الحفاظ على خصوصية موقع المستخدم للاستعلامات المستمرة للخدمات المعتمدة على الموقع الجغرافي

رائد سعيد نعمان الذبحاني

بحث مقدم لنيل درجة الدكتوراة في علوم الحاسبات

إشراف

د. إياد كاتب

أ.د. راشد محمود

مستخلص

أدى الانتشار الواسع للأجهزة المتنقلة والمزودة بمستشعرات تحديد الموقع الجغرافي وكذا الاتصال بشبكة الانترنت إلى طفرة في سوق الخدمات المعتمدة على المكان. استخدام هذه النوعية من الخدمات يتضمن مشاركة أجهزة خوادم مزودي هذه الخدمات ببيانات تواجد المستخدم في لحظة معينة من الزمان في مكان محدد. لذا، فإن استخدام هذه النوعية من الخدمات بدون الحفاظ على خصوصية موقع المستخدم يعطي الفرصة لمزودي هذه الخدمات الراغبين بإساءة استخدام هذه البيانات بجمع هذه البيانات وتخزينها وتقديمها إلى أي أطراف أخرى. نتيجة لذلك، تم اقتراح العديد من الحلول للحفاظ على خصوصية الموقع الجغرافي للمستخدم. الهدف من هذه الحلول هو استخدام طرق فعالة للاستعاضة عن ارسال الموقع الدقيق للمستخدم بنسخة مشوشة لذلك الموقع أو نسخة ذات دقة أقل. على الرغم من فعالية هذه الطرق في الحفاظ على خصوصية الموقع للاستعلامات الغير مستمرة، الإ أن أبرز المشاكل التي تواجهها هي الحفاظ على خصوصية الموقع للاستعلامات المستمرة. يرجع ذلك إلى عدم قدرة هذه الطرق على قياس تسرب الخصوصية الناتج من استخدام الاستعلامات المستمرة وكذا عدم القدرة على التعامل معها بالشكل المناسب. في هذا البحث، تم إقتراح إطار عمل يهدف للحفاظ على خصوصية الموقع للاستعلامات المستمرة للخدمات المعتمدة على الموقع الجغرافي. تم تحديد مجموعة من المتطلبات الواجب توفرها لتحقيق خصوصية موقع المستخدم أثناء استخدام الاستعلامات المستمرة. تم إقتراح أداة قياس لخصوصية موقع المستخدم بحيث تكون قادرة على قياس تسرب الخصوصية المتوقع للاستعلامات المستمرة.تم تنفيذ إطار العمل كتطبيق لإجهزة الحاسوب وكتطبيق لنظام الأندرويد. التجارب التي تم إجراءها على بيانات حقيقية أثبتت فعالية إطار العمل المقترح في هذه البحث بمتوسط نسبة تحسين في مستوى الخصوصية يبلغ ٣٤%. أخيرا، يعطي هذا البحث نظرة مستقبلية للقضايا المتعلقة بخصوصية الموقع الجغرافي في بيئة المدن الذكية، حيث تم استخدام إطار العمل المقترح في هذا البحث لإقتراح نظام للحفاظ على خصوصية الموقع الجغرافي في المدن الذكية.

Preserving Location Privacy for Continuous LBS Queries

Raed Saeed Al-Dhubhani

A dissertation submitted for the requirements of the degree of Doctor of Philosophy in Computer Science

Supervised By

Dr. Iyad Katib

Prof. Rashid Mehmood

Abstract

The popularity of mobile devices with positioning capability and Internet accessibility in recent years has led to a revolution in the Location-based services (LBSs) market. Unfortunately, without preserving the user's location privacy, LBS providers can collect and log the accurate location data of the service users and provide them to third parties. Many location privacy preserving mechanisms (LPPMs) have been proposed to preserve the LBS user's location privacy. These mechanisms provide a partial disclosure of the user's location. While said mechanisms have had demonstrable effectiveness with snapshot queries, the shortcoming of supporting continuous queries is their main drawback. This shortcoming is a result of the lack of ability to effectively measure and react to the privacy leakage produced by continuous queries. Continuous queries make location privacy preservation difficult due to the privacy leakage produced by correlating the user's reported locations. In this work, we aim to preserve user location privacy in the case of continuous LBS queries. To achieve that, we propose a framework, namely MOdeling and REacting to Privacy Leakage Sources (MOREPLS). As part of the framework, firstly, we propose a novel set of six requirements that any LPPM should meet in order to provide location privacy for continuous LBS queries. Secondly, we propose a novel

location privacy metric that is capable of measuring location privacy leakage of continuous LBS queries. Thirdly, the framework includes a novel two-phased probabilistic candidate selection algorithm that takes into consideration the correlation between the obfuscated locations in order to preserve privacy for continuous queries. We implement our framework as a desktop application and as an Android App, and evaluate it using a real world dataset (Epfl/mobility). The performance for the framework is compared with the geo-indistinguishability LPPM in terms of privacy (adversary estimation error) and the reported improvements average is 34%. Finally, to give an outlook, we leverage on the MOREPLS framework to propose a location privacy preservation system for smart cities.