PRIVACY-PRESERVING TRAJECTORY COLLECTION

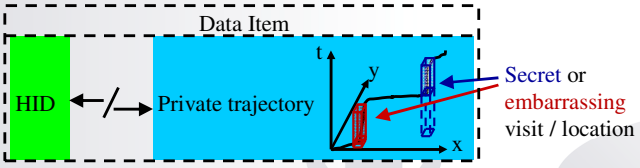
Győző Gidófalvi
Xuegang Huang and Torben Bach Pedersen

UPPSALA UNIVERSITET

AALBORG UNIVERSITY DENMARK GEOMATIC

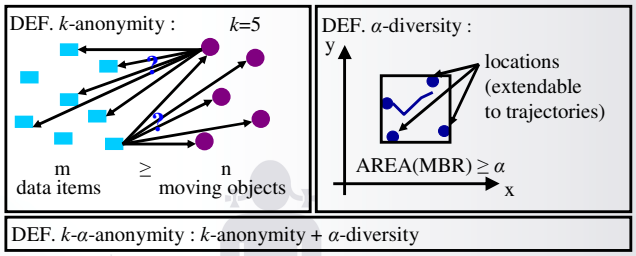
Problem Setting

Accurate trajectory patterns are necessary for Location-Based Services. A method that can collect exact trajectories in a privacy-preserving manner is needed. A method that uses free and energy-saving short-range P2P communication is desirable. However, during such communication a fixed hardware ID is exposed. Hence it is necessary that when a data item, which contains the private trajectory with possibly secret or embarrassing locations, is communicated, the link between public and private information is broken.



Location Privacy Definitions

k-anonymity requires that each data item can be associated with at least *k* moving objects and vice versa. *α*-diversity requires some spatial or spatio-temporal diversity in a set of locations / trajectories. Finally, *k*-*α*-anonymity combines the two.



Privacy-Preserving Trajectory Collection in Five Stages

Client Registration (CR)

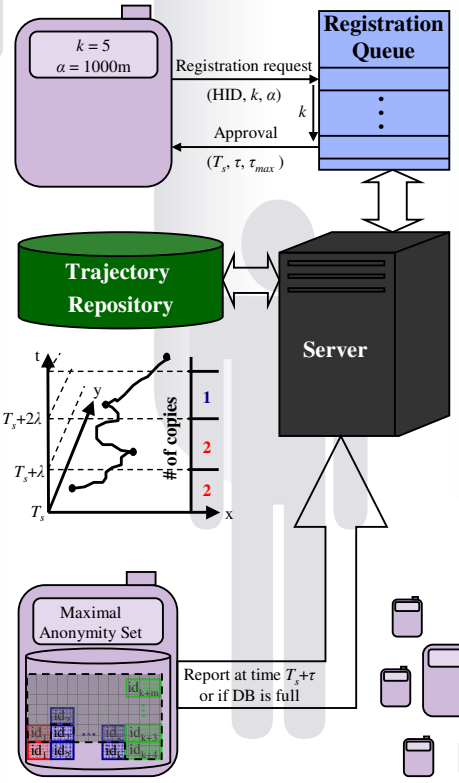
In the CR stage, the client expresses its privacy requirements (k,α). In response, the server **approves a group of *k* clients** and sends them timing parameters (start time: T_s, reporting period: τ). The CR stage ensures the ***k*-anonymity** of clients.

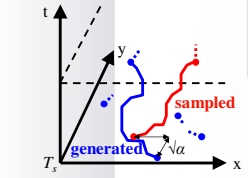
Data Summarization (DS)

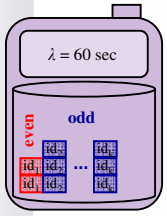
In the DS stage the server continuously records the reports, merges trajectory pieces and monitors the number of pdis received for each trajectory piece. For a given trajectory, if after $T_s+2\tau$ the majority parity of the number of pdis for the trajectory pieces is **even** the trajectory is **real** and is **stored** in the Trajectory Repository (TR), **otherwise** the trajectory is **synthetic** and is **discarded**. The DS stage ensures the ***k*-anonymity** of the data in TR.

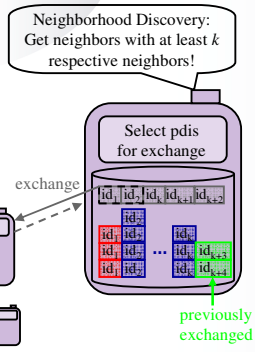
Data Reporting (DR)

After the reporting period has elapsed or the client DB is full, the client enters the DR stage. In the DR stage the client determines a **maximal anonymity set** of pdis, in which the number of pdis for each ID is statistically equal, and sends this set to the server. The DR stage ensures the ***k*-*α*-anonymity** of the reported data.









Trajectory Sampling and Anonymization (TSA)

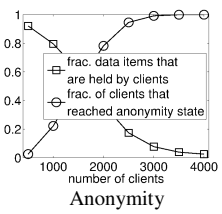
In the TSA stage, the client continuously samples its real trajectory and **generates *k*-1 realistic and pair-wise *α*-diverse synthetic trajectories** and cuts the trajectories into pieces at every λ-period. Trajectory **pieces of a trajectory are tagged with an ID** and form partial data items (pdis). At every λ-period an **even** number of copies of **sampled pdi** and **odd** number of copies of the **generated pdis** are stored in the trajectory DB of the client. The TSA stage ensures the ***k*-*α*-anonymity** of the client trajectory DB.

Trajectory Exchange (TE)

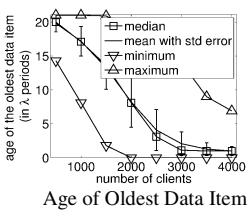
In the TE stage, the client periodically performs a Neighborhood Discovery (ND) process to find other clients to exchange pdis with. The pdis to be exchanged are randomly selected, but contain **at least two sampled or generated-pdis** and older pdis are prioritized. The TE stage ensures the ***k*-*α*-anonymity** of the exchanged data.

Empirical Evaluation and Results

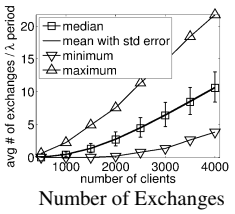
Realistic simulation shows that the method works under reasonable conditions and anonymity settings (communication range = 10 meters and $k = 5$ is shown). In particular, most clients can report most of the collected data in a privacy-preserving fashion. The collection is virtually lossless. In summary, the proposed system collects exact trajectories without loss, does not require trusted components, and provides strong privacy guarantees.



Anonymity



Age of Oldest Data Item



Number of Exchanges

Győző Gidófalvi: Uppsala University – Department of Information Technology – gyozo.gidofalvi@it.uu.se
Xuegang Huang: Aalborg University – Department of Computer Science – xghuang@acm.org
Torben Bach Pedersen: Aalborg University – Department of Computer Science – tbp@cs.aau.dk