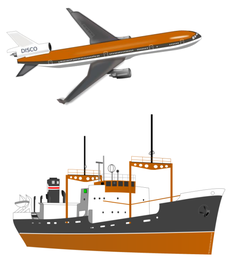
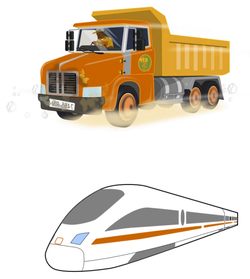


Secure Path Verification

using mobility-differentiated time of arrival



Technische Universität Kaiserslautern

Matthias Schäfer[†] Vincent Lenders[‡] Jens Schmitt[†]

[†] disco, TU Kaiserslautern, Germany [‡] armasuisse, Switzerland

disco distributed computer systems

Problem

- Imagine a car, train, plane, ship, … moving along a **path** and reporting its **location** periodically

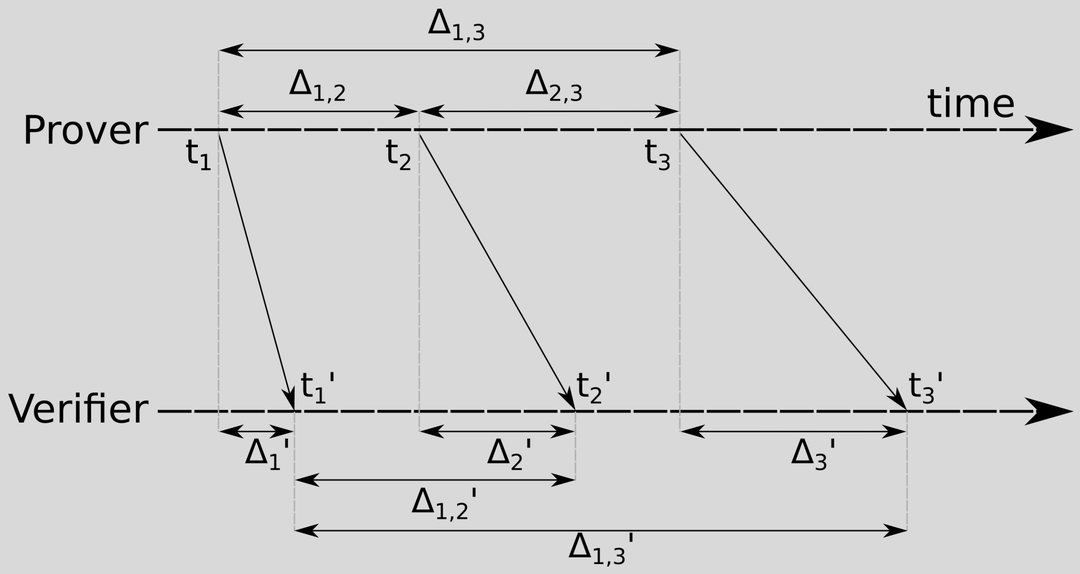
  ⇨ path claim := sequence of location claims
- E.g. traffic management and collision avoidance rely on this information
- Claiming fake paths could have life-threatening consequences

How to verify that a mobile node really moves along the claimed path?

- Existing location verification schemes require specialized protocols, tight time synchronization, or special-purpose hardware

Idea

- Mobility is not a challenge, it's a feature!



- Inter-arrival time $\Delta_{i,j}'$ differs from inter-transmission time $\Delta_{i,j}$ by the change in propagation delay
- **Principle:** Verifiers at different positions check this condition:

$$\Delta_{i,j}' \stackrel{?}{=} \Delta_{i,j} + (\Delta_j' - \Delta_i')$$

Results

Benefits

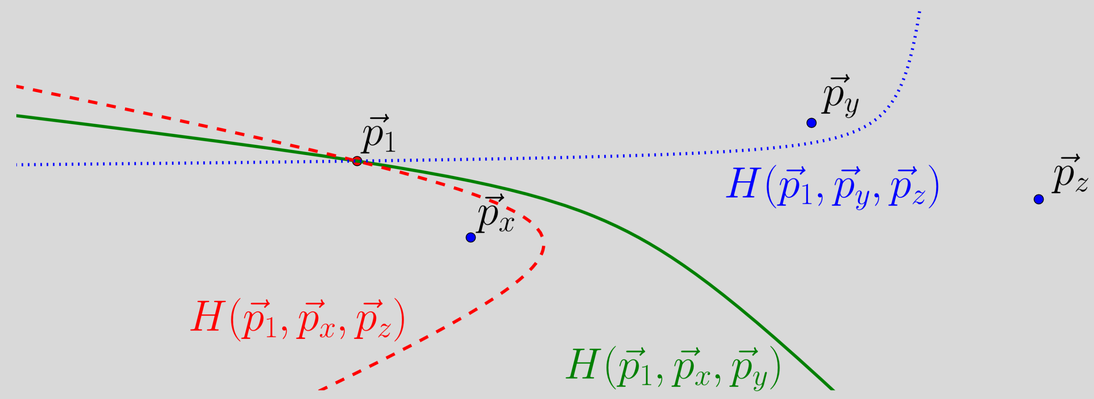
- No time synchronization needed
- No extra communication needed

Security

- Attacker: stationary, omni-directional antenna, knows everything
- Single verifier can be tricked easily by adjusting the transmission times
- Increasing number of verifiers reduces attacker's degree of freedom quickly and significantly
- Attacker can only claim positions where the differences in propagation delays to each verifier don't change ⇨ only holds for intersections of pairwise hyperbolas H
- There are *at most 2* intersections for three verifiers

Illustration

- 3 verifiers located at p_x, p_y, and p_z
- Attacker falsely claims to be at p_1



⇨ there is no position left which could be undetectably spoofed by the attacker ✓

Practical Considerations

- We face measurement errors and clock drifts in practice
- Consider likelihood instead of Boolean decision variables