مخطط فعال للسمعة والحفاظ على الخصوصية في الاستشعارعن الحشد بواسطة الهواتف المحمولة

بيــان حشــر سعيــد العمــري

المستخلص

الإستشعار عن الحشد بواسطة الهاتف النقال هي تقنية ناشئة بواسطتها يقوم حاملي الهواتف النقالة بتجميع بيانات قيمة ومشاركتها لتطبيقات مختلفة. هذه التقنية أتاحت لنطاق واسع من تطبيقات الإستشعار باستخدام الهواتف النقالة حول العالم لتحسين نوعية حياة الناس. حماية خصوصية المشتركين ومصداقية بيانات الإستشعار تعتبر أهداف متعارضة وأيضاً تحديات في هذا المجال.

تظهر مشكلة الخصوصية في تطبيقات الإستشعار عن الحشد بواسطة الهواتف النقالة بسبب الكشف عن المعلومات المرتبطة بموفر البيانات مثل هوية المشتركين. أيضا مصداقية بيانات الإستشعار مهمة لتطبيقات الإستشعار بواسطة الهواتف المحمولة لانها تشعرالمستخدمين النهائيين لها بالثقة.

في هذا البحث سنتناول مصداقية بيانات الإستشعاروالحفاظ على خصوصية المشتركين ولفعل ذلك سنقوم بتصميم مخطط فعال للسمعة والذي سيقوم بالحفاظ على خصوصية المشتركين في الإستشعار عن الحشد بواسطة الهواتف النقالة. والذي سيتناسب مع جميع التطبيقات في هذا المجال. سنقوم آيضا بمقارنة الإطار المقترح مع المنهجيات الموجودة مسبقاً.

مخطط فعال للسمعة والحفاظ على الخصوصية في الاستشعارعن الحشد بواسطة الهواتف المحمولة

بيــان حشــر سعيــد العمــري

بحث مقدم لنيل درجة الماجستير في العلوم
تخصص تقنية المعلومات

إشراف
د. محمد مصطفى منور
د. سهير الشهري

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبد العزيز
جدة – المملكة العربية السعودية
رمضان ١٤٣٩هـ – مايو 2018 م

An Effective Privacy Preserving Reputation Scheme for Mobile Crowdsensing

Bayan Hashr Saeed Alamri

A thesis submitted for the requirements of the degree of Master of Science

In Information Technology

Supervised by
Dr. Muhammad Mostafa Monowar
Dr. Suhair Alshehri

Faculty of Computing and Information Technology
KING ABDULAZIZ UNIVERSITY
JEDDAH-SAUDI ARABIA
Ramadan 1439 H – May 2018 G

An Effective Privacy Preserving Reputation Scheme for Mobile Crowdsensing

Bayan Hashr Alamri

ABSTRACT

Mobile Crowdsensing (MCS) is an emerging technology in which mobile carriers collect and contribute valuable data for different applications. This technology enables a broad range of sensing applications by leveraging mobile objects worldwide to improve people's quality of life. Protecting the privacy of participants and the trustworthiness of the sensor data are conflicting objectives and, key challenges in this area. Privacy issues arise from the disclosure of the user-related context information of data providers, such as participants' identities. The trustworthiness of sensed data is important to provide confidence to its end users. This thesis proposes a privacy preserving reputation schema that preserves privacy and ensure data trustworthiness of the sensor readings for MCS applications. The proposed work also counters a number of possible attacks that might occur in MCS applications. We present a detailed security analysis to prove the effectiveness of our approach in terms of its resistance to different kinds of attacks and its low overhead. We conducted an extensive simulation to investigate the performance of our schema. The obtained results show that the proposed schema is practical; it succeeds in identifying malicious users in most scenarios. In addition, it tolerates a large number of colluding adversaries even if their number surpass 65%. Moreover, it detects On-Off attackers even if they report trusted data with high probability (0.8).