Guest editorial: Location-centric Privacy in Mobile Services

Guest Editors:
Maria Luisa Damiani (Dept. of Computer Science, University of Milan, Italy – damiani@di.unimi.it)
Gabriel Ghinita (Dept. of Computer Science, University of Massachusetts Boston – Gabriel.Ghinita@umb.edu)

Individual location of users is an enabling factor in a variety of mobile applications, such as location-based services (LBS) and participatory sensing. LBS provide users with valuable information that is relevant to their geospatial context, whereas participatory sensing enables gathering of geo-referenced data through sensor-equipped mobile phones. In all of these applications, the users' locations are communicated to a third party that is not necessarily trusted. Sending location data to untrusted parties may lead to serious privacy risks, resulting in disclosure of sensitive individual details, such as health status, political affiliations, alternative lifestyles, etc.

The goal of this special issue is to disseminate recent advances in location privacy models and technologies for mobile applications. We selected for inclusion in this issue a number of three articles, discussed next.

The first article is entitled "Protecting Query Privacy in Location-based Services", and is written by Xihui Chen and Jun Pang (both from University of Luxembourg). This work presents an approach to protect users' anonymity in LBS through location generalization. The authors address the challenging case when additional background information is available to an attacker, in the form of contextual information. Specifically, the work examines in detail two types of contexts: user profiles and query dependencies. This approach goes beyond the concept of location k-anonymity to develop a comprehensive framework including alternative privacy metrics, grounded on probabilistic models, as well as algorithms for the computation of generalized locations based on the users' privacy preferences. The overall result is a solid framework that advances the state-of-the-art in privacy-preserving location generalization.

The second article is "Effective Mix-zone Anonymization Techniques for Mobile Travelers", by Balaji Palanisamy (University of Pittsburgh) and Ling Liu (Georgia Institute of Technology). The authors present an approach based on the deployment of mix-zones in the context of LBS supporting continuous queries within a road network. When deployed on road networks, mix-zones are subjected to powerful attacks that factor in knowledge about the network infrastructure, patterns of user mobility, as well as temporal, spatial and semantic correlations of location queries. The article examines such attacks, and proposes countermeasures to defend against them.

The third paper, "User-Side Adaptive Protection of Location Privacy in Participatory Sensing", is written by Berker Agir, Thanasis G. Papaioannou, Rammohan Narendula, Karl Aberer and Jean-Pierre Hubaux (all from École Polytechnique Fédérale de Lausanne). Here, the problem is to protect the location of non-anonymous users participating in the collection of geo-referenced data against an attacker who has background knowledge on the user placement. The authors present a privacy model that consists of a location obfuscation mechanism which is adaptive and can be personalized according to user preferences. The model factors in the background knowledge available to an adversary, and expresses it in probabilistic terms. The article presents a formally grounded and novel approach to location obfuscation which can be applied in a variety of applications, beyond participatory sensing, e.g., LBS.

We hope that the readers will find the research published in this issue insightful and inspirational. The guest editors would like to thank the GeoInformatica editorial board for giving us the opportunity to publish these quality articles. We would also like to thank the authors for their contributions, and the reviewers for their efforts in putting together this special issue.