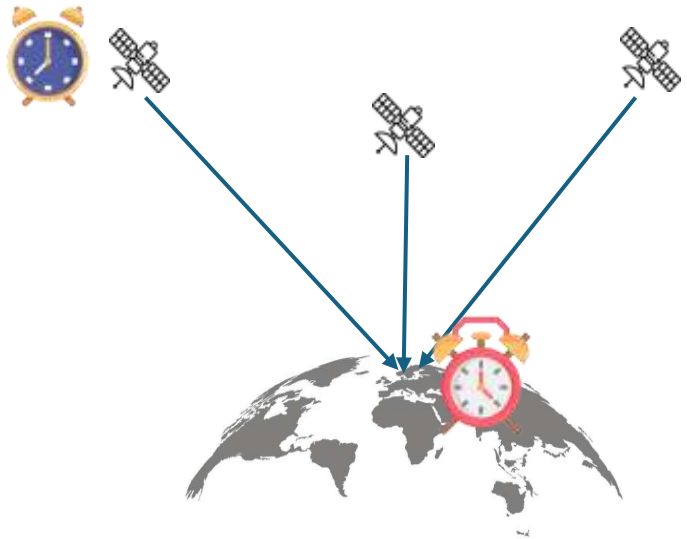




How can we use TWR to secure existing GNSS?

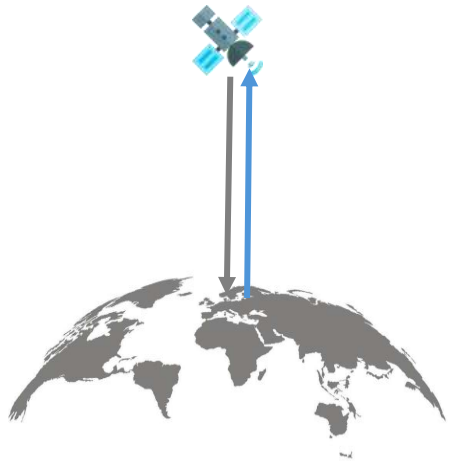
Why Two-way Ranging

Broadcast



- Measures are affected by the clock bias
- Positioning is based on the relative pseudoranges
- Vulnerable to selective delays (Motallebighomi et al. , *WiSec '23*)

Two-Way Ranging

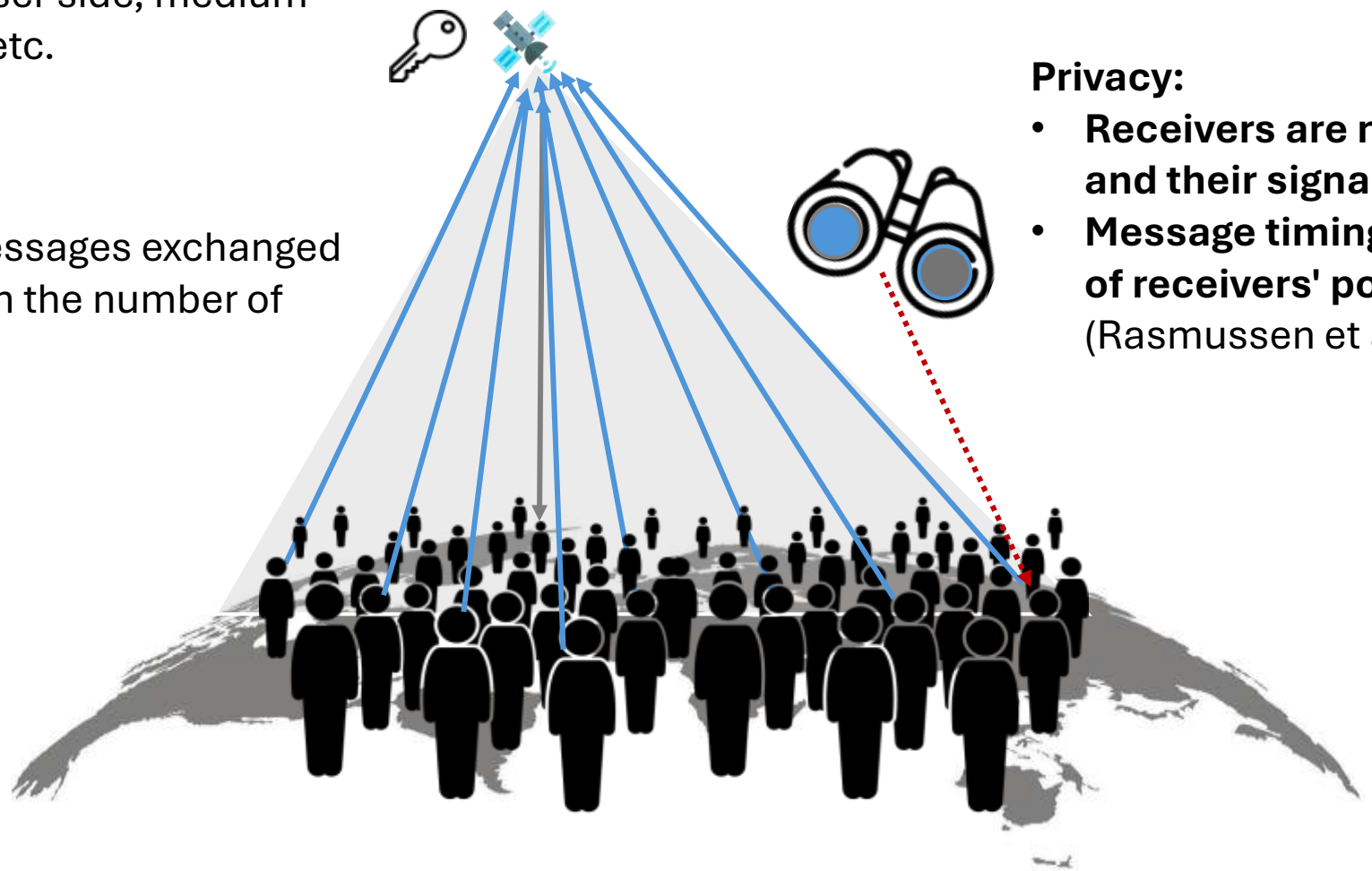


- Measures are NOT affected by the clock bias
- Measures are based on the round trip time

Two-Way Ranging Downsides

Complexity: key management on the user side, medium sharing etc.

Scalability: Messages exchanged grows linearly in the number of served users

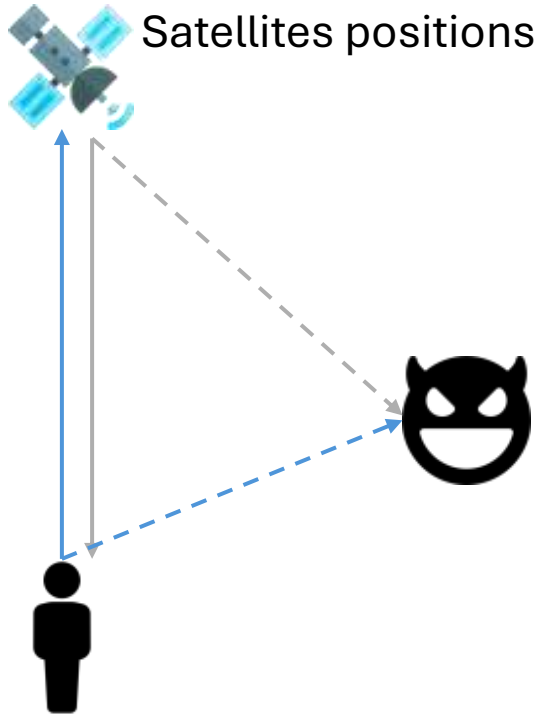


Privacy:

- **Receivers are not passive anymore and their signals can be observed**
- **Message timing leaks information of receivers' position** (Rasmussen et al., *CCS '08*)

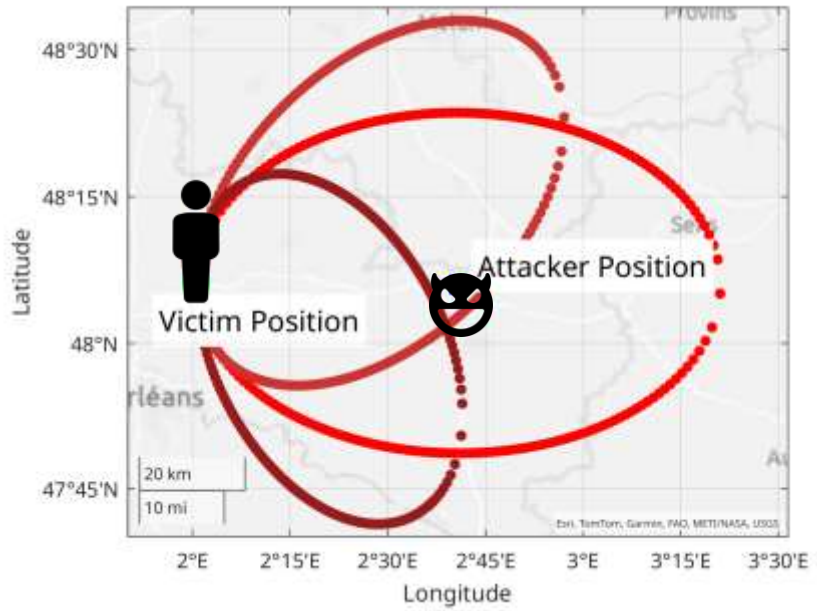
Location Leakage in TWR (Rasmussen et al., *CCS '08*)

- An adversary observing a two-way ranging exchange can derive constraints on the user location because
- Three TWR are sufficient to localize the receiver



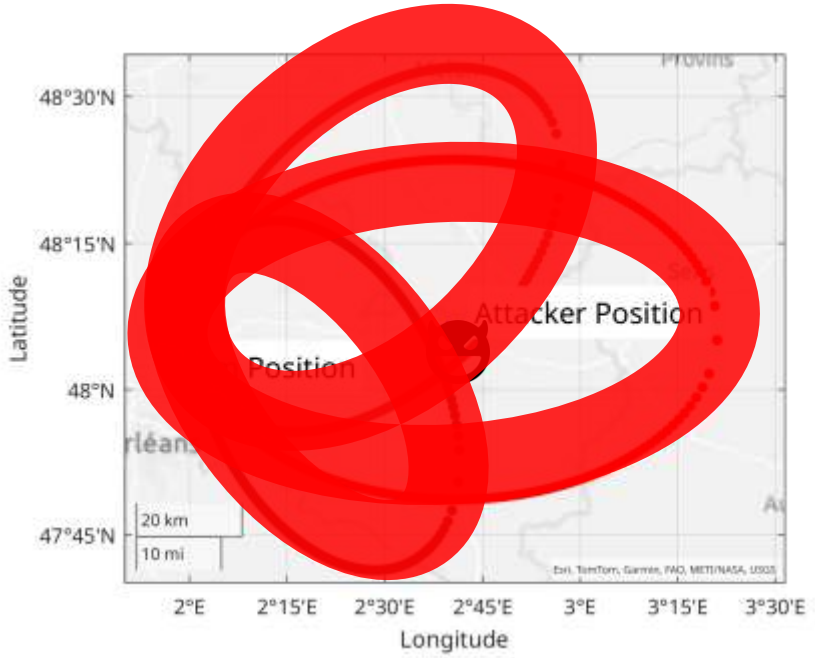
Satellites positions are known

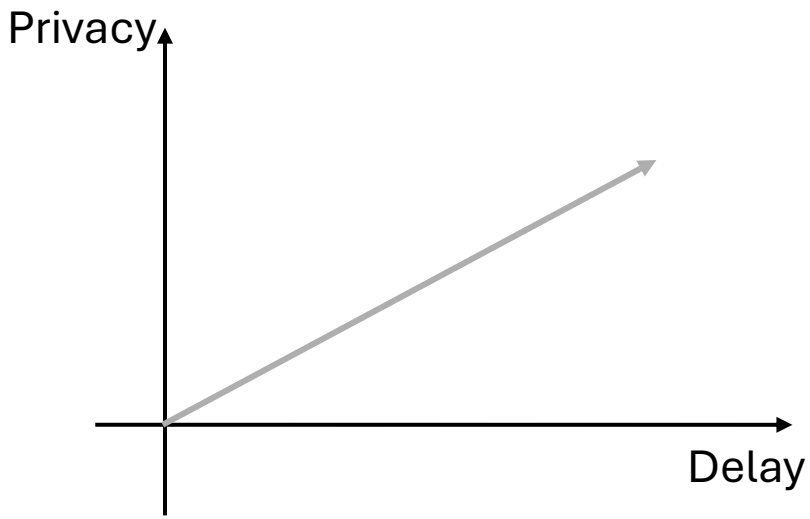
The adversary records the time of arrival of each ranging message



Privacy Preserving TWR (Rasmussen et al., *CCS '08*)

- Rasmussen et. al. proposed to **randomize the reply times** and hide the user location in noise
- The adversary cannot distinguish between a larger distance and a longer reply times

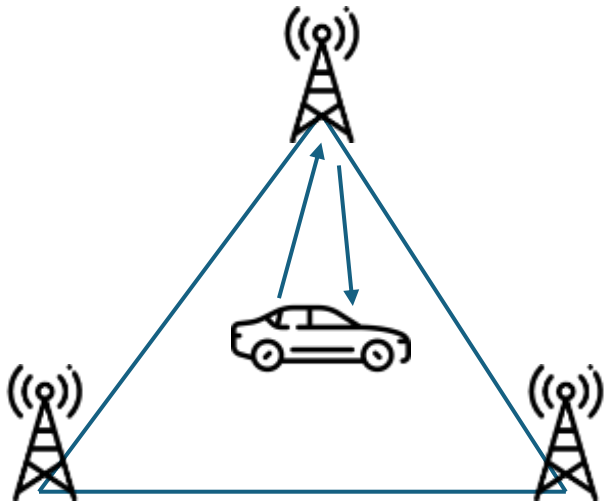




Privacy Preserving TWR (Rasmussen et al., *CCS '08*)

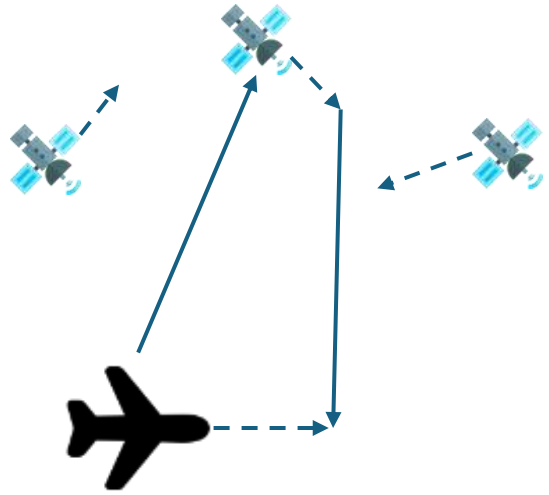
- Adding a random delay to the original reply times increase the overall reply time
- Works well for static or slow-moving systems
- Introduces errors for dynamic systems

Static / Slow



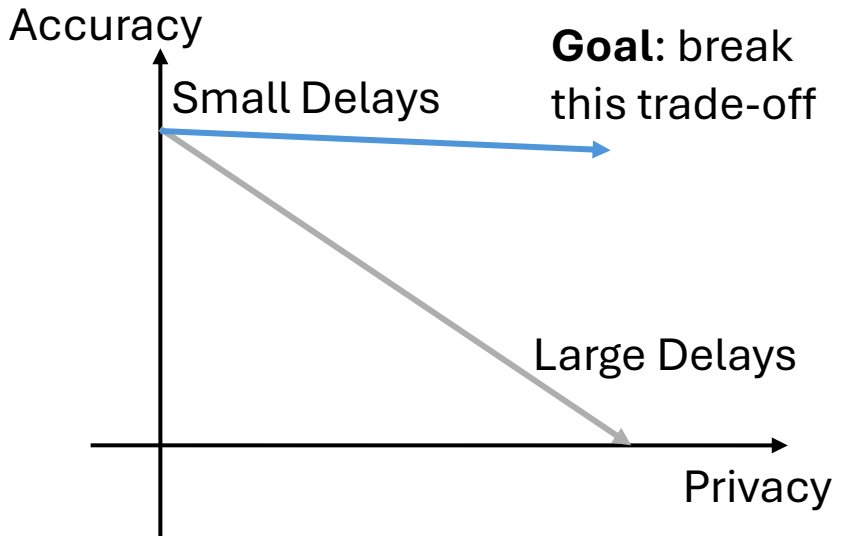
✓

Dynamic

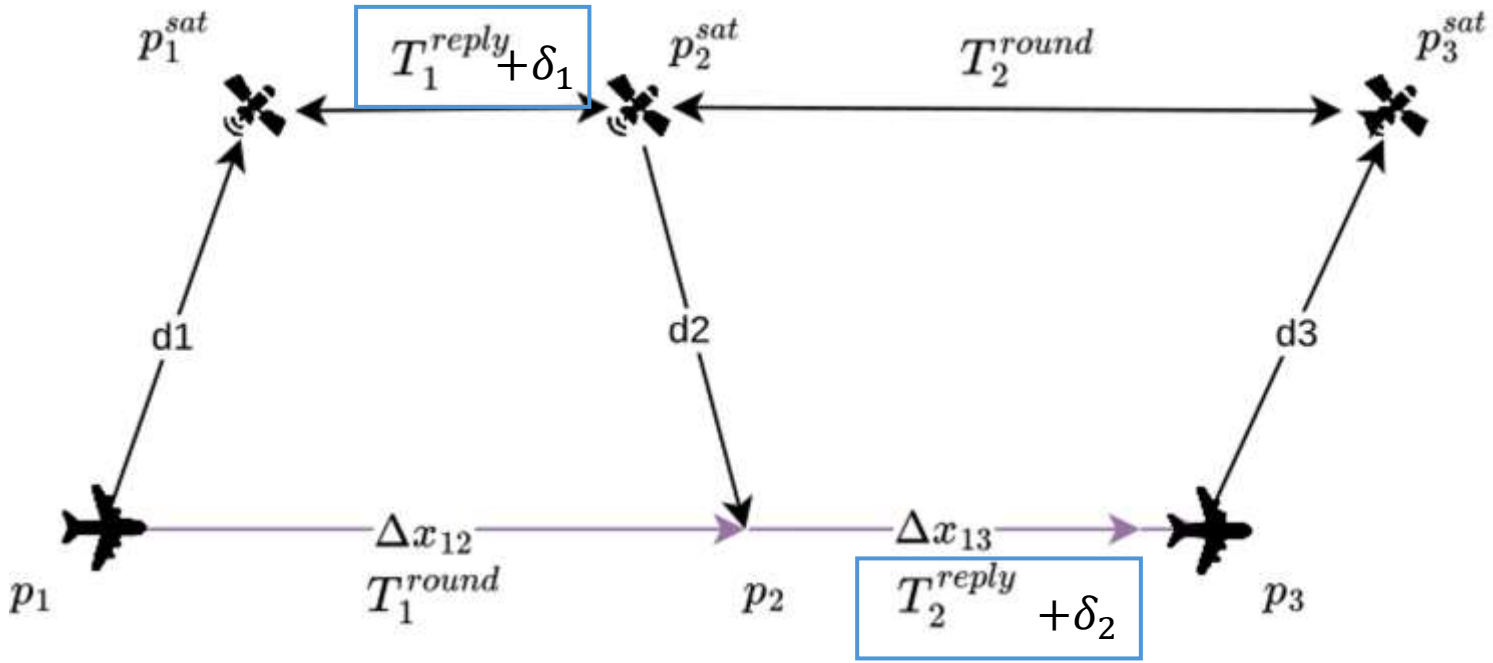


≈

Trade-off



Privacy Preserving TWR in LEO



- Satellites and user move during the TWR measure
- Longer reply times increases the displacement
- TWR computes an average of the three distances

Shortcomings of a Strawman Approach

Static satellite

$$d_{twr} = \|p - p_1^{sat}\|$$

Large Errors

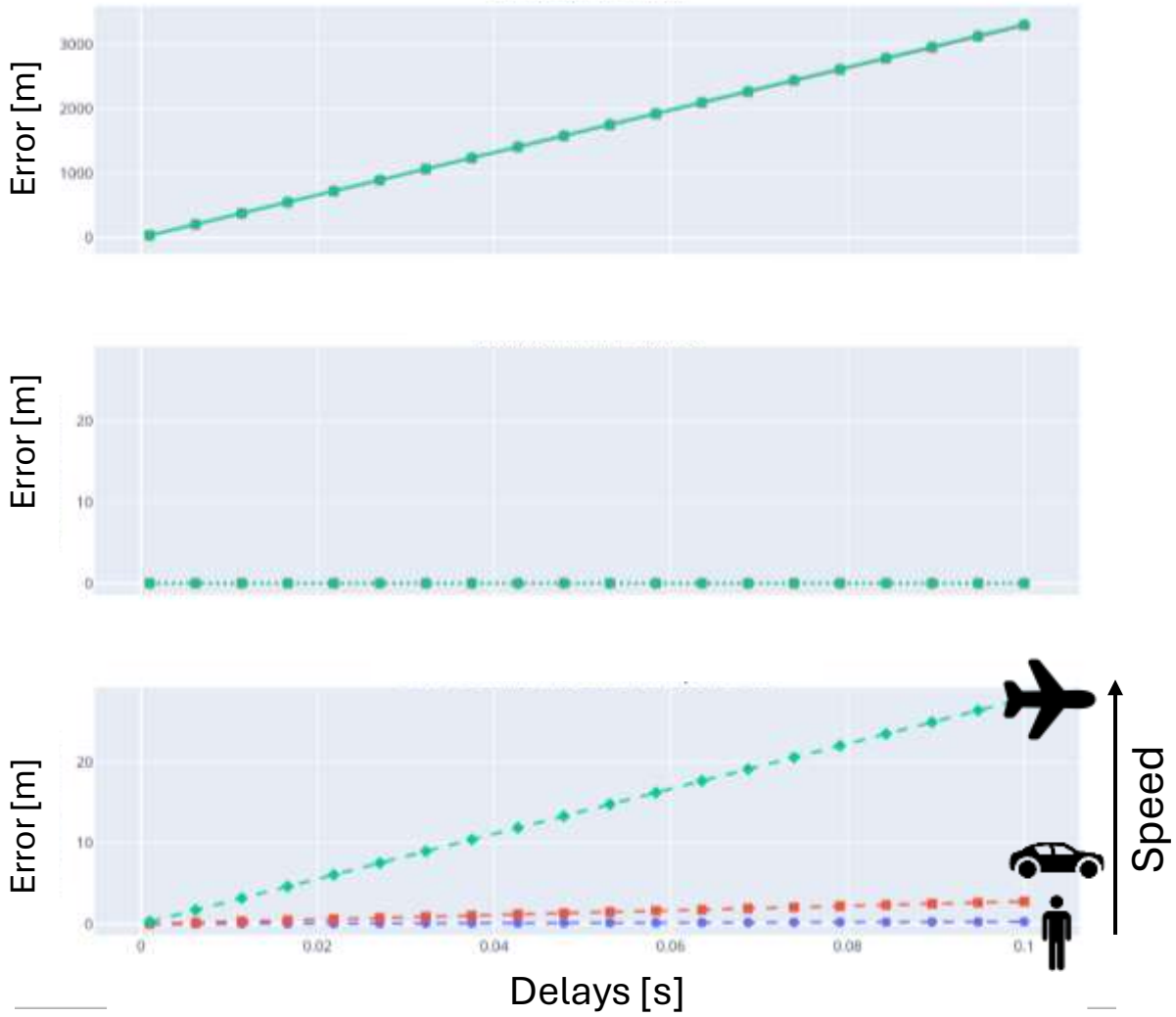
Moving satellite

$$d_{twr} = \frac{\|p - p_1^{sat}\| + 2\|p - p_2^{sat}\| + \|p - p_3^{sat}\|}{4}$$

Smaller Error

- Measure the distance with three satellites using TWR and solve for (x,y,z)
- Problem: **satellites movements must be taken into account**

Shortcomings of a Strawman Approach

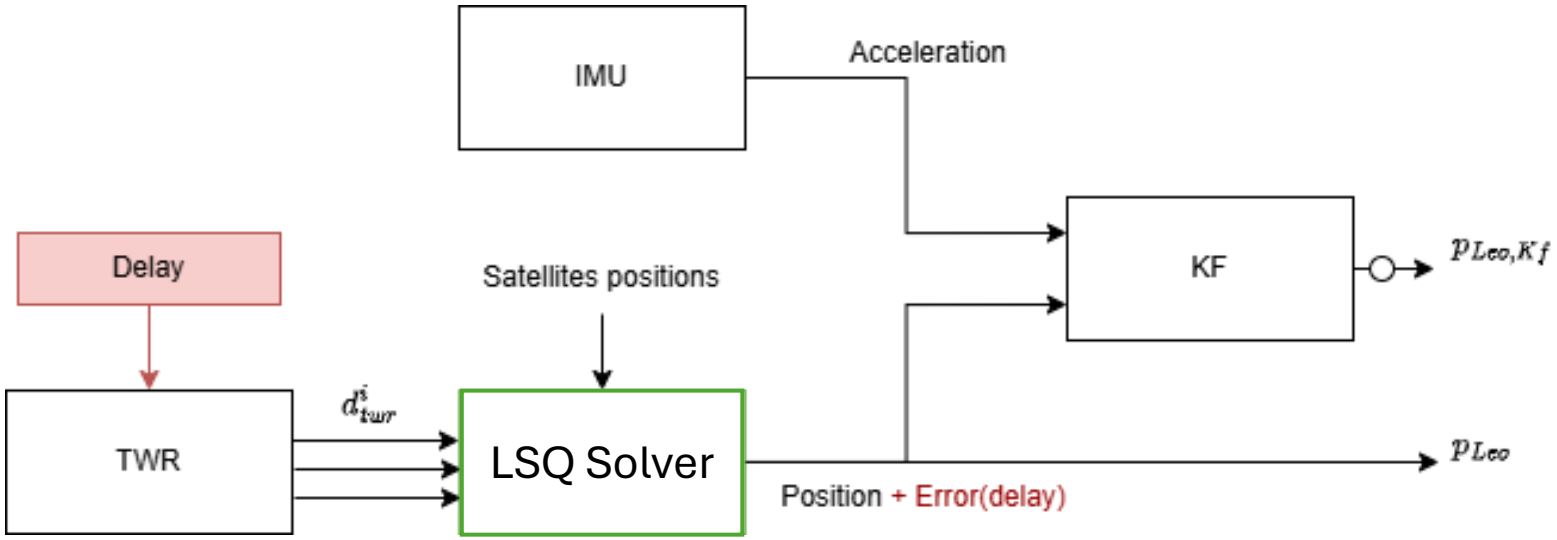


Strawman with Two-way Ranging

Strawman with Broadcast:
No error on the positions

Strawman TWR
with satellite compensation:
Fast moving object still have non negligible errors

Baseline: GNSS and IMU fusion

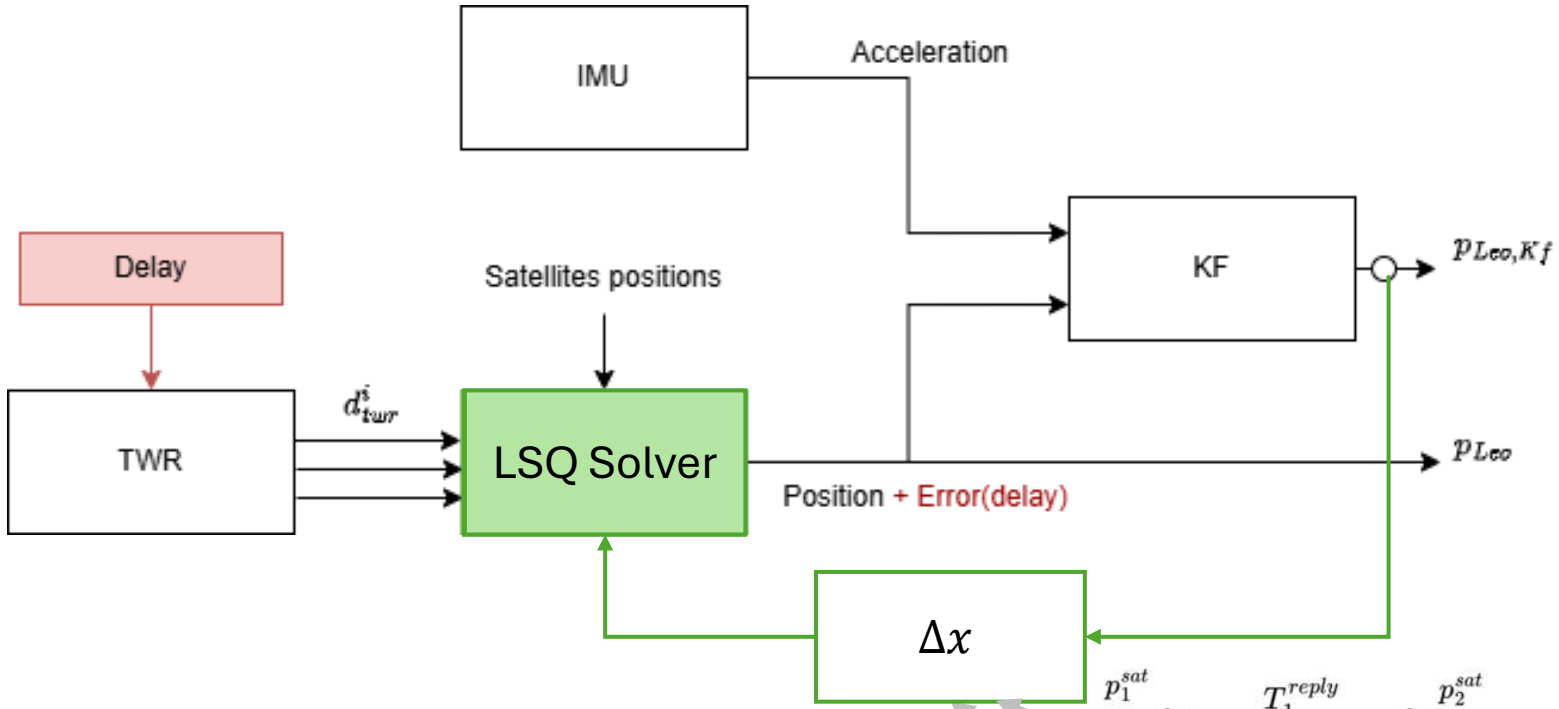


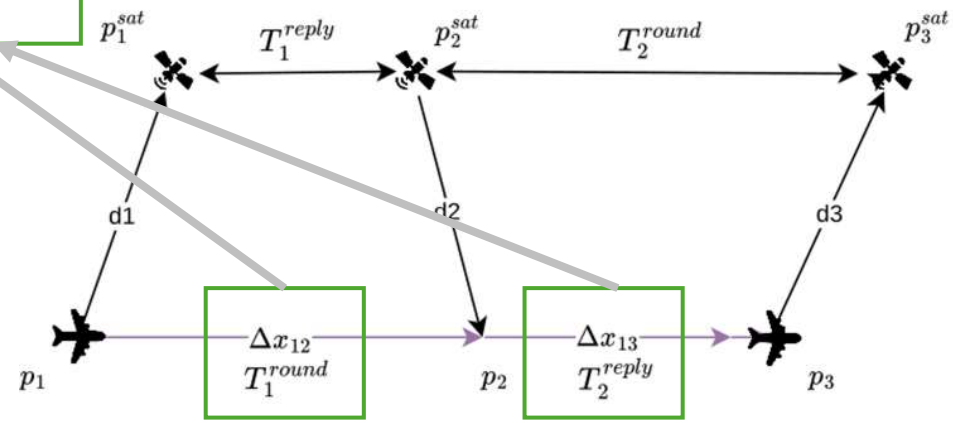
Baseline

- Compensate for satellite movement
- Inertial Measurement Unit (IMU)
- Kalman Filter to fuse GNSS and IMU measurements

Will the IMU compensate for the errors introduced by the user movement?

Our Solution: **LeoDelta**





Difference with typical sensor fusion

- GNSS and IMU measures are not independent
- The IMU displacements are fed back to the LSQ solver

Baseline vs LeoDelta

Baseline

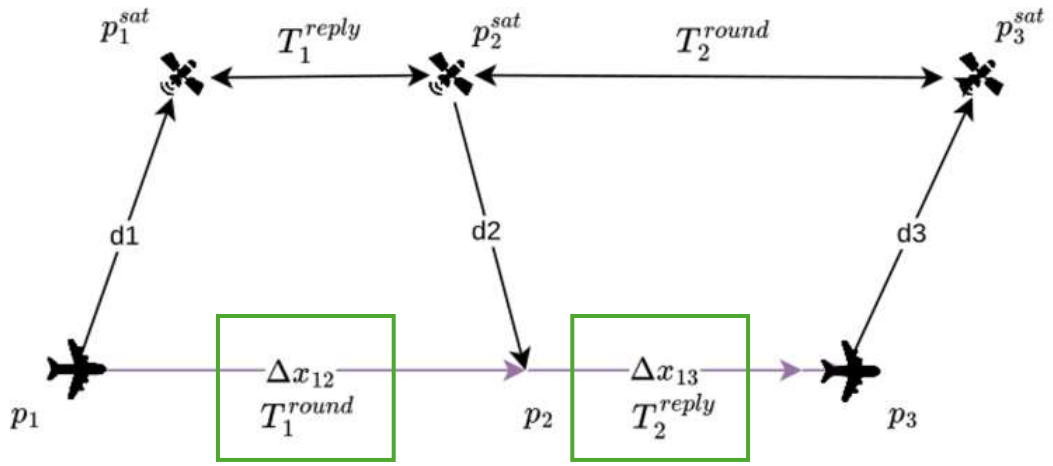
- Compensate for satellite movement
- **No feedback loop** for user movement
- Equation used by the LSQ solver:

$$d_{twr} = \frac{\|p - p_1^{sat}\| + 2\|p - p_2^{sat}\| + \|p - p_3^{sat}\|}{4}$$

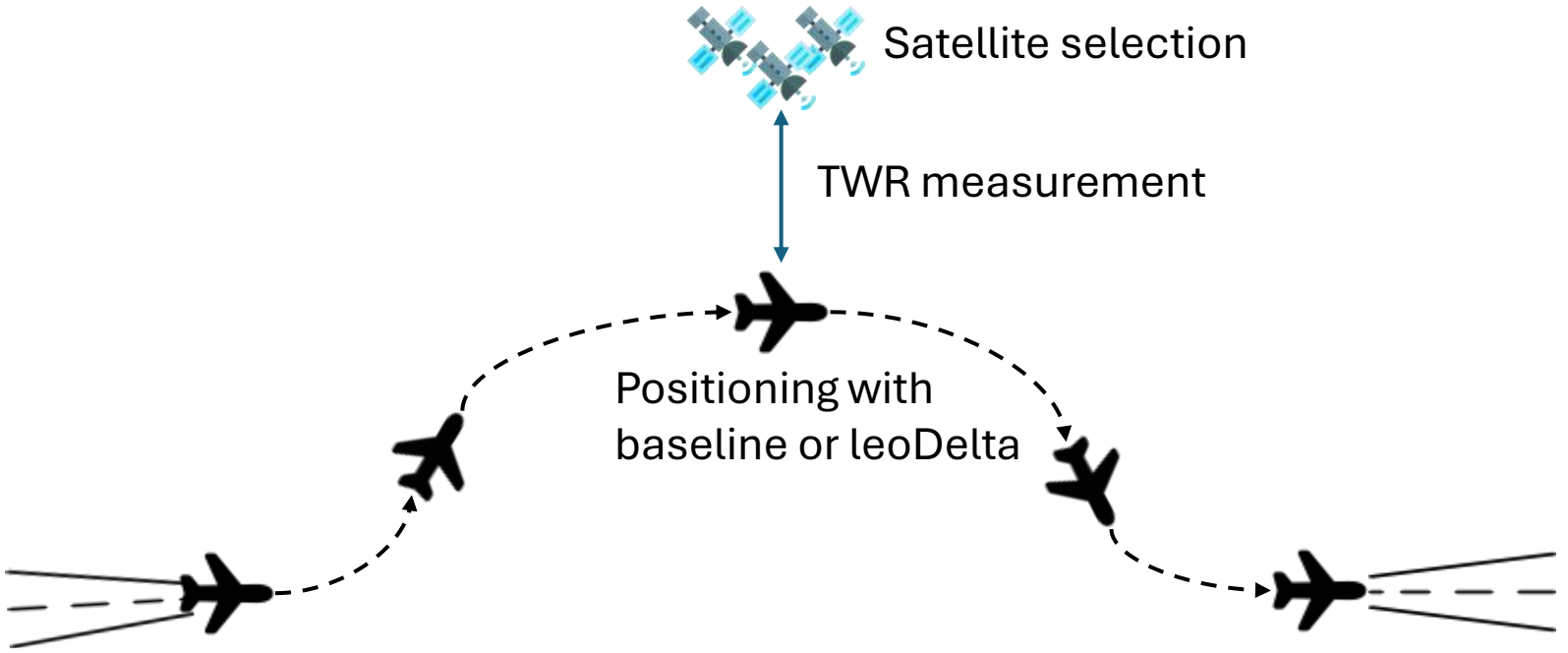
LeoDelta

- Compensate for satellite movement
- User **displacements during TWR** are **fed** back **to** the **LSQ solver**
- Equation used by the LSQ solver:

$$d_{twr} = \frac{\|p - \Delta x_{23} - \Delta x_{12} - p_1^{sat}\| + 2\|p - \Delta x_{23} - p_2^{sat}\| + \|p - p_3^{sat}\|}{4}$$



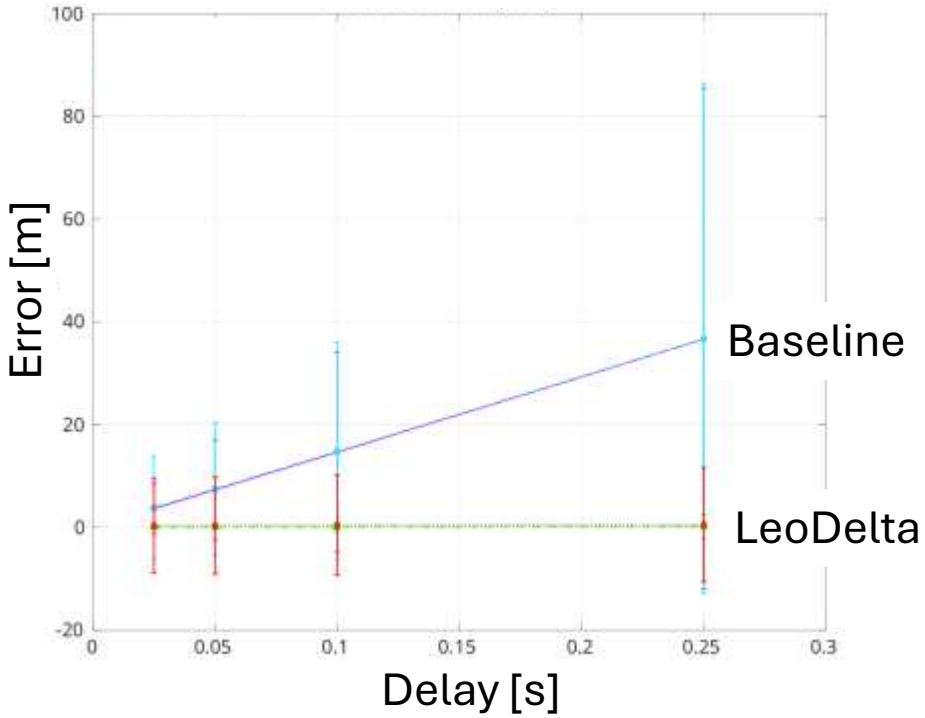
Evaluation



- 600 trajectories of planes in landing areas and while cruising
- We simulate a LEO satellite positioning system based on Starlink constellation
- Compare the **baseline** solution to **leoDelta**

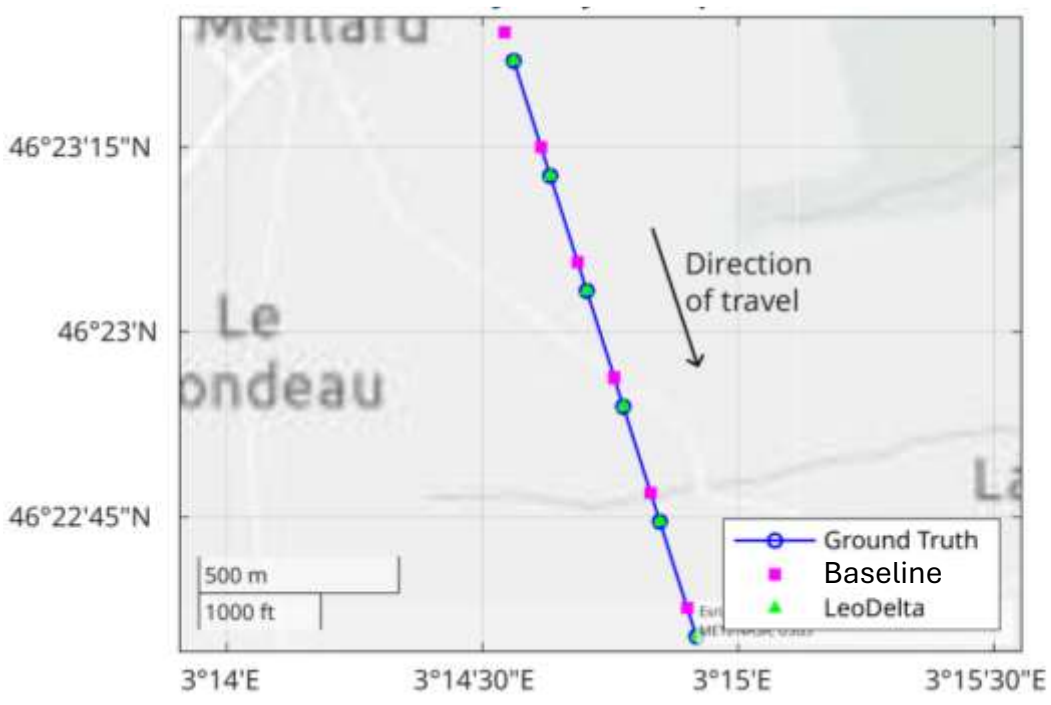
Results

LeoDelta vs Baseline



Without our compensation, the positioning error grows linearly in the delay (146 m/s)

Example Trajectory



The trajectory follows the correct one, but lags behind the correct position

Conclusions

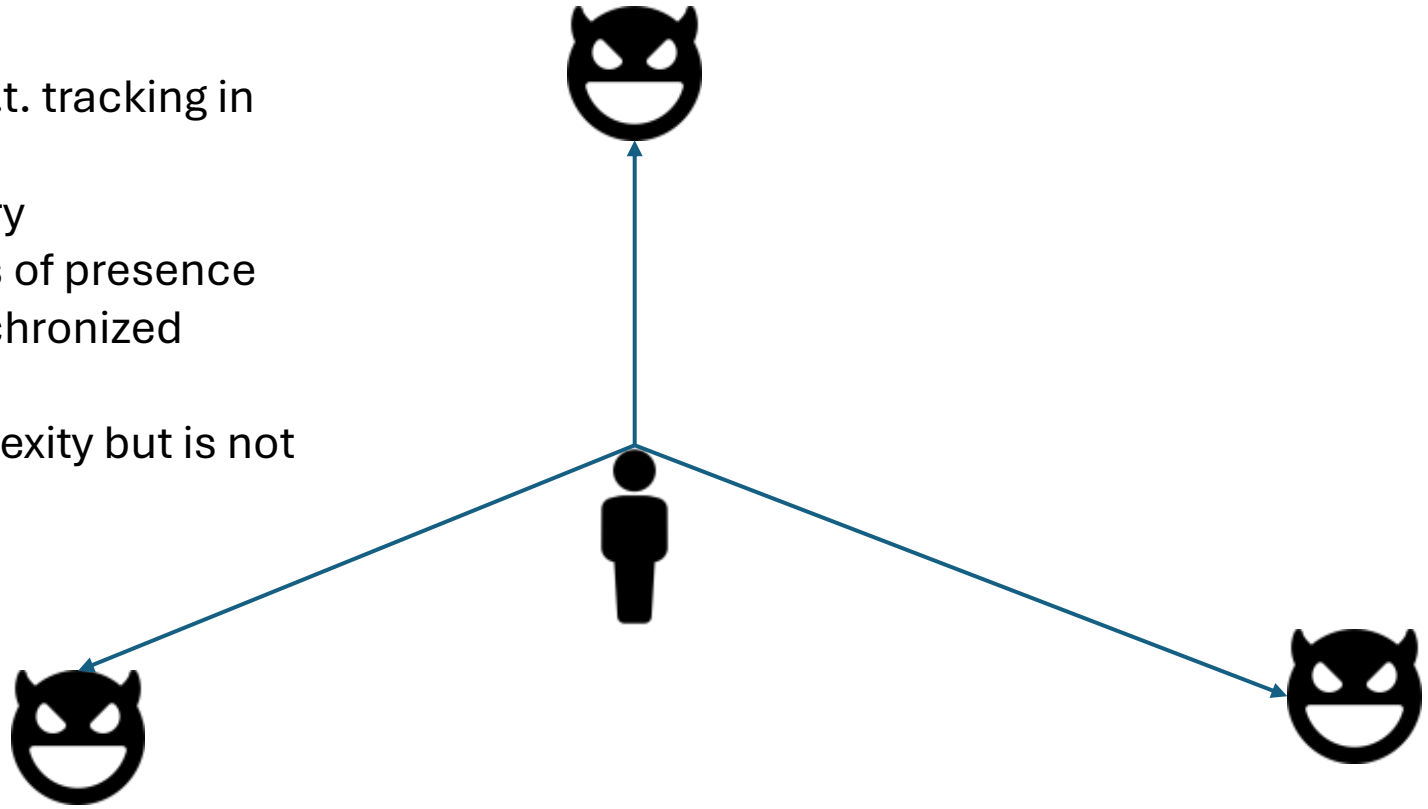
- TWR provides new opportunities as well as challenges in the future of secure positioning
- Privacy leakage for positioning systems based on TWR is a problem
- Existing countermeasures introduce positioning errors for fast moving targets
- The short-term stability of an IMU is sufficient to correct for such errors

Location Leakage for Active Users

An adversary with three points of observation can triangulate a user that is transmitting.
This requires significantly more effort w.r.t. tracking in case of twr:

1. 3 anchors and receivers are necessary
2. The adversary must have three points of presence
3. The adversary receivers must be synchronized

Our solution increases the attack complexity but is not a silver bullet.



Location Leakage in TWR