# MobiCrowd: A Collaborative Location-Privacy Preserving Mobile Proxy

Reza Shokri, Panos Papadimitratos, and Jean-Pierre Hubaux
Laboratory for Computer Communications and Applications, EPFL, Switzerland
firstname.lastname@epfl.ch

**Abstract:** ***We demonstrate the first, to the best of our knowledge, LBS client that safeguards user privacy against non-trustworthy LBS servers. Our collaborative approach allows the client to obtain responses from its near-by peers rather than submitting the query to the LBS. Our demo makes the user aware of her privacy level and offers tunable user parameters. The demo contributes a novel user-centric approach that enhances privacy without altering the business model of location-based services.***

**Introduction.** Smart phone users are now offered localization devices (integrated GPS receivers) or positioning services (e.g., based on near-by infrastructure). This enables a range of *location-based services* (LBS), allowing users to submit queries on their *points of interest* (POI) when they find themselves in place and get the LBS server response. The loss of privacy and even more dire consequences is the flip-side of getting information when and where it is needed. User queries provide sensitive information to the LBS provider, which could be non-trustworthy, i.e., misuse or fail to protect LBS logs and cause a breach of user privacy. The user could be tracked in time and space and even be identified [1]. Worse even, learning that a user is away from her home could allow a house break-in or a blackmail [2].

To enhance LBS user privacy, location samples could be obfuscated [3], a trusted third party or a centralized proxy run by the LBS could anonymize queries before passing them to the LBS. Such approaches have a down-side, e.g., obfuscation cannot be effective against absence disclosure [4]; or they require centralized intervention, or changes to the LBS, with little incentive to be adopted.

**Our Approach.** Our *main contribution* is a novel collaborative privacy protection mechanism: basically, a user device can avoid disclosing private information (location and sensitive information on the user's activities) if it can obtain a response to her LBS query by near-by peers (i.e., other reachable user devices) that have the sought information on the POI. Our scheme leverages the abilities of contemporary smart phones: they can establish ad hoc connections when in range, beyond connecting to infrastructure (e.g., cellular base stations and Wi-Fi access points).

We build a *mobile proxy* in each device that protects the user privacy. Devices maintain a POI buffer, checked for available information when the user enters a query. If not available, our mobile proxy broadcasts the query (i.e., the region and information of interest) to other nearby devices. If and only if none of those neighbors can provide the requested information, the LBS is queried. Intuitively, our approach eliminates a significant part of queries to and thus user information made available at the LBS. This prevents or significantly limits privacy breaches: the mobile device can essentially "hide" from the LBS, while it can still obtain promptly the sought information.

**Implementation.** We implemented our scheme on the Nokia N810 and N900 mobile devices, and demonstrate it with the Maemo Mapper. First, mobile devices contact each other and the server via one WiFi interface, thus the mobile proxy automatically switches from ad-hoc to infrastructure mode (and vice-versa) to enable both peer-to-peer and LBS communication (e.g., via an AP). Second, the mobile proxy can connect to the LBS through the cellular interface, thus eliminating the need for WiFi mode switching and imposing a negligible delay to connect to the LBS.

Our scheme does not mandate any real-time interaction with the user. Our demonstration system offers features for flexibility and usability: (i) it displays a continuously updated user *privacy level metric*, for the user to be aware of how well she is "hidden" from the LBS; and it allows the user to tune (ii) a *peer-to-peer query response time-out*, trading off privacy protection for prompt data acquisition, and (iii) a *collaboration level*, i.e., the extent (e.g., time, number of times) the user wishes her device to respond to LBS queries, to control personal cost.

**Performance Evaluation.** A poster with detailed simulation results will show that few user collaborations can hide a great amount of information and thus drastically reduce the ability to track and eventually identify users or the their absence. The collaboration cost (e.g., energy expenditure) is also kept low, with each user servicing very few queries.

## 1. REFERENCES

[1] P. Golle and K. Partridge, On the Anonymity of Home/Work Location Pairs, *Pervasive*, Berlin, Germany, 2009

[2] URL: http://www.pleaserobme.com

[3] M. Gruteser and D. Grunwald, Anonymous Usage of Location-Based Services through Spatial and Temporal Cloacking, *ACM MobiSys*, New York, USA, 2003

[4] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, A Distortion-based Metric for Location Privacy, *ACM WPES*, Chicago, IL, 2009