بنية متينة مُتعمدة على الوكيل لحماية شاملة للخصوصية في الخدمات المعتمدة على الموقع

محمد شادي احمد الرحال

بحث مقدم لنيل درجة دكتوراه الفلسفة
في علوم الحاسب

إشراف
أ.د ماهر خماخم, أ.د كمال جمبي

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

بنية متينة مُعتمدة على الوكيل لحماية شاملة للخصوصية في الخدمات المعتمدة على الموقع

محمد شادي احمد الرحال

المستخلص

تلقَّت الخدمات المعتمدة على الموقع في الآونة الأخيرة اهتماماً كبيراً من قبل المجتمع العلمي بسبب التطور في أجهزة المحمول و انفتاح الشبكات اللاسلكية. في تطبيقات الخدمات المعتمدة على الموقع, يُجْبَر المستخدم على بناء استعلامه معتمداً على موقعه الجغرافي الحقيقي للبحث عن نقاط الاهتمام الأقرب. يُمكن أن يُتَتَبع الموقع الحقيقي للمستخدم, كما يُمكن أن تُحلل استعلاماته المُرسلة - من قبل مهاجم ما - بغرض جمع معلومات شخصية حسَّاسة. عندما يكون مزود الخدمات المعتمدة على الموقع هو المهاجم, فإن الضرر الحاصل قد يصل إلى مستويات خطيرة جداً قد تُهدد حياة مستخدمي الخدمات المعتمدة على الموقع. بالتالي, فإن ضمان حماية الخصوصية الشاملة تُعد مسألة بالغة الأهمية. في هذا العمل, نُقدم نظاماً يضمن حماية الخصوصية لمستخدمي الخدمات المعتمدة على الموقع. نظامنا المُقترح يحد من إمكانية المهاجم (مزود الخدمة كعضو خبيث) من تجميع معلومات شخصية حتى و إن تم تطبيق مزيج من هجمات الاستنتاج المتقدمة, مثل هجوم تجانس الموقع, هجوم تقطيع الاستعلام, و هجوم الموقع الدلالي. تحديداً, نُقدم نهج القائد الذي يمنع كل أعضاء العنقود من الاتصال أساساً بمزود الخدمة. يعمل نهج القائد بطريقة تعاونية تضمن حماية خصوصية كاملة لمستخدمي الخدمات المعتمدة على الموقع اعتماداً على علاقة التكافل بين القائد و أعضاء عنقوده. إضافةً لذلك, نُقدم

نهج اختيار الموقع الكاذب الحكيم لضمان حماية خصوصية الموقع لمستخدمي الخدمات المعتمدة على الموقع بشكل إفرادي. يقوم نهج اختيار الموقع الكاذب الحكيم بتوليد مواقع كاذبة لا يُمكن تمييزها عن الموقع الحقيقي للمستخدم. لضمان حماية خصوصية شاملة, فإن كلا النهجين (نهج القائد و نهج اختيار الموقع الكاذب الحكيم) يتكاملان مع نهج مُعتمد على التقسيم يُدعى التقسيم-أيمن-أيسر. يضمن نهج التقسيم-أيمن-أيسر حماية خصوصية الاستعلام خلال مراحل الإرسال, المعالجة, و الإجابة. لمعالجة استعلامات الجيران الأقرب بشكل فعَّال, فإننا نُقدم أيضاً تقنية فهرسة معتمدة على الخلية. تضمن أيضاً تقنية الفهرسة المعتمدة على الخلية سرعة و دقة إجابات استعلامات الجيران الأقرب. أظهرت النتائج تفوُّق النُّهُج المقترحة في هذا البحث على مثيلاتها في مصطلحات مستوى حماية الخصوصية المُحقق, المتانة ضِدَّ الهجمات الاستدلالية, تكاليف الاتصال, و زمن الاستجابة. تم اقتراح موديل استهلاك طاقة - مُخصص للخدمات المعتمدة على الموقع - كمقياس لتقييم النُّهج المُقترحة في هذا البحث. اعتماداً على موديل استهلاك الطاقة المُقترح, تم تقديم توصيات لمستخدمي الخدمات المعتمدة على الموقع للحفاظ على طاقة البطارية لأجهزتهم المحمولة.

A Robust Agent Based Architecture for Comprehensive Privacy Protection in Location Based Services

Mohamad Shady Ahmad Alrahhal

A thesis submitted for the requirements of the

Doctorate Philosophy Degree in Computer Science

Supervised By
Professor Maher Khemahkem
Professor Kamal Jambi

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

A Robust Agent Based Architecture for Comprehensive Privacy Protection in Location Based Services

Mohamad Shady Ahmad Alrahhal

ABSTRACT

Recently, Location Based Services (LBS) have received significant amount of attention from the research community due to the development of mobile devices and the openness of wireless networks. In LBS, the users are forced to build their queries based on their real locations to find the nearest Point of Interests (POI). The real locations of the LBS users and their sent queries could be tracked and analyzed by an attacker to gather personal and sensitive information. When LBS server (or its maintainer) is the attacker, the damage caused by compromising the privacy can reach dangerous levels that may threaten the lives of the LBS users. Consequently, ensuring comprehensive privacy protection is a critical issue. In this work, we introduce a system that ensures comprehensive privacy protection for LBS users. Our proposed system can limit the ability of the LBS server (a malicious party) from collecting personal information, even if a mixture of advanced inference attacks are applied, such as location homogeneity, query sampling, and semantic location attacks. Specifically, we introduce the Leader approach that prevents all cluster members from connecting to the LBS server. The Leader approach ensures full privacy protection in a collaborative way based on a symbiotic relationship between the Leader and his cluster members. In addition, we introduce the Wise Dummy Selection Location (WDSL) approach to ensure the location privacy of LBS users individually. The WDSL approach generates strong dummy locations that cannot be distinguished from the real location of the LBS user. To ensure comprehensive privacy protection, both the Leader and WDSL approaches are integrated with a fragmentation based approach called Left-Right-Fragmentation (LRF). The proposed LRF approach ensures the query privacy during sending, processing, and responding phases. To manipulate K-Nearest Neighbor (K-NN) queries efficiently, we introduce the Cell Based Indexing (CBI) technique. The CBI technique ensures the speed and accuracy of the K-NN queries' responses. The results showed that the proposed approaches outperform the similar approaches in terms of privacy protection level, resistance against inference attacks, communication costs, and response time. A power consumption model, customized for LBS applications, is proposed as a metric to evaluate our own proposed approaches. Depending on the proposed power consumption model, recommendations are presented for the LBS users to save the lifetime of their mobile devices' battery.