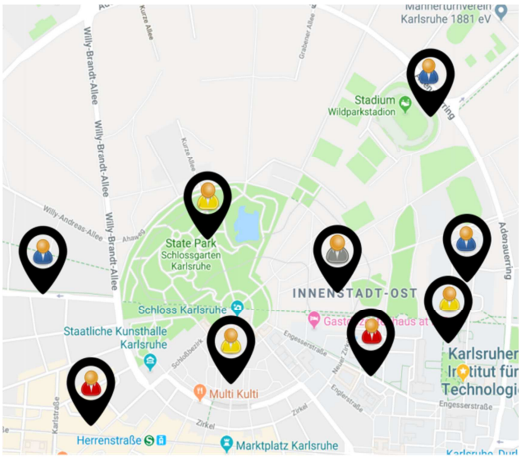
Institut für Programmstrukturen und Datenorganisation (IPD)
Lehrstuhl für Systeme der Informationsverwaltung, Prof. Böhm
Bachelor/Master Thesis

Karlsruher Institut für Technologie

Bachelor/Master Thesis

Location sharing with secrecy guarantees in mobile social networks



With the emergence of mobile computing, a new mode of social networks known as mobile social networks (mSNs), like Facebook Place, PCube, Foursquare, Badoo, has become popular in the last years. Similarly to traditional social networks, mSNs allow users to create virtual communities for spreading contents, but they also let users share their location with other users. In fact, location-based services are one of the most popular services provided by mSNs. Location-based services allow users to connect with others based on their current locations and perform location-dependent queries like “who are my nearby friends?” While location-based services offer great advantages to daily life, secrecy concerns have become one of the main worries due to location information exposure. Indeed, the physical position of a user can be used to infer other personal information such as political affiliations, state of health or personal preferences.

The challenges in location sharing in mSNs regarding secrecy are manifold:

1. How to offer location secrecy guarantees? The physical position of users must not be learned by any unauthorized user including the service provider.
2. How to offer relationships secrecy guarantees? Adversaries, including the service provider, should not learn the relationships existing between users.
3. How to conduct location-dependent queries while guaranteeing 1 and 2? For instance, one type of query that users in mSNs are interested in is “who are my nearby friends?”

The target of this thesis is to come up with an approach for location sharing in mSNs that tackle challenges 1-3 in combination. For bachelor students, we will provide certain simplifications of the assignment. This includes the following tasks:

- Literature review of existing approaches in the area.
- Designing and implementing your proposed approach, together with some reference approaches.
- Evaluation of your proposed approach and comparison with existing ones in terms of secrecy guarantees and performance.

Throughout this work, the student will use encryption techniques and will learn how to conduct controlled experiments to compare results of her/his work to the state of art.

Contact

Gabriela Suntaxi | Gabriela.suntaxi@kit.edu | +49 721 608-45433 | Raum: 352

Am Fasanengarten 5 | 76131 Karlsruhe | Gebäude: 50.34