Toward Robust Wireless Localization in 6G Networks

Rethinking Wireless Protocol Design for the 6G Era

Alireza Pourafzal, Ph.D.

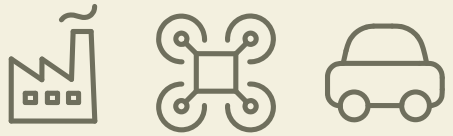
Department of Electrical Engineering
Chalmers University of Technology
Gothenburg, Sweden
email: alireza.pourafzal@chalmers.se

About Me

Alireza Pourafzal, Ph.D.

Department of Electrical Engineering
Chalmers University of Technology
Gothenburg, Sweden

Paradigm Shift: From Data Pipe to Sensor



Traditional View (4G/5G-L)

Design: Communication-Centric (Co-Co)

Goal: Maximize spectral/energy efficiency.

Output: Decoded bits.

The network is viewed as a bit-transport medium.

The ISAC Paradigm (5G-H/6G)

Design: Distributed Radar/Sensor Array

Goal: Jointly optimize Comm (R) & Sensing (S).

Output: Data AND geometric/kinematic parameters.

Every uplink transmission acts as a radar pulse.

Intrinsic Sensing Capability

Time & Range

Time-of-Arrival (ToA)

Wideband OFDM Signals.

Space & Direction

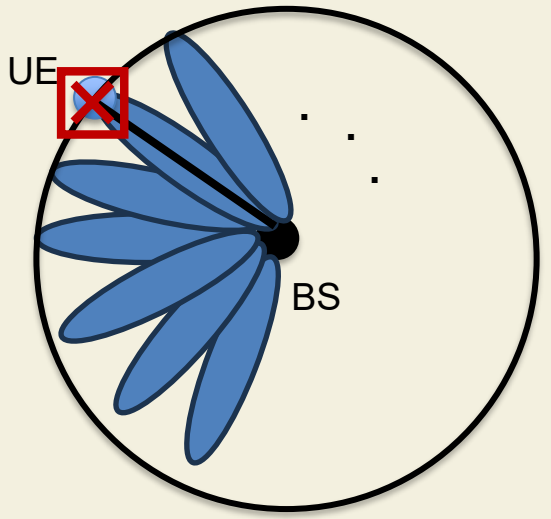
AoA & AoD

Beam Steering to have good SNR at UE

Environment

NLoS Reflections

If there is a reflection, there is a “landmark”



Experimental Validation

Single-Anchor mmWave Positioning

Setup: Commercial 5G mmWave Base Station (~28 GHz) and a vehicle with custom UE receiver & high-precision GNSS/IMU.

Mechanism: Deterministic beam sweeping + UE channel estimation.

Result: Approx. 2m positioning error (90th percentile) in LoS scenarios.

Mapping: Successfully reconstructed scattering points on building façades using multipath components.

Ge, Y., ... & Wymeersch, H. (2024). Experimental validation of single BS 5G mmWave positioning and mapping for intelligent transport. IEEE Transactions on Vehicular Technology, 73(11), 16744-16757.

Twist: From Sensing To Tracking & Attacks

Accurate PHY feature estimation  Accurate Localization and Tracking

The Risk of Localization without User Consent

The geometric information (CSI) is extracted directly from the physical layer (pilots/RSs).

- Standard-compliant receivers can process signals as passive radar.
- Bypasses application-layer encryption and permissions.
- Enables tracking without consent.

Angle-Based Authentication

Provides a physical-layer location fingerprint for device authentication

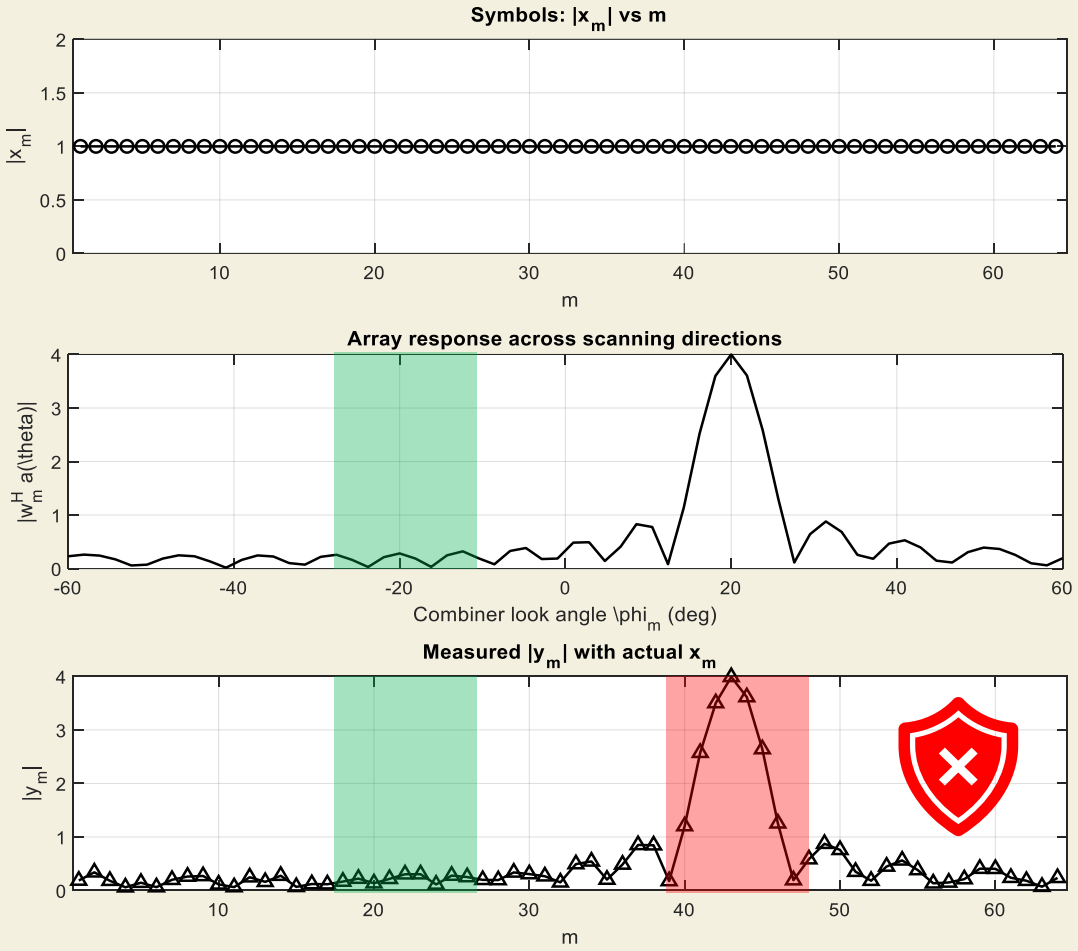
Challenge
Presenting a task or signal for user interaction.

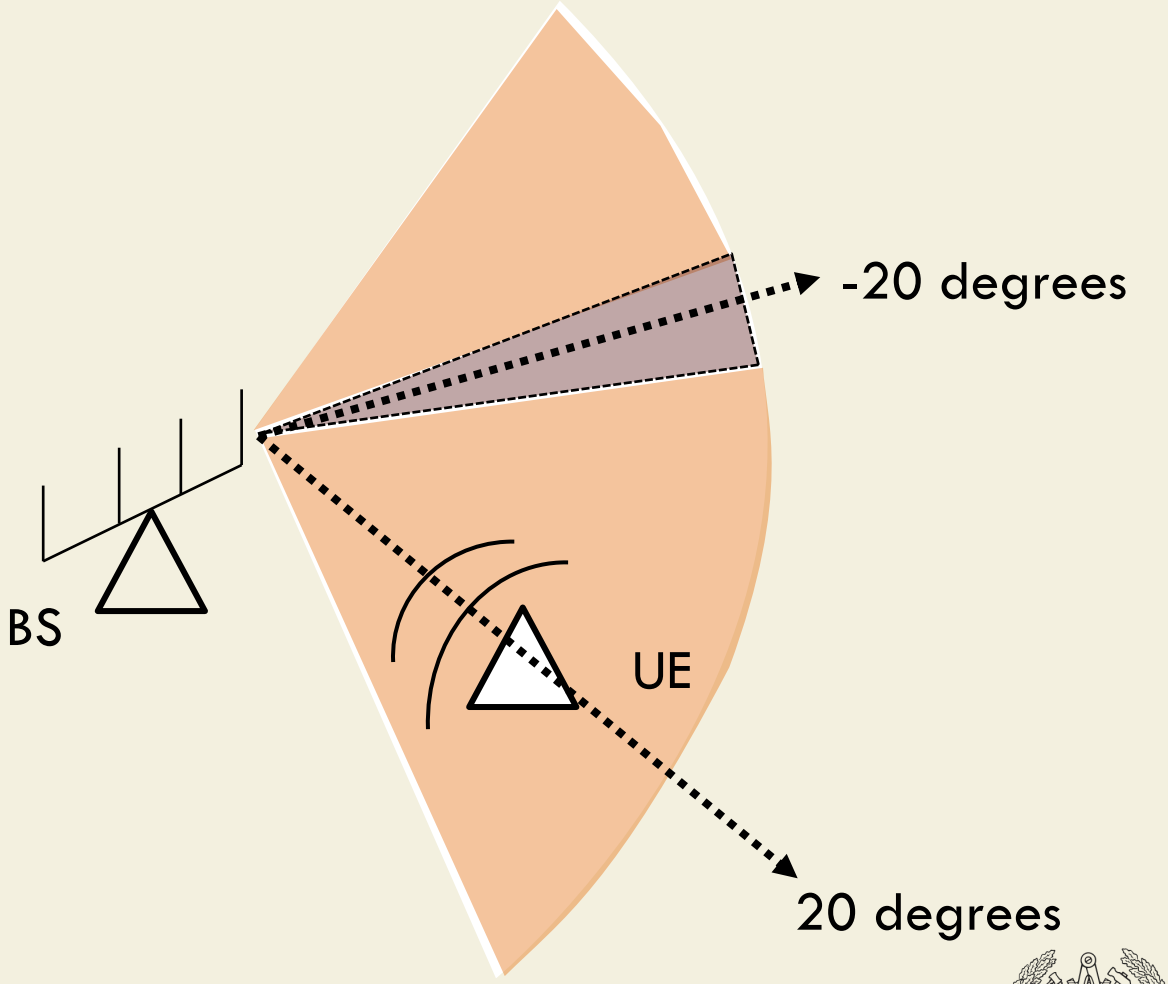
Decision
Final approval or outcome based on previous steps.

Enrollment
Initial sign-up and registration process for new users.

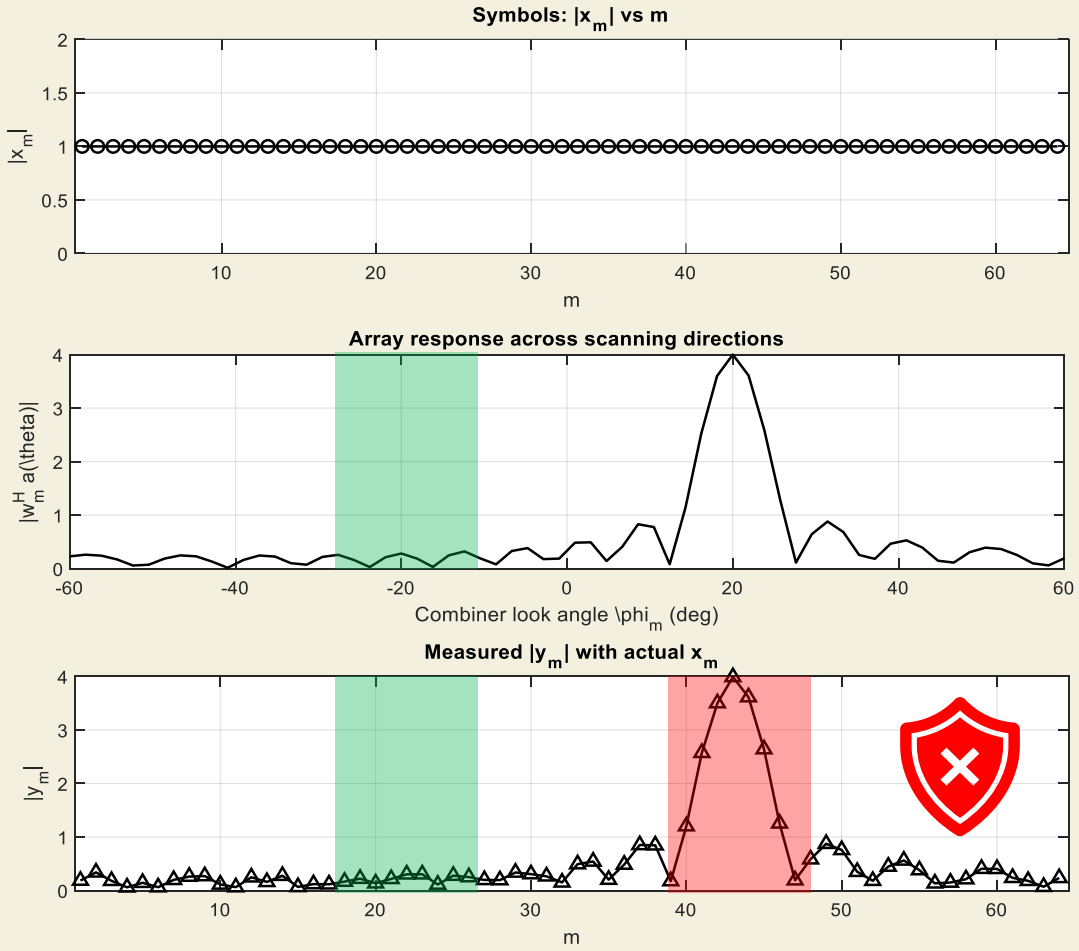
Verification
Confirming identity or action with a security check.

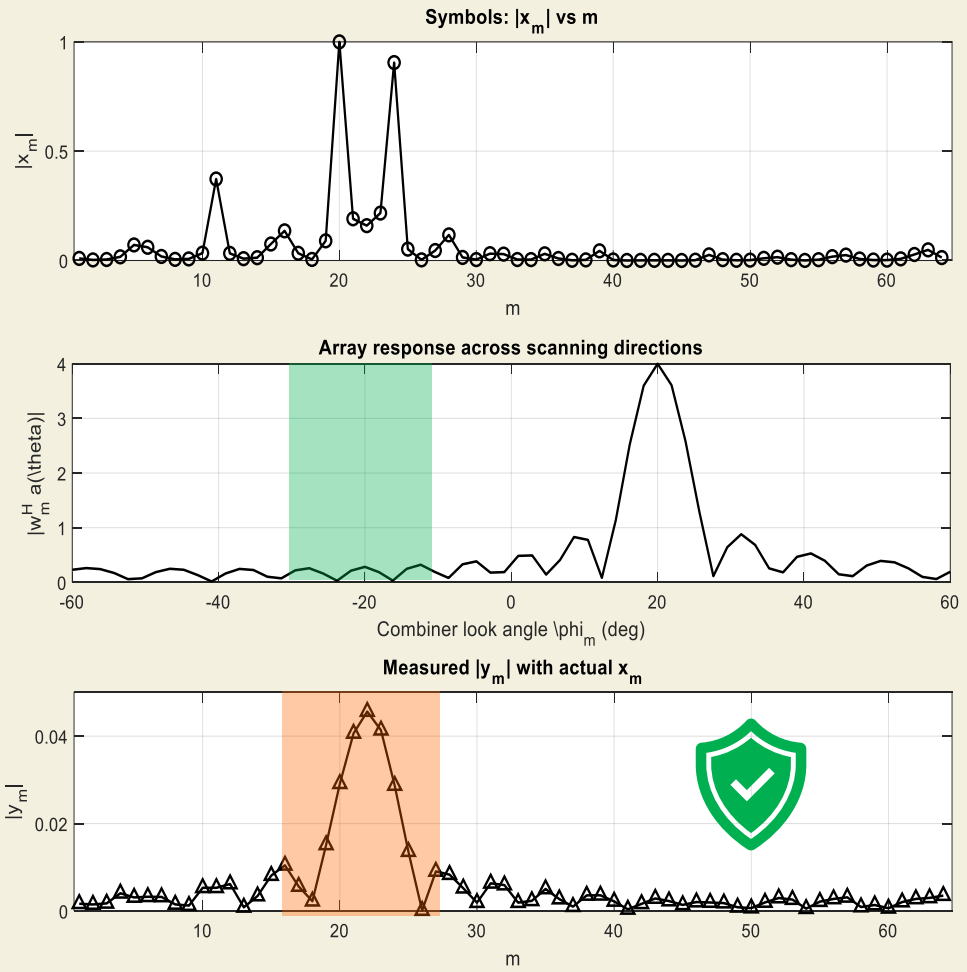
Fragility of Analog Arrays





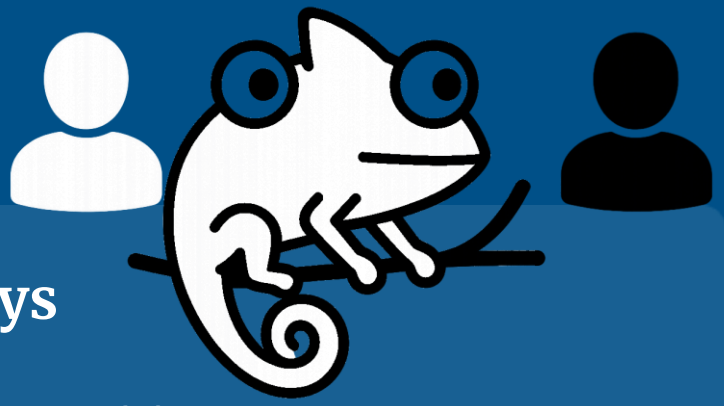
Fragility of Analog Arrays





M. Srinivasan, … , and H. Wymeersch, "AoA-based physical layer authentication in analog arrays under impersonation attacks," in Proc. 2024 IEEE 25th Int. Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 2024, pp. 495–500.

Extension to Hybrid Architectures

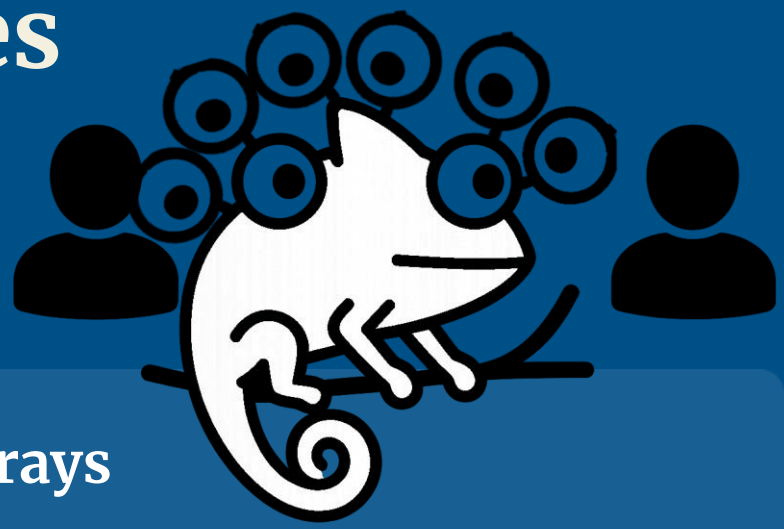


Hybrid Arrays

Single Eve not successful

Cooperative Attack

Pourafzal et al. "Cooperative Impersonation in Angle-Based Physical Layer Authentication." In ICC 2025-IEEE International Conference on Communications, pp. 3321-3326. IEEE, 2025.



Digital Arrays

Not viable to Attack

Expensive Equipment

T. M. Pham et al., “Machine learning-based robust physical layer authentication using angle of arrival estimation,” in GLOBECOM 2023 IEEE Global Communications Conference. IEEE, 2023, pp.13–18.

Enforcing Location Privacy at PHY Layer

Goal & Limitations

Goal: User control over inferred location (Privacy) and defense against manipulation (Integrity).

Limitations: Traditional higher-layer privacy (pseudonyms, encryption) fails completely against PHY-layer tracking mechanisms.

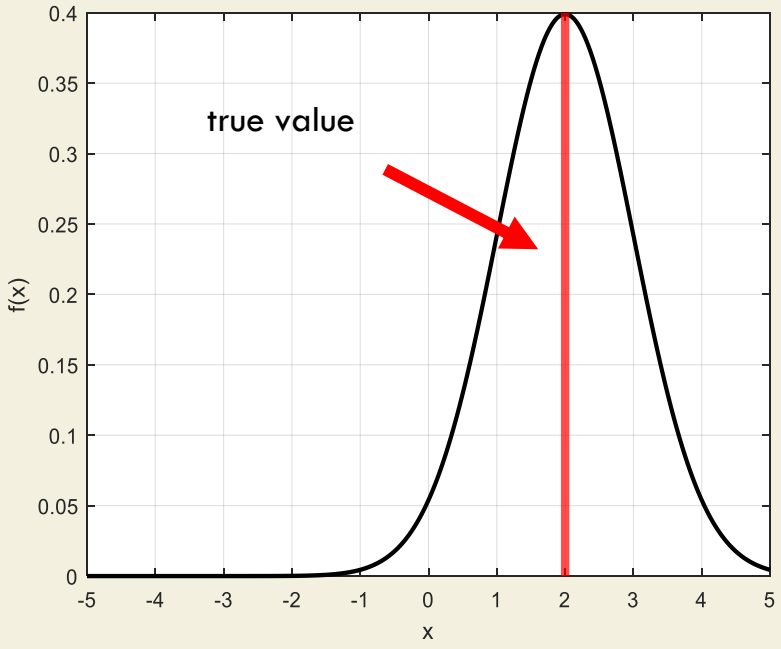
User Location Privacy

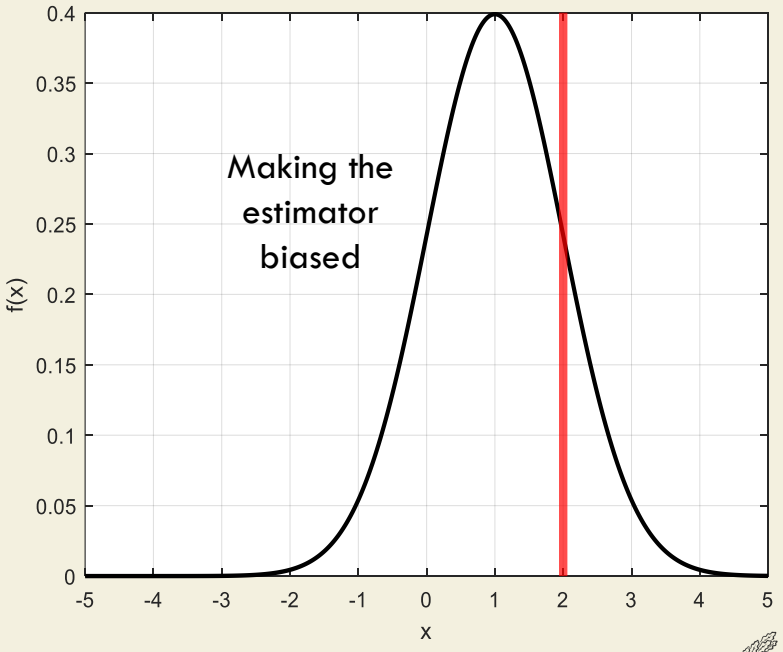
1. Obfuscation: Introducing controlled noise or signal modification to degrade the localization Cramer-Rao Bound (CRB).

2. Spoofing (Concealment): Actively pushing the estimated location to a specific, arbitrary fake position.

Physical-Layer Location Privacy

- BS acts as an estimator of location parameters $(\hat{\tau}, \hat{\theta})$
- Estimator accuracy governed by SNR and resources available (bandwidth, aperture)
- **User strategy**: corrupt the estimator's input so that its output (location) is unreliable.





CHALMERS UNIVERSITY OF TECHNOLOGY

Variance Attack: Adding Artificial Noise

Eve transmits

Artificial Noise Samples

$$x_m = \sqrt{1-\beta}\,\bar{x}_m + \beta z_m$$

Effective pilot SNR at BS

$$\mathrm{SNR} = \frac{(1-\beta)P|\alpha|^2}{\beta P|\alpha|^2 + N_0}$$

Estimator CRB examples

ToA variance: $\mathrm{var}\,(\hat{\tau}) \propto 1/(\mathrm{SNR} \times \mathrm{Bandwidth})$

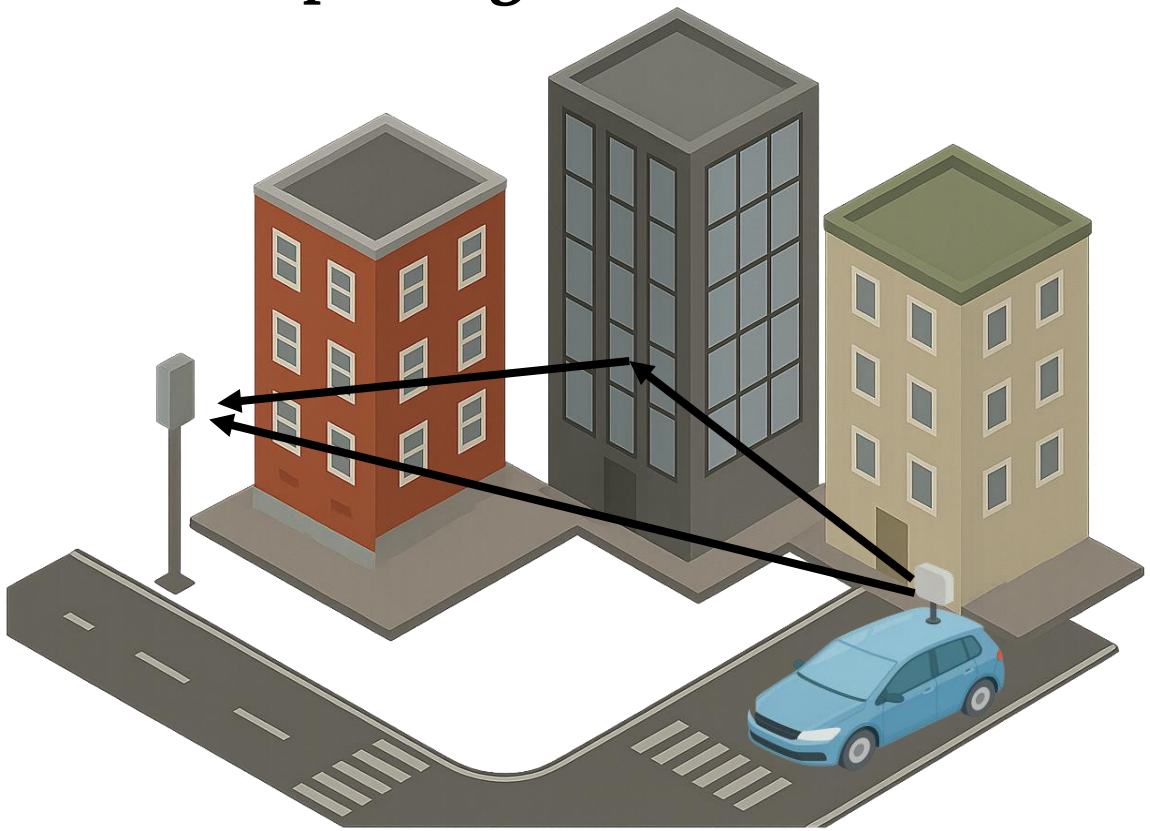
AoA variance: $\mathrm{var}\,(\hat{\theta}) \propto 1/(\mathrm{SNR} \times \mathrm{Beam\ Resolution})$

More AN → lower SNR → larger variance → poorer localization.

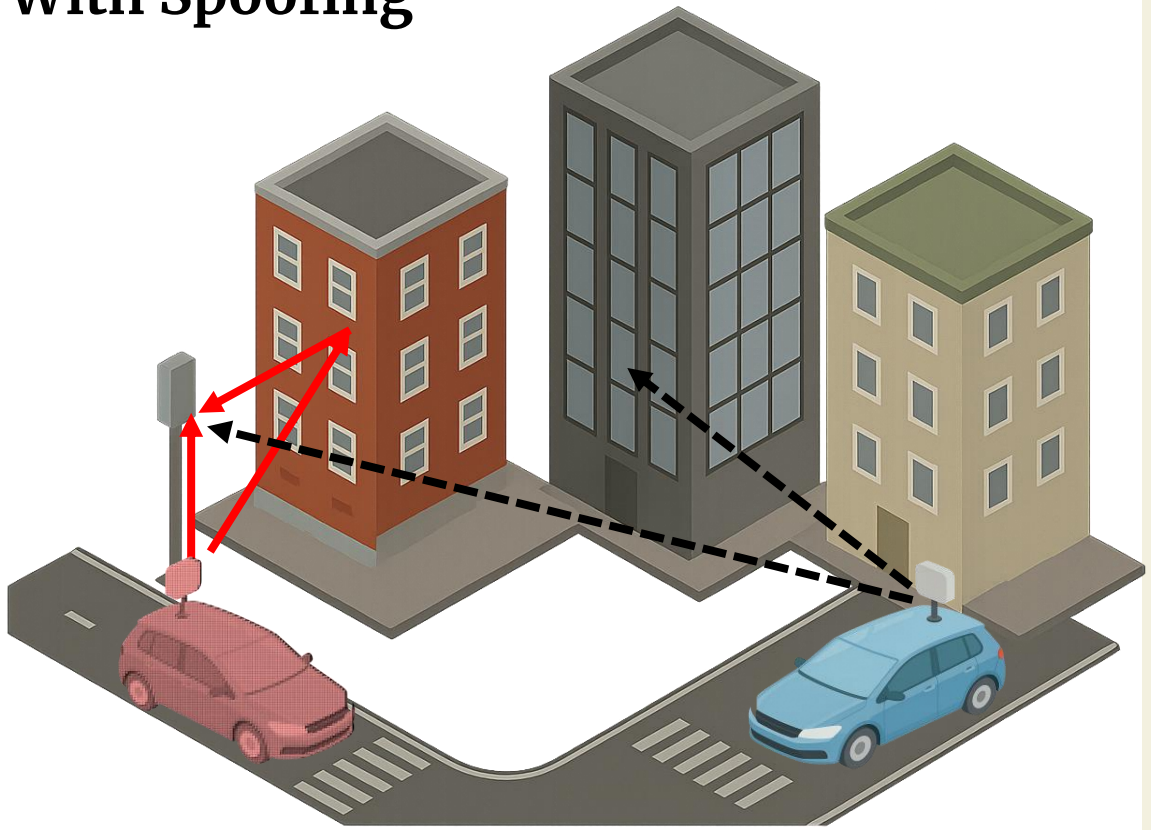
Y. Zhang, Hui Chen, and Henk Wymeersch. "Privacy preservation in delay-based localization systems: Artificial noise or artificial multipath?." In GLOBECOM 2024-2024 IEEE Global Communications Conference, pp. 2755-2760. IEEE, 2024.

Transition into bias-based attacks

Without Spoofing



With Spoofing



Transition into bias-based attacks

HoloTrace Oracle

Analog array

No Synchronization

Requires CSI Knowledge

Italiano, Lorenzo, Alireza Pourafzal, Hui Chen, Mattia Brambilla, Gonzalo Seco-Granados, Monica Nicoli, and Henk Wymeersch. "HoloTrace: a Location Privacy Preservation Solution for mmWave MIMO-OFDM Systems." (2025).

HoloTrace Blind

Analog array

No Synchronization

CSI-Free

Italiano, Lorenzo, Alireza Pourafzal, Hui Chen, Mattia Brambilla, Gonzalo Seco-Granados, Monica Nicoli, and Henk Wymeersch. "HoloTrace: a Location Privacy Preservation Solution for mmWave MIMO-OFDM Systems." (2025).

DAIS

Hybrid array

Synchronized

CSI-Free

Li, Jianxiu, and Urbashi Mitra. "Delay-Angle Information Spoofing for Channel State Information-Free Location-Privacy Enhancement." arXiv preprint arXiv:2504.14780 (2025).

Case Study: HoloTrace

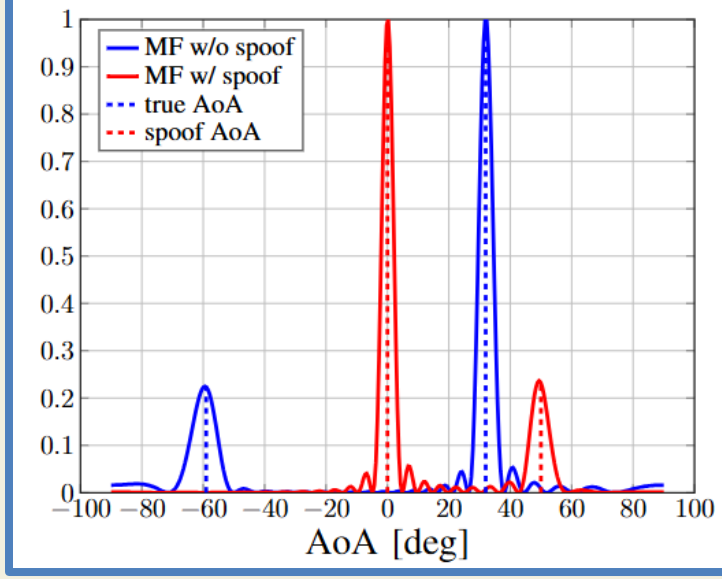
Waveform-Level Spoofing

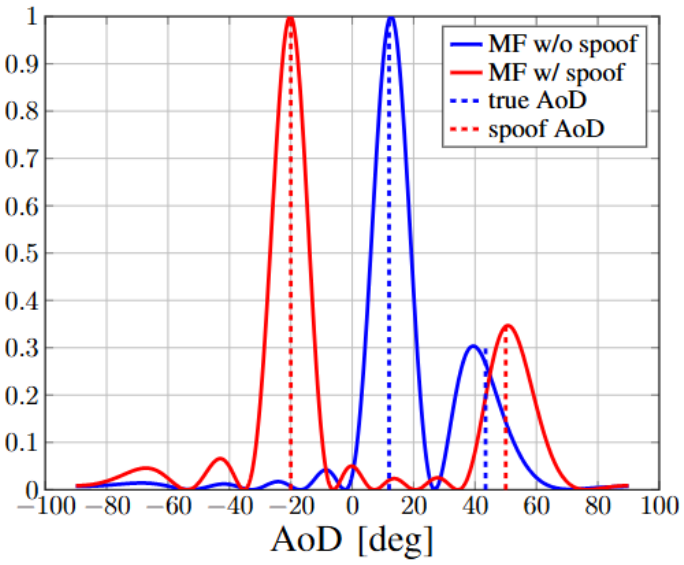
Problem: Spoof location while maintaining high Comm Rate.

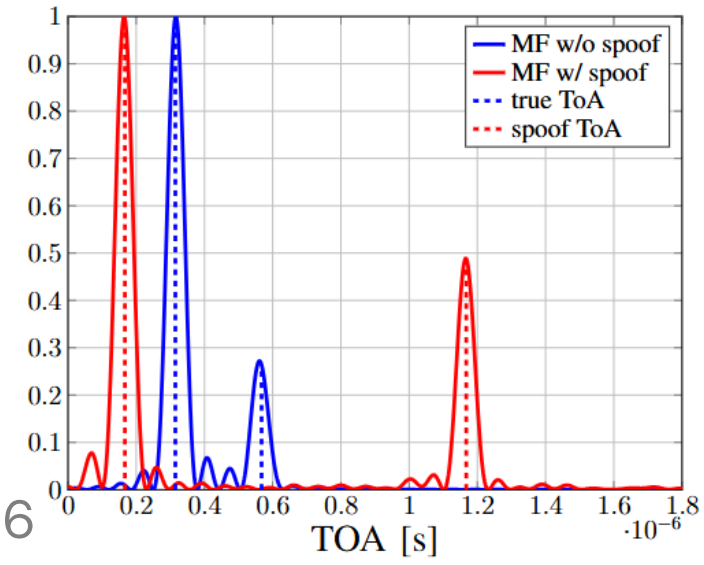
Mechanism: The UE attempts to find minimal pilot perturbation such that the channel response maps to a fake location.

$$\mathbf{y} = \text{diag}\,(\mathbf{x})\mathbf{A}(\boldsymbol{\theta})\boldsymbol{\alpha} + \mathbf{n} \qquad \text{Spoofing: } \underset{\mathbf{x}}{\text{argmin}} \left|\left|\mathbf{y} - \mathbf{A}(\boldsymbol{\theta}_{Fake})\boldsymbol{\alpha}_{Fake}\right|\right|$$

Outcome: The BS estimates geometric parameters AoA and TDoA that map to Fake Points

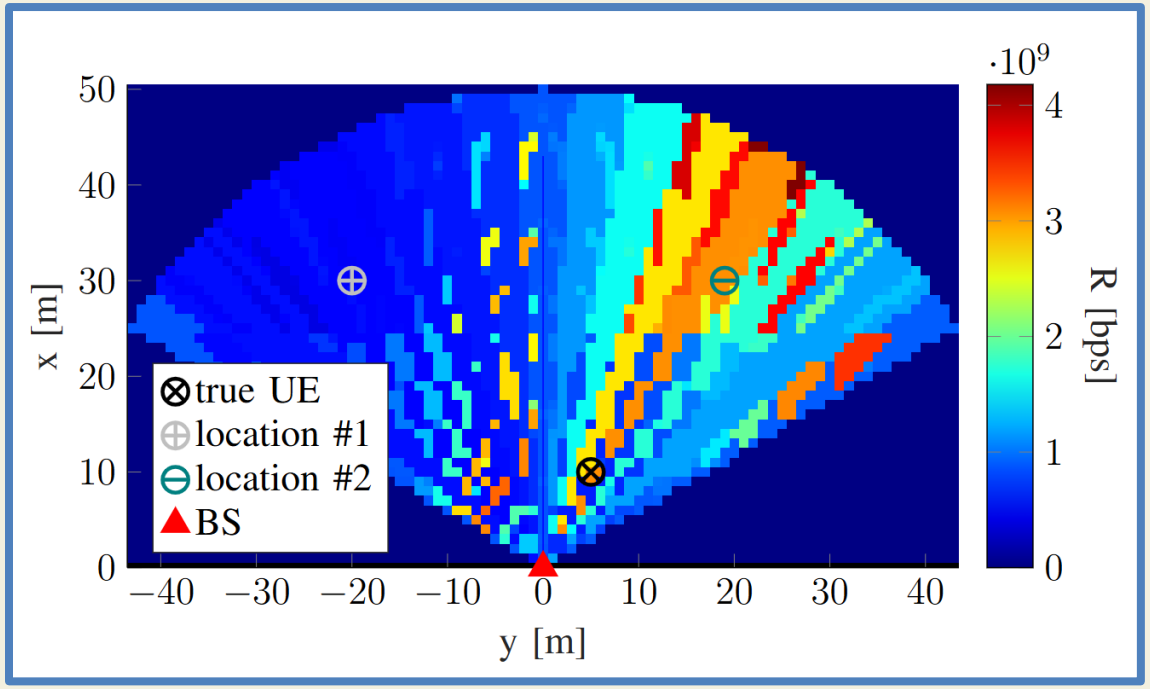






Conclusion & Open Directions

- 5G / 6G networks act as distributed sensor arrays
- Real experiments: single-BS 5G mmWave can do meter-level positioning + mapping
- Location privacy at PHY: user can distort or spoof its geometric



HoloTrace: Different Spoofed Locations resulted in Different Communication Capabilities

Thank you for your attention.

Questions?

Toward Robust Wireless Localization in 6G Networks

Alireza Pourafzal, Ph.D.

Department of Electrical Engineering
Chalmers University of Technology
Gothenburg, Sweden
email: alireza.pourafzal@chalmers.se