**Hiding in the Mobile Crowd: Location Privacy through Collaboration**

**ABSTRACT:**

Location-aware smartphones support various location-based services (LBSs): users query the LBS server and learn on the fly about their surroundings. However, such queries give away private information, enabling the LBS to track users. We address this problem by proposing a user-collaborative privacy-preserving approach for LBSs. Our solution does not require changing the LBS server architecture and does not assume third party servers; yet, it significantly improves users’ location privacy. The gain stems from the collaboration of mobile devices: they keep their context information in a buffer and pass it to others seeking such information. Thus, a user remains hidden from the server, unless all the collaborative peers in the vicinity lack the sought information. We evaluate our scheme against the Bayesian localization attacks that allow for strong adversaries who can incorporate prior knowledge in their attacks. We develop a novel epidemic model to capture the, possibly time-dependent, dynamics of information propagation among users. Used in the Bayesian inference framework, this model helps analyze the effects of various parameters, such as users’ querying rates and the lifetime of context information, on users’ location privacy. The results show that our scheme hides a high fraction of location-based queries, thus significantly enhancing users’ location privacy. Our simulations with real mobility traces corroborate our model-based findings. Finally, our implementation on mobile platforms indicates that it is lightweight and the cost of collaboration is negligible.

**EXISTING SYSTEM:**

Among other increasingly powerful mobile computing devices, offer various methods of localization. Integrated GPS receivers, or positioning services based on nearby communication infrastructure (Wi-Fi access points or base stations of cellular networks), enable users to position themselves fairly accurately, which has led to a wide offering of Location-based Services (LBSs). Such services can be queried by users to provide real-time information related to the current position and surroundings of the device, e.g., contextual data about points of interest such as petrol stations, or more dynamic information such as traffic conditions. The value of LBSs is in their ability to obtain on the fly up-to-date information. Although LBSs are convenient, disclosing location information can be dangerous. Each time an LBS query is submitted, private information is revealed. Users can be linked to their locations, and multiple pieces of such information can be linked together. They can then be profiled, which leads to unsolicited targeted advertisements or price discrimination.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Can be inferred from a user’s whereabouts. This could make user the target of blackmail or harassment.
* A stalker can also exploit the location information.
* Misuse their rich data by, e.g., selling it to advertisers or to private investigators.

**PROPOSED SYSTEM:**

We propose a novel location-privacy preserving mechanism for LBSs. To take advantage of the high effectiveness of hiding user queries from the server, which minimizes the exposed information about the users’ location to the server, we propose a mechanism in which a user can hide in the mobile crowd while using the service. The rationale behind our scheme is that users who already have some location-specific information (originally given by the service provider) can pass it to other users who are seeking such information. They can do so in a wireless peer-to-peer manner. Simply put, information about a location can “remain” around the location it relates to and change hands several times before it expires. Our proposed collaborative scheme enables many users to get such location-specific information from each other without contacting the server, hence minimizing the disclosure of their location information to the adversary

**ADVANTAGES OF PROPOSED SYSTEM:**

* The System is attached to the information and protected with the digital signature.
* Malicious users cannot mislead others into receiving fake information, because messages are digitally signed by the LBS.
* A user’s query becomes hidden from the server due to MobiCrowd protocol.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium IV 2.4 GHz.
* Hard Disk : 40 GB.
* Floppy Drive : 1.44 Mb.
* Monitor : 15 VGA Colour.
* Mouse : Logitech.
* Ram : 512 Mb.
* MOBILE : ANDROID

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/7.
* Coding Language : Java 1.7
* Tool Kit : Android 2.3 ABOVE
* IDE : Eclipse

**REFERENCE:**

Reza Shokri, George Theodorakopoulos, Panos Papadimitratos, Ehsan Kazemi, and Jean-Pierre Hubaux, Fellow, IEEE “Hiding in the Mobile Crowd: Location Privacy through Collaboration” **IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 3, MAY-JUNE 2014**