Secure Systems Group, University of Helsinki

Andrey Shorov and Valtteri Niemi

Privacy issues of autonomous shared vehicles

Motivation

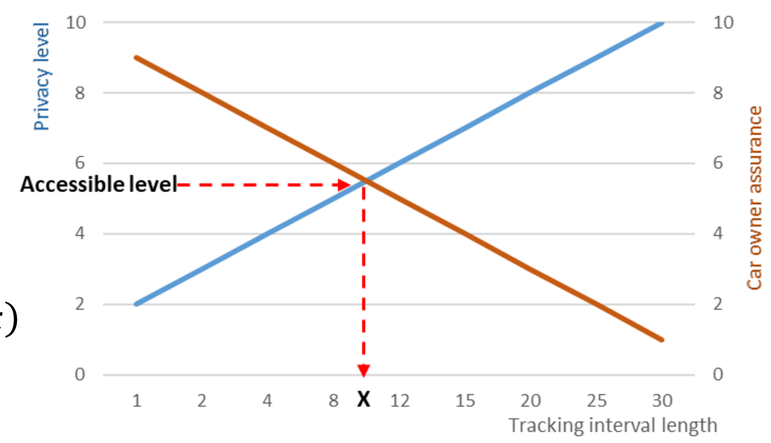
- Autonomous vehicles are an important car sharing service scenario
- Car sharing operators track users continuously during user trip → privacy concerns
- One option is to refuse continuous tracking and to use selective tracking interval
- It is important to find a trade-off between user privacy and car owner assurance

Privacy calculations

- We focus on location privacy i.e. how to preserve uncertainty about user path while maintaining assurance for car owner
- How to find privacy level that satisfies both user and car owner?

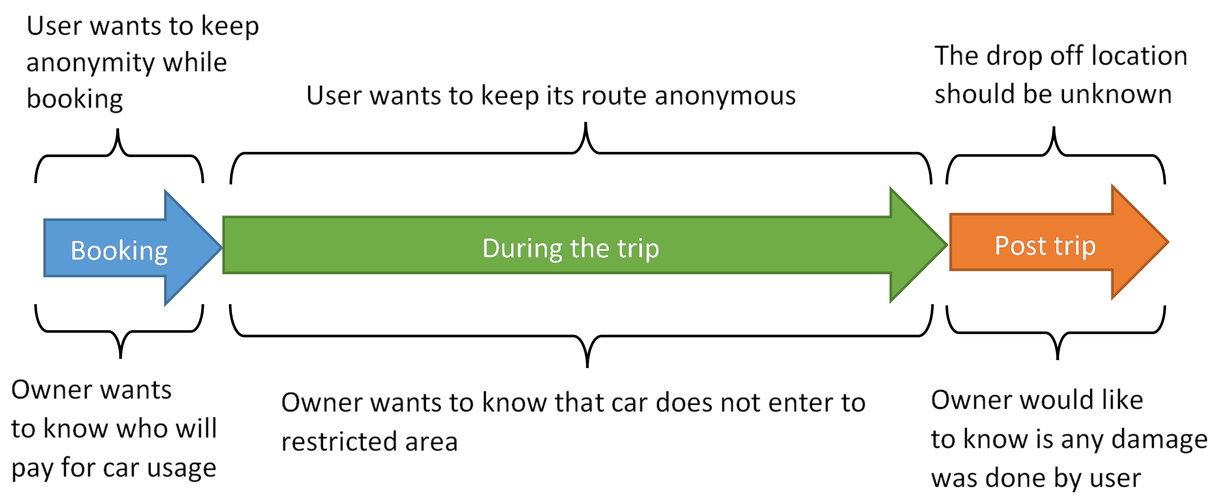
Shannon Entropy measures adversary uncertainty:

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x)$$

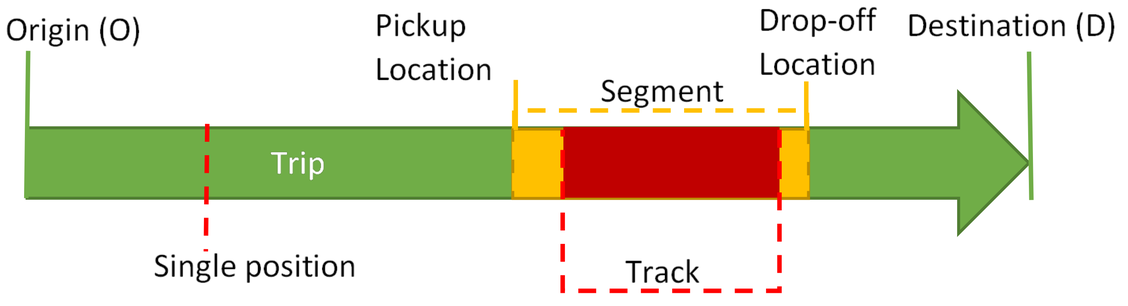


Design

- Three phases of service timeline

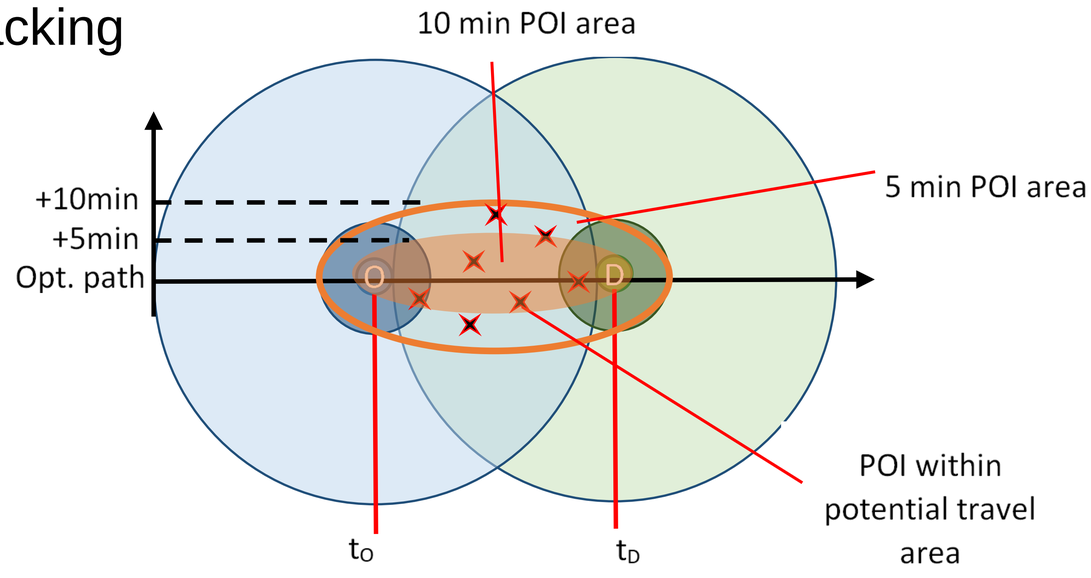


- Main focus on location privacy during the trip



Maximum movement boundary attack*

- Car owner can find visited POI even if no permanent tracking



- Attacker can find potential position of a user based on moving speed

Implementation

Google maps:

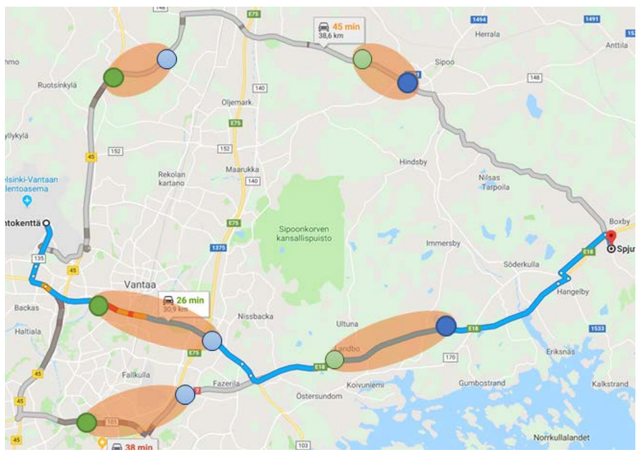
- Both user and vehicle owner can find potential path
- User can choose most private path
- Car owner can evaluate where is user at moment
- Library can be embedded to maps applications

Design consideration using attack principle

- No stop probability based on lognormal distribution
- Probability of visit POI using mean time to visit and POI rating with help of normal distribution
- Total entropy for path created by Google maps

Another way of use:

- Path can be recovered if user was spotted between two points
- If surveillance spots are known, user can increase its privacy during journey



UNIVERSITY OF HELSINKI

*Ghinita G, et al. (2009) Preventing velocity-based linkage attacks in location-aware applications. Proc. of the 17th ACM SIGSPATIAL int. conf. on advances in geographic information systems, pp 246–255